



governmentattic.org

"Rummaging in the government's attic"

Description of document: Excerpts from ten Treasury Inspector General for Tax Administration (TIGTA) reports, 2000 - 2003

Requested date: 28-April-2011

Released date: 14-June-2011

Posted date: 08-August-2011

Titles of documents: See following page

Source of document: Treasury Inspector General for Tax Administration
Office of Chief Counsel Disclosure Branch
1125 15th Street, N.W.
Room 700A
Washington, DC 20005
ATTN: Disclosure Officer
Fax: (202) 622-3339
Email: FOIA.Reading.Room@tigta.treas.gov

Note: The release consists of the first ten pages of each of the included reports

The governmentattic.org web site ("the site") is noncommercial and free to the public. The site and materials made available on the site, such as this file, are for reference only. The governmentattic.org web site and its principals have made every effort to make this information as complete and as accurate as possible, however, there may be mistakes and omissions, both typographical and in content. The governmentattic.org web site and its principals shall have neither liability nor responsibility to any person or entity with respect to any loss or damage caused, or alleged to have been caused, directly or indirectly, by the information provided on the governmentattic.org web site or in this file. The public records published on the site were obtained from government agencies using proper legal channels. Each document is identified as to the source. Any concerns about the contents of the site should be directed to the agency originating the document in question. GovernmentAttic.org is not responsible for the contents of documents published on the website.

TIGTA REPORT EXTRACTS INCLUDED

Reference No.	Title
2001-10-010	Management Advisory Report: Review of Alleged Regulatory Violation in Administering the Accounting Support Services Contract), October 2000, released in full.
2003-20-220	The Information Technology Services Organization Needs to Complete Its Business Resumption Planning, September 2003, released in full.
2003-20-211	Key Security Controls of the Currency and Banking Retrieval System Have Not Been Implemented, September 2003, released in full.
2001-30-160	The Offshore Credit Card Project Shows Promise, but Improvements Are Needed to Ensure That Compliance Objectives Are Achieved, August 2003, released in full.
2003-20-019	Computer Security Vulnerabilities Vary Among Internal Revenue Service Offices, October 2002, released in full.
2003-30-020	Management Oversight of the Acceptance Agent Program Is Needed to Assure that Individual Taxpayer Identification Numbers Are Properly Issued, November 2002, released in full.
2003-40-108	Controls Need to Be Improved to Ensure Accurate Direct Deposit of Tax Returns, May 2003. We are releasing the ten (10) pages in part. We are asserting FOIA subsections (b)(3) in conjunction with I.R.C. § 6103(a) and (b)(7)(C) as the justification for withholding.
2004-40-016	Increased Taxpayer Awareness and Improved Guidance Are Needed to Ensure Accurate Direct Deposit of Tax Refunds Claimed on E-Filed Tax Returns, October 2003. We are releasing the ten (10) pages in part. We are asserting FOIA subsections (b)(3) in conjunction with I.R.C. § 6103(a) and (b)(7)(C) as the justification for withholding.
2001-20-108	Persistent Physical Security Vulnerabilities Should Be Corrected to Better Protect Facilities and Computer Resources, July 2001, released in full.
2001-20-020	Computer Security Controls Should Be Strengthened in the Former Brooklyn District, November 2000, released in full. The DRAFT version is the only available copy.



DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20005

INSPECTOR GENERAL
FOR TAX
ADMINISTRATION

June 14, 2011

This is in response to your April 28, 2011, Freedom of Information Act (FOIA) request, seeking access to records maintained by the Treasury Inspector General for Tax Administration (TIGTA). The TIGTA Disclosure Branch received your request on May 4, 2011. Specifically, you requested a copy of the first ten (10) pages of each of the following TIGTA reports:

2001-10-010 dated October 2000
2003-20-220, dated September 2003
2003-20-211, dated September 2003
2003-30-160, dated August 2003
2003-20-019, dated October 2002
2003-30-020, dated November 2002
2003-40-108 dated May 2003
2004-40-016 dated October 2003
2001-20-108 dated July 2001
2001-20-020 dated November 2000

Enclosed is a copy of the first ten (10) pages of each of the referenced audit reports that have been reviewed for release to you under the FOIA:

<u>Reference Number</u>	<u>Title</u>
2001-10-010	<i>Management Advisory Report: Review of Alleged Regulatory Violation in Administering the Accounting Support Services Contract), October 2000, released in full.</i>
2003-20-220	<i>The Information Technology Services Organization Needs to Complete Its Business Resumption Planning, September 2003, released in full.</i>

- 2003-20-211 *Key Security Controls of the Currency and Banking Retrieval System Have Not Been Implemented*, September 2003, released in full.
- 2001-30-160 *The Offshore Credit Card Project Shows Promise, but Improvements Are Needed to Ensure That Compliance Objectives Are Achieved*, August 2003, released in full.
- 2003-20-019 *Computer Security Vulnerabilities Vary Among Internal Revenue Service Offices*, October 2002, released in full.
- 2003-30-020 *Management Oversight of the Acceptance Agent Program Is Needed to Assure that Individual Taxpayer Identification Numbers Are Properly Issued*, November 2002, released in full.
- 2003-40-108 *Controls Need to Be Improved to Ensure Accurate Direct Deposit of Tax Returns*, May 2003. We are releasing the ten (10) pages in part. We are asserting FOIA subsections (b)(3) in conjunction with I.R.C. § 6103(a) and (b)(7)(C) as the justification for withholding.
- 2004-40-016 *Increased Taxpayer Awareness and Improved Guidance Are Needed to Ensure Accurate Direct Deposit of Tax Refunds Claimed on E-Filed Tax Returns*, October 2003. We are releasing the ten (10) pages in part. We are asserting FOIA subsections (b)(3) in conjunction with I.R.C. § 6103(a) and (b)(7)(C) as the justification for withholding.
- 2001-20-108 *Persistent Physical Security Vulnerabilities Should Be Corrected to Better Protect Facilities and Computer Resources*, July 2001, released in full.
- 2001-20-020 *Computer Security Controls Should Be Strengthened in the Former Brooklyn District*, November 2000, released in full.
The DRAFT version is the only available copy.

As noted, we have withheld information from the audit reports pursuant to FOIA FOIA subsections (b)(3) in conjunction with I.R.C. § 6103(a) and (b)(7)(C). The withheld information in the audit reports contains return information, as that term is defined in I.R.C. § 6103(a), of individuals other than you. The information pertaining to third parties was collected by the Secretary of the Treasury with respect to determining the liability of individuals under Title 26, and therefore is exempt from disclosure in

response to your FOIA request. Accordingly, we are withholding this material pursuant to FOIA subsection (b)(3) in conjunction with I.R.C. § 6103(a).

FOIA subsection (b)(7)(C) permits an agency to withhold "information compiled for law enforcement purposes the release of which could reasonably be expected to constitute an unwarranted invasion of personal privacy." The withheld information consists of identifying information compiled with regard to third parties. Releasing the withheld information would not shed any light into the Agency's performance of its official functions, but instead could result in an invasion into the personal privacy of the individuals whose names and personal information have been withheld. The information was collected as part of the audit and the privacy interest of the third parties outweighs the public's interest in having the information released. As a result, this information has been withheld in response to your request.

We have enclosed an Information Sheet that explains the subsections cited above as well as your administrative appeal rights. You may appeal this decision within thirty-five (35) days from the date of this letter. Your appeal must be in writing and signed by you. You should address the envelope as follows:

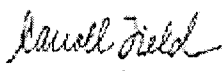
Freedom of Information Act Appeal
Treasury Inspector General for Tax Administration
Attn: IG:CC Room 700A
1125 15th Street, NW
Washington, DC 20005

Since the cost incurred for processing this FOIA request is less than \$25.00, the threshold set by Treasury's FOIA regulation, we are not assessing any fees.

These ten (10) audit reports have been decontrolled for release and the "Limited Official Use" designations have been removed pursuant to Treasury Directive TD P 15-71, Department of the Treasury Security Manual.

If you have any questions concerning this matter, please contact Program Analyst Carroll Field at (202) 927-7032 and refer to case number 2011-FOI-00126.

Sincerely,


(For) Amy P. Jones
Disclosure Officer

Enclosures

Audit Reference Numbers:

2001-10-010
2003-20-220
2003-20-211
2003-30-160
2003-20-019
2003-30-020
2003-40-108
2004-40-016
2001-20-108
2001-20-020

Information on a TIGTA Determination to Withhold Records Exempt From The Freedom of Information Act – 5 U.S.C. § 552

Appeal Rights

You may file an appeal with the Treasury Inspector General for Tax Administration (TIGTA) within 35 days after we (1) determine to withhold records, (2) determine that no records exist, or (3) deny a fee waiver or a favorable fee category. If some records are released at a later date, you may file within 35 days after the date the last records were released.

The appeal must be in writing, must be signed by you, and must contain the following information:

your name and address
description of the requested records
date of the request (and a copy, if possible)
date of the letter denying the request (and a copy, if possible).

Mail your appeal to: Freedom of Information Appeal
Treasury IG for Tax Administration
Attn: IG:CC Room 700A
1125 – 15th Street, NW
Washington, DC 20005

Judicial Review

If we deny your appeal, or if we do not send you a reply within 20 days (not counting Saturdays, Sundays, or legal public holidays) after the date we receive the appeal, you may file a complaint with the U.S. District Court in the district where (1) you reside, (2) your principal place of business is located, or (3) the records are located. You may also file in the District Court for the District of Columbia.

The court will treat your complaint according to the Federal Rules of Civil Procedure (F.R.C.P.). Service of process is governed by Rule 4(d)(4) and (5), which requires that a copy of the summons and complaint be (1) personally served on the United State Attorney for the district in which the lawsuit is brought; (2) sent by registered or certified mail to the Attorney General of the United States at Washington, C.C.; and (3) sent by registered or certified mail to the Treasury Inspector General for Tax Administration, Attn: IG:CC, Room 700A, 1125 – 15th Street, NW, Washington, D.C. 20005.

In such a court case, the burden is on the Treasury Inspector General for Tax Administration to justify withholding the requested records, determining that no records exist, or denying a fee waiver or a favorable fee category. The court may assess against the United States reasonable attorney fees and other litigation costs incurred by the person who takes the case to court and who substantially prevails. You will have substantially prevailed if the court determines, among other factors, that you had to file the lawsuit to obtain the records you requested and that the Treasury Inspector General for Tax Administration had no reasonable grounds to withhold the records. See internal Revenue Service Regulations 26 CFR 601.702 for further details.

Exemptions

The Freedom of Information Act, 5 U.S.C. § 552, does not apply to matters that are –

- (b)(1) (A) specifically authorized under criteria established by an Executive Order to be kept secret in the interest of national defense or foreign policy and
- (B) are, in fact, properly classified under such an Executive Order;

- (b)(2) related solely to the internal personnel rules and practices of an agency;
- (b)(3) specifically exempt from disclosure by statute (other than section 552b of this title), provided that the statute
 - (A) requires that the matters be withheld from the public in such a manner as to leave no discretion on the issue, or
 - (B) establishes particular criteria for withholding or refers to particular types of matters to be withheld;

Note: subsection (b)(3) protects information exempted by certain qualifying statutes, such as Internal Revenue Code section 6103, which protects tax returns and information generated by and collected by the IRS with regard to a taxpayer.

- (b)(4) trade secrets and commercial or financial information obtained from a person and privileged or confidential;
- (b)(5) inter-agency or intra-agency memorandums or letters which would not be available by law to a party other than an agency in litigation with the agency;
- (b)(6) personnel and medical files and similar files that disclosure of which would constitute a clearly unwarranted invasion of personal privacy;
- (b)(7) records or information compiled for law enforcement purposes, but only to the extent that the production of such law enforcement records or information
 - (A) could reasonably be expected to interfere with enforcement proceedings,
 - (B) would deprive a person of a right to a fair trial or an impartial adjudication,
 - (C) could reasonably be expected to constitute an unwarranted invasion of personal privacy,
 - (D) could reasonably be expected to disclose the identity of a confidential source, including a State, local or foreign agency or authority or any private institution which furnished information on a confidential basis, and in the case of a record or information compiled by a criminal law enforcement authority in the course of a criminal investigation, or by an agency conducting a criminal investigation, or by an agency conducting a lawful national security intelligence investigation, information furnished by a confidential source.
 - (E) would disclose techniques and procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law, or
 - (F) could reasonably be expected to endanger the life or physical safety of any individual;
- (b)(8) contained in or related to examination, operating, or condition reports prepared by, on behalf of, or for the use of an agency responsible for the regulation or supervision of financial institutions; or
- (b)(9) geological and geophysical information and data, including maps, concerning wells.

Information on a TIGTA Determination to Withhold Records Exempt From The Freedom of Information Act – 5 U.S.C. § 552

Appeal Rights

You may file an appeal with the Treasury Inspector General for Tax Administration (TIGTA) within 35 days after we (1) determine to withhold records, (2) determine that no records exist, or (3) deny a fee waiver or a favorable fee category. If some records are released at a later date, you may file within 35 days after the date the last records were released.

The appeal must be in writing, must be signed by you, and must contain the following information:

your name and address
description of the requested records
date of the request (and a copy, if possible)
date of the letter denying the request (and a copy, if possible).

Mail your appeal to: Freedom of Information Appeal
Treasury IG for Tax Administration
Attn: IG:CC Room 700A
1125 – 15th Street, NW
Washington, DC 20005

Judicial Review

If we deny your appeal, or if we do not send you a reply within 20 days (not counting Saturdays, Sundays, or legal public holidays) after the date we receive the appeal, you may file a complaint with the U.S. District Court in the district where (1) you reside, (2) your principal place of business is located, or (3) the records are located. You may also file in the District Court for the District of Columbia.

The court will treat your complaint according to the Federal Rules of Civil Procedure (F.R.C.P.). Service of process is governed by Rule 4(d)(4) and (5), which requires that a copy of the summons and complaint be (1) personally served on the United State Attorney for the district in which the lawsuit is brought; (2) sent by registered or certified mail to the Attorney General of the United States at Washington, C.C.; and (3) sent by registered or certified mail to the Treasury Inspector General for Tax Administration, Attn: IG:CC, Room 700A, 1125 – 15th Street, NW, Washington, D.C. 20005.

In such a court case, the burden is on the Treasury Inspector General for Tax Administration to justify withholding the requested records, determining that no records exist, or denying a fee waiver or a favorable fee category. The court may assess against the United States reasonable attorney fees and other litigation costs incurred by the person who takes the case to court and who substantially prevails. You will have substantially prevailed if the court determines, among other factors, that you had to file the lawsuit to obtain the records you requested and that the Treasury Inspector General for Tax Administration had no reasonable grounds to withhold the records. See internal Revenue Service Regulations 26 CFR 601.702 for further details.

Exemptions

The Freedom of Information Act, 5 U.S.C. § 552, does not apply to matters that are –

- (b)(1) (A) specifically authorized under criteria established by an Executive Order to be kept secret in the interest of national defense or foreign policy and
- (B) are, in fact, properly classified under such an Executive Order;

- (b)(2) related solely to the internal personnel rules and practices of an agency;
- (b)(3) specifically exempt from disclosure by statute (other than section 552b of this title), provided that the statute
 - (A) requires that the matters be withheld from the public in such a manner as to leave no discretion on the issue, or
 - (B) establishes particular criteria for withholding or refers to particular types of matters to be withheld;

Note: subsection (b)(3) protects information exempted by certain qualifying statutes, such as Internal Revenue Code section 6103, which protects tax returns and information generated by and collected by the IRS with regard to a taxpayer.
- (b)(4) trade secrets and commercial or financial information obtained from a person and privileged or confidential;
- (b)(5) inter-agency or intra-agency memorandums or letters which would not be available by law to a party other than an agency in litigation with the agency;
- (b)(6) personnel and medical files and similar files that disclosure of which would constitute a clearly unwarranted invasion of personal privacy;
- (b)(7) records or information compiled for law enforcement purposes, but only to the extent that the production of such law enforcement records or information
 - (A) could reasonably be expected to interfere with enforcement proceedings,
 - (B) would deprive a person of a right to a fair trial or an impartial adjudication,
 - (C) could reasonably be expected to constitute an unwarranted invasion of personal privacy,
 - (D) could reasonably be expected to disclose the identity of a confidential source, including a State, local or foreign agency or authority or any private institution which furnished information on a confidential basis, and in the case of a record or information compiled by a criminal law enforcement authority in the course of a criminal investigation, or by an agency conducting a criminal investigation, or by an agency conducting a lawful national security intelligence investigation, information furnished by a confidential source.
 - (E) would disclose techniques and procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law, or
 - (F) could reasonably be expected to endanger the life or physical safety of any individual;
- (b)(8) contained in or related to examination, operating, or condition reports prepared by, on behalf of, or for the use of an agency responsible for the regulation or supervision of financial institutions; or
- (b)(9) geological and geophysical information and data, including maps, concerning wells.

**Management Advisory Report:
Review of Alleged Regulatory Violation in
Administering the Accounting Support
Services Contract**

October 2000

Reference Number: 2001-10-010



INSPECTOR GENERAL
for TAX
ADMINISTRATION

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

October 26, 2000

MEMORANDUM FOR CHIEF, AGENCY-WIDE SHARED SERVICES
CHIEF FINANCIAL OFFICER

Pamela J. Gardiner

FROM: Pamela J. Gardiner
Deputy Inspector General for Audit

SUBJECT: Final Management Advisory Report – Review of Alleged
Regulatory Violation in Administering the Accounting Support
Services Contract

This report presents the results of our review of an allegation regarding whether the Internal Revenue Service (IRS) violated regulations when administering the accounting support services contract. In summary, we found that the allegation could not be substantiated; however, the IRS could have more completely documented the factors considered before exercising the contract option years and taken additional steps to prevent the appearance of an employer-employee relationship between the IRS and the contractor. This report is for information purposes only and does not require a response.

The Treasury Inspector General for Tax Administration has designated this report as Limited Official Use (LOU) pursuant to Treasury Directive TD P-71-10, Chapter III, Section 2, "Limited Official Use Information and Other Legends" of the Department of Treasury Security Manual. Because this document has been designated LOU, it may only be made available to those officials who have a need to know the information contained within this report in the performance of their official duties. This report must be safeguarded and protected from unauthorized disclosure; therefore, all requests for disclosure of this report must be referred to the Disclosure Unit within the Treasury Inspector General for Tax Administration's Office of Chief Counsel.

Please contact me at (202) 622-6510 if you have questions, or your staff may call Maurice S. Moody, Associate Inspector General for Audit (Headquarters Operations and Exempt Organizations Programs), at (202) 622-8500.

Management Advisory Report: Review of Alleged Regulatory Violation in Administering the Accounting Support Services Contract

Objective and Scope

The objective of this review was to determine whether an allegation that the IRS violated the FAR when administering the accounting support services contract could be substantiated.

The objective of this review was to determine whether an allegation that the Internal Revenue Service (IRS) violated the Federal Acquisition Regulations (FAR)¹ when administering the accounting support services contract could be substantiated. The review was performed from May 2000 to August 2000 at the Chief Financial Officer (CFO) and Procurement Offices in Washington, D.C., and at the contractor work site in Beckley, West Virginia.

The scope of our work was limited to reviewing the specific allegation and the related documentation concerning the contract. Fieldwork tests included reviewing contracting files and interviewing program office employees, CFO staff, and contractor personnel. All of the work in this review was performed in accordance with the President's Council on Integrity and Efficiency's *Quality Standards for Inspections*.

Major contributors to this report are listed in Appendix I. Appendix II contains the Report Distribution List.

Background

During the IRS' restructuring effort, the CFO recognized the need to maintain essential accounting and clerical functions at the Beckley Administrative Service Center (BASC) in Beckley, West Virginia. The IRS' goal is to centralize all IRS payments at the BASC by January 2001. To assist in this effort, the IRS obtained a contractor to perform some duties at the BASC after the office of the CFO determined that the workforce needs were greater than the IRS' hiring authority.

¹ GENERAL SERVS. ADMIN. ET AL., FEDERAL ACQUISITION REG. ("FAR"), 48 C.F.R. parts 1-52 (1997).

Management Advisory Report: Review of Alleged Regulatory Violation in Administering the Accounting Support Services Contract

In August 1997, the IRS awarded a contract for accounting support services to be performed at the BASC. The contract included a base year and 4 option years. According to the contract, the contractor is responsible for processing of accounting documents, preparation of reports and procedures, data entry, filing, and other general recurring office tasks.

The Treasury Inspector General for Tax Administration Office of Investigations received an allegation that the IRS had improperly contracted for accounting support services that should have been performed by government employees. In addition, the allegation stated that the contract was a prohibited personal service contract under the provisions of the FAR. The Office of Investigations determined that the case lacked criminal merits and forwarded the allegation to the Office of Audit for further assessment.

Results

We determined that the allegation could not be substantiated.

Based on our limited review, we determined that the allegation could not be substantiated. The accounting support services being acquired were commercial activities. Accordingly, the government has the option of using contractors or government employees to perform them. In this regard, the IRS established a valid business need for contractor support when it first awarded the contract. However, the IRS did not adequately document its business case for extending the contract.

Additionally, although the IRS is not providing day-to-day supervision of contractor employees, aspects of administering the contract could be improved to prevent the risk of a prohibited employer-employee relationship.

**Management Advisory Report: Review of Alleged Regulatory Violation in
Administering the Accounting Support Services Contract**

**The Internal Revenue Service Did Not
Document All Factors Considered Before
Exercising Contract Options**

According to the cost comparison, contracting out these services cost the government approximately \$283,000 more each year than using government employees.

The IRS decided to use a contractor for support services at the BASC even though the cost comparison² did not support this decision. The cost comparison performed by the IRS in Fiscal Year 1998 indicates that it was more economical to perform the accounting support services with government personnel. According to the cost comparison, using a contractor to perform these services cost the government approximately \$283,000 more each year than it would have cost to use government employees.

The accounting support services contract was awarded in August 1997 because a hiring freeze imposed at the IRS prevented the BASC from meeting the work demands. The contract was subsequently renewed in 1998, 1999, and 2000 under the option-year provisions based on the satisfactory performance of the contractor.

A business need was identified when the contract was initially awarded; however, we determined that other possible alternatives were not properly documented before exercising the option years. IRS management attested that other non-monetary considerations impacted the decision to continue the contract, although they did not document them in the contract file. These non-monetary considerations included increasing workload, existing resources, and limitations on available full-time equivalent positions.

The Office of Management and Budget Circular A-76 and the Federal Activities Inventory Reform Act³

² Due to the limited scope of this review, we did not validate the completeness of the IRS' cost comparison. However, the comparison appeared to reflect reasonable cost elements.

³ Federal Activities Inventory Reform Act of 1998, Pub. L. No. 105-270.

Management Advisory Report: Review of Alleged Regulatory Violation in Administering the Accounting Support Services Contract

provide that the federal government should contract out commercial activities when cost beneficial.

Although the cost comparison showed that contractor services would be more expensive, IRS management determined that the contractor was needed to supplement in-house staff to meet requirements for a peak workload. In this regard, the IRS should have maintained better documentation of the relevant factors, both monetary and non-monetary, used to make the decision to award the original contract and in exercising the contract provision for option years.

Aspects of Administering the Contract Can Be Improved to Prevent the Appearance of an Employer-Employee Relationship

While we found no violation of the FAR, the IRS was administering the BASC accounting support services contract in a manner that could give the appearance of an employer-employee relationship. In addition, some of the activities on this contract exposed the IRS to a risk of engaging in prohibited practices.

The FAR provides that the government should not award a contract or administer a contract in a manner that would create an employer-employee relationship. In determining whether an employer-employee relationship exists, the key question is whether the government exercised relatively continuous supervision and control over the contractor personnel performing the contract. Also, the FAR provides descriptive elements for consideration when determining whether an employer-employee relationship exists.⁴ One of these

⁴ There are six descriptive elements to be assessed when determining whether a contract is personal in nature. We believe the first five elements (i.e., performance on site, government furnished principal tools, furtherance of agency mission, comparable services performed by civil service personnel at other agencies, and expected to last beyond 1 year) were met in this contract.

**Management Advisory Report: Review of Alleged Regulatory Violation in
Administering the Accounting Support Services Contract**

The terms and conditions of the contract did not create a personal service contract.

descriptive elements is whether the government directly or indirectly provided supervision to the contractor.

The accounting support services contract states "The parties recognize and agree that no employer-employee [relationship] exists or will exist under the contract between the Government and the Contractor's employees." Additionally, we found no evidence that the IRS is directly supervising contractor employees. However, the IRS is engaging in activities that could be construed as developing an employer-employee relationship.

For example, the IRS is allowing contractor employees to attend training classes with the BASC employees. These training classes (Equal Employment Opportunity (EEO), Unauthorized Access (UNAX), Automated Financial System Security, and local area networking) are geared to government employees and are required for the BASC employees. Although the EEO and UNAX training may be beneficial to contractor employees, we do not believe that these classes are directly related to the contractor's duties. IRS management stated that they believe the training was appropriate and related to the work being performed by the contractor's employees.

Although the contract clearly states that the IRS will provide training for only the first 90 days, the IRS continues to provide training to the contractor's new employees.

In addition, the IRS is continuing to assist the contractor with training new employees. The contract required the IRS to provide training to the contractor within the first 90 days of the contract. After the first 90 days, the contractor was expected to train all new employees at the contractor's expense. However, IRS employees continued to assist in training new contractor employees after the first 90 days.

Further, in a requisition modifying the contract, the justification stated that the IRS was requesting contract employees to work overtime, on a volunteer basis, in order to meet a due date. Under the terms of the contract, scheduling contractor employees is the sole responsibility of the contractor, and the contractor has an on-site supervisor to oversee contractor employees.

Management Advisory Report: Review of Alleged Regulatory Violation in Administering the Accounting Support Services Contract

We believe the IRS' actions in advising the contractor on how to schedule its employees to meet the requested due date could be construed as indirect supervision of the contractor. IRS management explained that they do not believe they told the contractor how to schedule its employees but were acknowledging that overtime would be necessary, thus eliminating the need for the contractor to come back and request overtime. In our opinion, the contractor should have made the decision about the need for overtime and then requested IRS approval for the overtime premiums.

While we believe the contract itself is not a prohibited personal service contract under the provisions of the FAR, the above practices could give the appearance that the contract employees are being treated like government employees and increase the IRS' risk of engaging in prohibited contract practices. Accordingly, the IRS should take the necessary steps to ensure that the terms of this contract are enforced and to prevent any appearance of an employer-employee relationship.

Conclusion

The allegation that the IRS improperly contracted for accounting support services that should have been performed by government employees and entered into a contract that was a prohibited personal service contract could not be substantiated. The accounting support services being acquired were commercial activities that could be legally performed by a contractor. However, the IRS did not adequately document the non-monetary factors considered in making the decision to extend the contract when the IRS' cost comparison indicated it was more economical to perform these tasks in-house. Additionally, some of the actions taken by the IRS could give the appearance of an employer-employee relationship and expose the IRS to a risk of engaging in prohibited contract practices.

**Management Advisory Report: Review of Alleged Regulatory Violation in
Administering the Accounting Support Services Contract**

Appendix I

Major Contributors to This Report

Maurice S. Moody, Associate Inspector General for Audit (Headquarters Operations and
Exempt Organizations Programs)

John Wright, Director

Nancy LaManna, Audit Manager

Regina Dougherty, Senior Auditor

Dawn Smith, Senior Auditor

Andrew Harvey, Auditor

TD P 15-71

**The Information Technology Services
Organization Needs to Complete Its Business
Resumption Planning**

September 2003

Reference Number: 2003-20-220

TD P 15-71



INSPECTOR GENERAL
for TAX
ADMINISTRATION

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

September 30, 2003

MEMORANDUM FOR CHIEF INFORMATION OFFICER

Gordon C. Milbourn

FROM: Gordon C. Milbourn III
Assistant Inspector General for Audit (Small Business and
Corporate Programs)

SUBJECT: Final Audit Report - The Information Technology Services
Organization Needs to Complete Its Business Resumption
Planning (Audit # 200320032)

This report presents the results of our review of the Information Technology Services (ITS) organization's efforts to develop business resumption plans to ensure it can effectively support the Internal Revenue Service's (IRS) critical business processes and information systems following a disaster. Business resumption is the process of re-opening an organization's components or business processes following a disaster. Business resumption planning is undertaken by organizations to provide employees with a documented set of actions to perform in the event of a disaster, enabling business processing to be resumed within critical time periods. The ITS organization will play a critical role in helping to recover IRS information systems and business operations in the event of a disaster at one or more facilities, and should have a specific business resumption plan to timely resume its own operations so it can support the IRS' operations. As such, the ITS organization must be able to recover itself before it can support the information systems needs of its customers.

In summary, business resumption plans have been completed or are in development throughout the ITS organization. At the Atlanta and Memphis Submission Processing Sites,¹ the ITS organization's End-User Equipment & Services function² completed business resumption plans that included sufficient direction to support the resumption of the critical systems we selected for review. These plans included procedures to:

- Resume operations at an offsite location.

¹ Submission processing sites are responsible for processing tax returns and payments.

² The End-User Equipment & Services function provides computer equipment and desktop support to IRS employees located at submission processing sites and field offices within its territory.

- Reassign ITS employees to replace injured employees.
- Acquire office equipment and supplies.
- Designate damage assessment teams.
- Notify other essential ITS offices and contractors.
- Update the employee contact information.

Similarly, at the Laguna Niguel Territory Office's End-User Equipment & Services function,³ the business continuity plan included general procedures to resume operations at an offsite location, acquire office equipment and supplies, and update the employee contact information.

While the ITS organization has made progress in business resumption planning, business resumption plans were not completed for all branches at the Tennessee and Martinsburg Computing Centers⁴ and at the Laguna Niguel Territory Office. At the Tennessee Computing Center, the ITS functions did not have complete business resumption plans for recovering four of the six critical systems operations we selected for review. In the Martinsburg Computing Center, specific business resumption plans have not been prepared. The Laguna Niguel Territory Office did not include the recovery priorities and procedures necessary for the ITS organization's End-User Equipment & Services function to resume its own business.

We also found that the ITS organization can improve the plans it has completed. The plans did not completely identify essential process priorities, designate clear process resumption time periods, document the plan change history, or document plan testing and results.

While the ITS' Mission Assurance office is responsible for coordinating business resumption plans throughout the IRS, it has not provided clear guidance and direction to accomplish this throughout its own organization. Clear procedures to implement actions to resume the IRS' own business operations and support its critical computing and communications systems do not exist. To address this absence of direction, the Mission Assurance office is developing templates for ITS organization personnel to use in developing its respective business resumption plans. These templates are in a draft status, and the governance process for the plan development, approval, and maintenance is in development, as well.

The absence of guidance within the ITS organization in developing its own business resumption plans for recovering after a major incident could jeopardize its ability to timely support the IRS' critical computing and communications systems. As part of its mission, the IRS annually processes 230 million tax returns, collects \$2 trillion in taxes, issues 90 million individual refunds, and provides assistance to 120 million taxpayers.

³ Territory offices service taxpayers within a specified geographical area.

⁴ IRS computing centers support tax processing and information management through a data processing and telecommunications infrastructure.

Delays in restoring critical business processes would significantly affect the IRS' ability to deliver these customer services and effectively administer the tax administration system.

To improve the recovery from an incident or disaster affecting the IRS, we recommended that the Chief Information Officer (CIO) ensure the Mission Assurance office develops and provides the direction and guidance for the completion and implementation of adequate business resumption plans within the ITS organization. Additionally, we recommended that the CIO ensure that the Mission Assurance office acquires the technical expertise for developing, implementing, and reviewing the adequacy of the ITS organization's business resumption plans. This expertise will help ensure all applicable information and essential processes have been included in the business resumption plans and that the plans are appropriate for the ITS organization.

Management's Response: Management's response was due on September 26, 2003. As of September 26, 2003, management had not responded to the draft report.

The Treasury Inspector General for Tax Administration (TIGTA) has designated this report as Limited Official Use (LOU) pursuant to Treasury Directive TD P-71-10, Chapter III, Section 2, "Limited Official Use Information and Other Legends" of the Department of Treasury Security Manual. Because this document has been designated LOU, it may only be made available to those officials who have a need to know the information contained within this report in the performance of their official duties. This report must be safeguarded and protected from unauthorized disclosure; therefore, all requests for disclosure of this report must be referred to the Disclosure Section within the TIGTA's Office of Chief Counsel.

Please contact me at (202) 622-6510 if you have questions or Margaret E. Begg, Assistant Inspector General for Audit (Information Systems Programs), at (202) 622-8510.

**The Information Technology Services Organization Needs to Complete
Its Business Resumption Planning**

Table of Contents

Background	Page 1
Business Resumption Plans Are in Development Throughout the Information Technology Services Organization	Page 3
Guidance and Direction Are Needed to Complete Business Resumption Plans.....	Page 4
<u>Recommendation 1:</u>	Page 7
Completed Business Resumption Plans Can Be Improved.....	Page 7
<u>Recommendation 2:</u>	Page 9
Appendix I – Detailed Objective, Scope, and Methodology.....	Page 10
Appendix II – Major Contributors to This Report	Page 12
Appendix III – Report Distribution List	Page 13

The Information Technology Services Organization Needs to Complete Its Business Resumption Planning

Background

Business resumption is the process of re-opening an organization's components or business processes following a disaster. Business resumption planning is undertaken by organizations to provide employees with a documented set of actions to perform in the event of a disaster, enabling business processing to resume within critical time periods.

An effective business resumption plan is wholly dependent on a comprehensive disaster recovery plan, which should encompass issues such as failed hard drives and processors, data loss, data damage, viruses, external or internal attacks, and other affects upon the network and its entities. The disaster recovery plan generally outlines backup routines, offsite storage requirements, emergency boot disk preparation, etc. The business resumption plan deals with who will be responsible for restoring operations following a disaster, what they will do, and how, where, and when they will do it. Together, the business resumption and disaster recovery plans contribute to the business continuity program at the Internal Revenue Service (IRS).

The IRS has placed organizational responsibility for coordinating its business continuity efforts in the Mission Assurance office within the Information Technology Services (ITS) organization. We recently issued an audit report on business continuity in the IRS¹ and reported that there are disaster recovery and business resumption plans in place for the IRS submission processing sites,² and a plan was developed for use in restoring essential National Headquarters' functions following an incident or disaster. We recommended that the Chief Information Officer (CIO) clarify the business continuity responsibilities of the various IRS organizations, offices, and executives, including

¹ *The Internal Revenue Service Has Made Substantial Progress in Its Business Continuity Program, but Continued Efforts Are Needed* (Reference Number 2003-20-026, dated December 2002).

² Submission processing sites are responsible for processing tax returns and payments.

The Information Technology Services Organization Needs to Complete Its Business Resumption Planning

defining organizational expectations and roles, and updating the Internal Revenue Manual.³

The IRS' business continuity plan identifies the need to provide computing and communications resources to restore critical business functions. To accomplish this responsibility, the ITS organization should have a specific business resumption plan to timely resume its own operations following an emergency or disaster so it can support the IRS' critical business processes.

To assess the adequacy of the ITS organization's plans to resume its operations after an emergency or disaster, we reviewed the status of the plans for resumption of business activity to restore six critical IRS business system operations.⁴ Our reviews included assessments of the ITS organization's business resumption planning for these systems at the Martinsburg and Tennessee Computing Centers;⁵ the Atlanta and Memphis Submission Processing Sites; and the Laguna Niguel Territory Office.⁶ We also reviewed available documentation and interviewed IRS executives, managers, and analysts located at the IRS' National Headquarters and the New Carrollton Federal Building. We performed this audit from April through July 2003 in accordance with *Government Auditing Standards*. Detailed information on our objective, scope, and methodology is presented in Appendix I. Major contributors to the report are listed in Appendix II.

³ The Internal Revenue Manual is the single official IRS source of all policies, procedures, guidelines, and delegations of authority to administer the nation's tax laws.

⁴ See Appendix I for information on the six business systems operations we reviewed.

⁵ IRS computing centers support tax processing and information management through a data processing and telecommunications infrastructure.

⁶ Territory offices service taxpayers within a specified geographical area.

The Information Technology Services Organization Needs to Complete Its Business Resumption Planning

Business Resumption Plans Are in Development Throughout the Information Technology Services Organization

The ITS organization is completing business resumption plans to designate responsibilities and resources to support and restore the IRS' critical computing and communications systems. At the Atlanta and Memphis Submission Processing Sites, the ITS organization's End-User Equipment & Services function⁷ completed business resumption plans that included sufficient direction to support the resumption of the critical systems we selected for review. These plans included procedures to:

- Resume operations at an offsite location.
- Reassign ITS employees to replace injured employees.
- Acquire office equipment and supplies.
- Designate damage assessment teams.
- Notify other essential ITS offices and contractors.
- Update the employee contact information.

We also visited the End-User Equipment & Services function at the Laguna Niguel Territory Office and reviewed its business continuity plan. This office provides support for the resumption of the business operations at the IRS field offices within this territory to ensure uninterrupted access to the critical computing and communications systems. The Laguna Niguel Territory Office's business continuity plan included general procedures to resume operations at an offsite location, acquire office equipment and supplies, and update the employee contact information.

At the Tennessee Computing Center, an ITS branch office's draft business continuity plan included details for the business resumption activities of the Electronic Federal Tax Payment System. While this plan is still in draft, it detailed the various recovery tasks and priorities necessary to resume this critical system in the event of an incident. This plan further included the identification of teams to perform the

⁷ The End-User Equipment & Services function provides computer equipment and desktop support to IRS employees located at submission processing sites and field offices within its territory.

The Information Technology Services Organization Needs to Complete Its Business Resumption Planning

Guidance and Direction Are Needed to Complete Business Resumption Plans

various resumption tasks, and provided procedures to resume operations at an offsite location, reassign ITS employees to replace injured employees, acquire office equipment, designate a damage assessment team, and notify other essential ITS offices and contractors.

While the ITS organization has made progress in business resumption planning, business resumption plans were not completed for all branches at the two computing centers and the territory office we reviewed.

At the Tennessee Computing Center, the ITS organization had initiated, but not completed, business resumption plans for recovering the critical business systems we selected for review. The Tennessee Computing Center management official responsible for the recovery of the critical systems cited several reasons for not completing business resumption plans for its own operations, including:

- A reliance on another computing center as a back-up for the critical systems.
- An approach that business resumption planning at the computing centers was only for resuming processing for the business functions, and not relevant for the ITS organization to be able to resume its own operations.
- An implementation of the Enterprise Operations Services Triplex program that will allow for back-up processing at other computing centers with associated cross-training that could reduce the need for separate business resumption plans. However, the Enterprise Operations Services Director stated that this program is not ready for implementation in the short term and may not resolve business resumption planning needs. The Director also indicated that the Enterprise Operations Services has not provided the necessary emphasis for the business resumption planning process and must do more to encourage the development of business resumption plans for the computing centers.

The Information Technology Services Organization Needs to Complete Its Business Resumption Planning

At the Martinsburg Computing Center, the ITS organization had not prepared specific business resumption plans. The disaster recovery coordinator at the Martinsburg Computing Center stated that aspects of business resumption currently reside in the disaster recovery plans. Preparation of specific business resumption plans was awaiting approval of guidance from the Mission Assurance office.

At the Laguna Niguel Territory Office, the ITS business continuity plan did not include a separate business resumption plan section. Our review of the plan found that the recovery priorities (necessary for the ITS organization's End-User Equipment & Services function to resume its own business) were not included in this plan. Additionally, the plan did not include procedures to reassign ITS employees to replace injured employees, notify other essential ITS offices and contractors, designate a damage assessment team, or provide specific details to resume operations at an offsite location. The End-User Equipment & Services function staff stated that they were not aware of any guidance or efforts to add the business resumption activities to their business continuity plan.

The Security Services function has been tasked to work with the ITS organization and the IRS business units to identify existing and planned business resumption capabilities, including establishing executable business resumption plans. The Mission Assurance office, part of Security Services, is responsible for coordinating the IRS' business resumption efforts to ensure the IRS has the ability to quickly resume operations in the event of a disaster.

The Mission Assurance office has not provided clear guidance and direction to develop and implement business resumption plans in the ITS organization. Clear procedures to implement actions to resume its own business operations and support the IRS' critical computing and communications systems do not exist. To address this absence, the Mission Assurance office is developing templates for the ITS organization to follow in developing its respective business resumption plans. These templates are in a draft status, and the governance process for the plan

**Key Security Controls of the Currency and
Banking Retrieval System Have Not Been
Implemented**

September 2003

Reference Number: 2003-20-211



INSPECTOR GENERAL
for TAX
ADMINISTRATION

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

September 26, 2003

MEMORANDUM FOR COMMISSIONER, SMALL BUSINESS/SELF-EMPLOYED
DIVISION
CHIEF INFORMATION OFFICER

Gordon C. Milbourn III

FROM: Gordon C. Milbourn III
Assistant Inspector General for Audit (Small Business and
Corporate Programs)

SUBJECT: Final Audit Report - Key Security Controls of the Currency and
Banking Retrieval System Have Not Been Implemented
(Audit # 200320004)

This report presents the results of our review of the Currency and Banking Retrieval System (CBRS). The overall objective of this review was to determine whether appropriate security policies and procedures have been developed, effectively implemented, and tested to protect the CBRS from malicious intrusions and unauthorized access.

The CBRS is an online database that contains sensitive information on large cash and suspicious financial transactions reported under the Bank Secrecy Act (BSA).¹ The BSA requires financial institutions, trades or businesses, and other persons to report to the Federal Government a variety of financial transactions, such as bank deposits and withdrawals made in cash exceeding \$10,000. Approximately 13 million BSA reports are filed each year. This financial information is used by about 16 Federal Government agencies and over 75 state and local law enforcement agencies for examination, compliance, and enforcement efforts. The sensitivity of the data and the volume of accounts on the CBRS make it an attractive target for persons wanting to steal, manipulate, or destroy the information.

The Department of the Treasury's Financial Crimes Enforcement Network (FinCEN) is one of the key agencies responsible for establishing, overseeing, and implementing

¹ Pub. L. No. 91-508, 84 Stat. 1114 to 1124 (1970) (codified as amended in scattered sections of 12 U.S.C., 15 U.S.C., and 31 U.S.C.)

policies to prevent and detect money laundering. The FinCEN is also responsible for screening and granting access to non-Internal Revenue Service (IRS) users of the CBRS. The IRS Small Business/Self-Employed (SB/SE) Division is the business owner of the CBRS database and is ultimately responsible for the security controls of the CBRS. The Detroit Computing Center is responsible for the design, maintenance, and upgrading of the CBRS.

The IRS has developed adequate security policies and procedures to protect CBRS data. Policies and procedures have been effectively implemented for 6 of the 14 control topics we reviewed. However, management did not implement or test several key IRS policies and procedures pertaining to the other eight control topics. As a result, security of the CBRS is not adequate. Specifically, SB/SE Division management has not:

- Maintained up-to-date risk assessments and security plans.
- Recertified the CBRS after the authority to operate expired in February 2001.
- Devoted sufficient attention to limiting the number of persons with access to the CBRS.
- Ensured background investigations had been performed for those granted access.
- Ensured employees with key security responsibilities have been properly trained.
- Provided sufficient attention to technical access controls and audit trails.

We attribute management's noncompliance with IRS policies and procedures to inadequate concern about the security of the CBRS. We recognize that management must balance security needs with other operational concerns. However, due to the sensitive nature of the data maintained on the CBRS and the wide access given to the data, we believe that management did not give sufficient priority to the security of this system.

To improve security over the CBRS, we recommended actions that should be taken by the Commissioner, SB/SE Division, and the Chief Information Officer. The risk assessment, security plan, and certification should be updated. The practice of reviewing security controls annually needs to be implemented. Operational and technical controls must be improved to limit access to the CBRS to those employees who need it to conduct their jobs. All required information, including background information status, must be included on the authorization form before creating a CBRS user account. All employees with CBRS responsibilities should be provided sufficient training to stay informed of security issues. Management should also ensure that the purpose of any group granted access to the CBRS is well defined and that only those personnel with a need are assigned to a group. In addition, audit trails should be executed routinely to detect inappropriate activities.

Management's Response: The Commissioner, SB/SE Division, and the Chief Information Officer agreed with the recommendations in this report and stated that

corrective actions will be taken to assure that CBRS security is adequate. Corrective actions include completing the system certification process; implementing system-based security reviews; implementing a system users archive procedure, including all data download activity on audit trails; and reviewing for completeness all authorizations submitted to create user accounts and rejecting those that are incomplete. Actions will also include issuing a written document to the FinCEN outlining IRS and Department of the Treasury security directives that apply to the CBRS, ensuring that proper training is given to employees with mainframe security responsibilities, better defining access privileges of groups and ensuring that CBRS users are in the proper user groups, and establishing an action plan to create the proper audit trail reports and ensure that they are reviewed. Management's complete response to the draft report is included as Appendix IV.

The Treasury Inspector General for Tax Administration (TIGTA) has designated this report as Limited Official Use (LOU) pursuant to Treasury Directive TD P-71-10, Chapter III, Section 2, "Limited Official Use Information and Other Legends" of the Department of Treasury Security Manual. Because this document has been designated LOU, it may only be made available to those officials who have a need to know the information contained within this report in the performance of their official duties. This report must be safeguarded and protected from unauthorized disclosure; therefore, all requests for disclosure of this report must be referred to the Disclosure Section within the TIGTA's Office of Chief Counsel.

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

**Key Security Controls of the Currency and Banking Retrieval System
Have Not Been Implemented**

Table of Contents

Background.....	Page 1
Management Controls Were Not Kept Up to Date.....	Page 3
<u>Recommendation 1:</u>	Page 5
<u>Recommendation 2:</u>	Page 6
Two Critical Operational Controls Were Not Effectively Implemented	Page 6
<u>Recommendation 3:</u>	Page 10
<u>Recommendations 4 through 6:</u>	Page 11
<u>Recommendation 7:</u>	Page 12
Technical Operating System Controls Were Not Effective and Audit Trails Were Not Reviewed.....	Page 12
<u>Recommendations 8 through 10:</u>	Page 15
Appendix I – Detailed Objective, Scope, and Methodology	Page 16
Appendix II – Major Contributors to This Report	Page 17
Appendix III – Report Distribution List.....	Page 18
Appendix IV – Management’s Response to the Draft Report.....	Page 19

Key Security Controls of the Currency and Banking Retrieval System Have Not Been Implemented

Background

The Currency and Banking Retrieval System (CBRS) contains sensitive information on large cash and suspicious financial transactions reported under the Bank Secrecy Act (BSA).¹ The BSA requires financial institutions, trades or businesses, and other persons to report to the Federal Government a wide variety of financial transactions, such as bank deposits and withdrawals made in cash exceeding \$10,000. Each year approximately 13 million BSA reports are filed.

The CBRS is an online database that contains records of over 120 million BSA reports. The reports are kept in the CBRS for 10 years and then archived. The CBRS resides on a mainframe computer at the Internal Revenue Service's (IRS) Detroit Computing Center (DCC).

IRS field agents query the CBRS when performing work in the Examination, Collection, and Criminal Investigation functions. Federal, state, and local law enforcement agencies (e.g., Customs and Border Protection, Department of Justice, Drug Enforcement Administration) may also query the database for researching tax cases, tracking money-laundering activities, obtaining investigative leads, gathering intelligence for tracking currency flows, and corroborating information.

Certain regulatory agencies (e.g., the Federal Reserve System, Securities and Exchange Commission) also use the CBRS for general examination, compliance, and enforcement efforts. About 16 Federal Government agencies and over 75 state and local law enforcement agencies have direct access to the CBRS.

The Department of the Treasury's Financial Crimes Enforcement Network (FinCEN), one of the key agencies responsible for establishing, overseeing, and implementing policies to prevent and detect money laundering, is responsible for screening and granting access to non-IRS users of the CBRS. The IRS Small Business/Self-Employed

¹ Pub. L. No. 91-508, 84 Stat. 1114 to 1124 (1970) (codified as amended in scattered sections of 12 U.S.C., 15 U.S.C., and 31 U.S.C.)

Key Security Controls of the Currency and Banking Retrieval System Have Not Been Implemented

(SB/SE) Division² is the business owner of the CBRS and is ultimately responsible under the Federal Information Security Management Act (FISMA)³ for the security controls of the CBRS. The DCC, a part of the IRS Modernization, Information Technology and Security (MITS) Services organization,⁴ is responsible for the design, maintenance, and upgrading of the CBRS.

During this review, we assessed the security of the CBRS database. To accomplish this, we used the *Security Self-Assessment Guide for Information Technology Systems* (Special Publication 800-26) prepared by the National Institute of Standards and Technology (NIST). This document builds on the *Federal Information Technology Security Assessment Framework* developed by the NIST for the Federal Chief Information Officer (CIO) Council.

The NIST Guide addresses 17 security control topics that focus on management, operational, and technical controls. In addition, the Guide provides control objectives and techniques that can be measured for each control topic. To measure the progress of the implementation for the needed security control, the NIST Guide provides five levels of effectiveness for each answer to a security control question:

- Level 1 – control objective is documented in a security policy.
- Level 2 – security controls are documented as procedures.
- Level 3 – procedures have been implemented.
- Level 4 – procedures and security controls are tested and reviewed.

² The SB/SE Division serves the needs of businesses with assets of \$10 million or less. It provides education, assistance, return processing, and compliance services for these customers.

³ The FISMA is part of the E-Government Act of 2002, Pub. L. No. 107-347, Title III, Section 301, 2002.

⁴ The MITS Services organization meets the information technology needs of the IRS by delivering information technology systems, products, services, and support.

Key Security Controls of the Currency and Banking Retrieval System Have Not Been Implemented

- Level 5 – procedures and security controls are fully integrated into a comprehensive program.

We did not review 3 of the 17 control topics contained in the NIST Guide. The three topics (life cycle, physical security, and incident response capability) either do not apply to operational systems or have been extensively covered in other Treasury Inspector General for Tax Administration (TIGTA) audits.

The audit was performed from January to April 2003 in the DCC and the FinCEN Headquarters in Washington, D.C. The audit was conducted in accordance with *Government Auditing Standards*. Detailed information on our audit objective, scope, and methodology is presented in Appendix I. Major contributors to the report are listed in Appendix II.

Management Controls Were Not Kept Up to Date

The IRS has developed adequate security policies and procedures to protect CBRS data. However, policies and procedures had not been effectively implemented for 8 of the 14 control topics we reviewed. The SB/SE Division also had not kept management controls up to date and had not implemented two critical operational controls. In addition, MITS Services had not ensured that technical access controls were effective and had not ensured that audit trails were reviewed. As a result, we concluded that security of the CBRS is not adequate.

Management controls are needed to ensure that appropriate security procedures are implemented to reduce the risks associated with a system. Functional managers charged with maintaining the system are responsible for these controls, which consist of four topics applicable to the CBRS: risk management, review of security controls, certification and accreditation, and system security plan.⁵

The SB/SE Division did not follow IRS policies and procedures for these topics. By not complying with the following procedures, management can have little

⁵ Controls in a fifth topic – life cycle – were either not applicable or duplicated in other control topics.

Key Security Controls of the Currency and Banking Retrieval System Have Not Been Implemented

confidence that the CBRS security controls are commensurate with the risks inherent in this system.

We attribute the noncompliance to inadequate concern about the security of the CBRS. We recognize that management must balance security needs with other operational concerns. However, due to the sensitive nature of the data maintained on the CBRS and the wide access given to the data, we believe that management did not give CBRS security sufficient priority.

Risk Management – A risk assessment is the process used for identifying threats and vulnerabilities of a system and the potential impact that a loss of information or the capabilities of the system would have on the agency. It is used as a basis for identifying and selecting appropriate and cost-effective measures for reducing or accepting risks.

The IRS is required to conduct risk assessments for its sensitive systems at least every 3 years, and it must review the risk assessments annually. The last CBRS risk assessment was conducted in May 2001, almost 4 years after the previous risk assessment. SB/SE Division management had not reviewed the risk assessment annually, as required, to ensure it was still valid. When risk assessments are delayed, security threats and vulnerabilities might not be identified timely, and additional controls to reduce these threats and vulnerabilities might not be timely devised and implemented.

Review of Security Controls – The FISMA requires that functional managers perform security reviews at least annually for each of the major systems that support their operations. The extent of such reviews can vary depending on risk and the scope of prior reviews. Without periodic reviews and tests, the IRS may not have adequate assurance that security controls are functioning effectively and providing an adequate level of protection.

The CBRS security controls were last reviewed as part of the May 2001 risk assessment. Prior to the 2001 assessment, the last security review was performed in 1997. At the time of our review, SB/SE Division management still

Key Security Controls of the Currency and Banking Retrieval System Have Not Been Implemented

had not taken action to address any of the security weaknesses identified in its May 2001 review. In addition, SB/SE Division management had not reviewed the FinCEN's controls for granting access to the CBRS for non-IRS users.

Certification and Accreditation – Certification is a technical evaluation of an information system to determine how well it meets security requirements, including all applicable Federal laws, policies, regulations, and standards. The certification process is the final step leading to system accreditation, which is the written authorization for a system to operate. All major applications and general support systems must be recertified and reaccredited at least every 3 years, or sooner if major system changes affect the security safeguards.

The CBRS' certification and authority to operate expired on February 28, 2001. Significant documentation required to recertify the CBRS was prepared in 2001 but has not yet been approved.

Security Plan – A security plan should provide an overview of the security requirements of the system and describe the controls in place or planned for meeting those requirements. The plan should delineate responsibilities and expected behavior of all individuals who access the system. The security plan should be reviewed periodically and updated to reflect current conditions and risks.

The last security plan was completed in May 2001, as part of the ongoing certification and accreditation process. However, it has yet to be approved and signed by management.

Recommendations

The Commissioner, SB/SE Division, should:

1. Take immediate steps to review, update, and approve the CBRS risk assessment and security plan and complete the certification process.

**The Offshore Credit Card Project Shows
Promise, but Improvements Are Needed to
Ensure That Compliance Objectives Are
Achieved**

August 2003

Reference Number: 2003-30-160



INSPECTOR GENERAL
for TAX
ADMINISTRATION

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

August 15, 2003

MEMORANDUM FOR COMMISSIONER, SMALL BUSINESS/SELF-EMPLOYED
DIVISION

Gordon C. Milbourn

FROM: Gordon C. Milbourn III
Assistant Inspector General for Audit (Small Business and
Corporate Programs)

SUBJECT: Final Audit Report - The Offshore Credit Card Project Shows
Promise, but Improvements Are Needed to Ensure That
Compliance Objectives Are Achieved (Audit # 200230056)

This report presents the results of our review to determine whether the Internal Revenue Service (IRS) had implemented an effective project to combat abusive offshore credit card accounts. Our overall objective was to determine how effective the Offshore Credit Card Project (OCCP) is in identifying abusive schemes using offshore credit cards and the actions taken to ensure future taxpayer compliance.

In our opinion, the OCCP reflects an innovative approach to combat tax-evasion schemes involving offshore credit card accounts. This approach complements the IRS' compliance strategy of focusing its resources on the high-risk areas of noncompliance. The OCCP uses the records from John Doe summonses¹ and merchant summonses² to trace the identities of credit card holders that may be hiding taxable income in an offshore bank account.

While the OCCP shows promise, improvements are needed to ensure fairness to all taxpayers, effective use of resources, and the availability of information to manage the Project. First, the OCCP had not established formal guidelines for assessing the

¹ A John Doe summons is any summons that does not identify the person with respect to whose liability the summons is issued. A John Doe summons can be issued only after approval by a Federal court.

² Referred to as "second level" John Doe summonses.

accuracy-related penalty. Without such guidelines, the IRS cannot ensure that the tax law is applied consistently and fairly for all taxpayers.

The second improvement area concerns the effective use of resources. The IRS may be examining returns beyond the assessment statute date for OCCP taxpayers even though most cases may not meet the Internal Revenue Code (I.R.C.)³ criteria for extending the statute. The effect of this decision is that unless fraud or a substantial understatement of gross income is proven, or the taxpayer did not file a tax return or information document, no assessments of tax can be made.

Finally, the IRS does not have an effective management information system to give management sufficient data with which to make decisions in combating abusive offshore credit card accounts. For example, there is no management information system that captures specific data regarding completed examinations of U.S. Individual Income Tax Returns (Form 1040) based on OCCP issues, including penalty assessments or costs of the Project. The existing IRS systems do not provide complete or timely information to assist management in controlling the Project, measuring noncompliance, enhancing the classification process, targeting training areas, controlling referrals to other enforcement functions, and targeting taxpayer education.

We recommended that the IRS provide formal guidance and training, and review OCCP cases to ensure consistent application of the accuracy-related penalty. The IRS should also ensure that OCCP resources are not expended on cases that result in barred assessments. To ensure compliance with provisions of the I.R.C., the IRS should request that the Office of Chief Counsel formally review the memorandum that provided guidance on allowing the examination of tax returns after the assessment statute date to determine its compliance with provisions of the I.R.C.⁴ Finally, the IRS should develop a system to quantify the specific results of OCCP cases at key points in the examination process and to identify patterns and trends.

Management's Response: Management agreed with some of our recommendations and stated that they have already completed some corrective actions. Specifically, management issued a written alert to their field offices reminding revenue agents to always consider the accuracy-related penalty. Management includes the application of penalties as part of the case review process, and if management determines that the need to further address this issue exists, a training module for future OCCP training classes may be developed.

Also, management conducted and documented a national review of in-process OCCP cases and will include this type of case in the Examination Quality Measurement System. Further, management is working with the Small Business/Self-Employed (SB/SE) Division's Office of Research in identifying trends that will result in the

³ I.R.C. §§ 6501(c)(1) and 6501(e) (2001).

⁴ I.R.C. § 6110 (2001).

development of cases, and management is capturing and analyzing data to identify patterns and trends in closed OCCP cases.

However, management did not agree with our second recommendation for ensuring resources are not expended on OCCP cases that may result in barred assessments. Management stated that revenue agents are instructed to consider the various scenarios for assessment statute extensions on each examination, specifically the provisions of I.R.C. § 6501. The written guidance provided to the field requires review and concurrence through the Territory Manager level in order to continue an examination past the assessment statute date. Management also stated that the closed cases available during our review would not be indicative of future cases, and to apply the rate of cases not meeting the I.R.C. statute extension criteria to the open inventory may not be reliable and would not affect a significant number of OCCP cases.

Also, management did not agree with our recommendation that the Office of Chief Counsel formally review the "Office of Compliance Policy's Statute of Limitations Management Memorandum" to determine its compliance with provisions of I.R.C. § 6110. Management stated that such a review is unnecessary because the memorandum reflected a business decision and not a legal determination from the Office of Chief Counsel. Management's complete response to the draft report is included as Appendix IV.

Office of Audit Comment: We agree that the corrective action of issuing a written alert to the SB/SE Division field offices is a good first step; however, we believe it is not as effective as incorporating the accuracy-related penalty into formal guidance documents as it appears in other abusive scheme program guidance. The significantly low rate of assessing the accuracy-related penalty on OCCP cases suggests that the penalty may not be considered in most cases. The portion of our recommendation concerning including the penalty assessment consideration in the review process has been sufficiently addressed. However, we believe that the OCCP training should immediately incorporate accuracy-related penalty assessments into the curriculum since management's response does not clearly indicate how the IRS will determine there is a need.

While we support the IRS' efforts to combat abusive offshore schemes beyond the statute when warranted, we are concerned that the IRS is at increased risk of the assessment being barred because the statute has expired. The OCCP open cases pertaining to Tax Years (TY) 1999 and prior accounted for over 36 percent of the open cases in field inventory at the time of our review. As we reported, less than 20 percent of the closed OCCP cases met the extended statute criteria of the I.R.C. We are concerned that management does not have the data to support their assertion that this issue will not affect a significant number of cases. Therefore, we believe that many of the open TY 1999 OCCP cases assigned to the field may not ultimately meet the I.R.C. criteria, resulting in inefficient use of resources. Further, the records from the March and August 2002 John Doe summonses have not yet been received. Depending upon time spent on taxpayer identification, case building, issuing formal document requests,

serving secondary summonses, and interviewing witnesses, the risk of barred assessments will continue to be an issue.

The purpose of our third recommendation was to have the Office of Chief Counsel make the determination as to whether this guidance is communicating a "business decision" or providing guidance on a significant tax issue that should be in compliance with the provisions of I.R.C. § 6110. Based on the importance of the OCCP in combating abusive offshore credit card accounts, we believe that examining tax returns after the assessment statute expiration date for a class of taxpayers is a significant tax issue and not merely a business decision. We still believe that the formal advice of the Chief Counsel is warranted to determine if the guidance on this tax issue is subject to provisions of I.R.C. § 6110.

We recognize that the IRS had taken some actions during and subsequent to the audit. However, the corrective action regarding the management information system is not sufficiently comprehensive to provide for the quantification of the project results and costing data. Without sufficient information, the IRS will have difficulty in determining its progress in combating abusive offshore credit card accounts. While we still believe our recommendations are worthwhile, we do not intend to elevate our disagreement concerning them to the Department of the Treasury for resolution.

The Treasury Inspector General for Tax Administration (TIGTA) has designated this report as Limited Official Use (LOU) pursuant to Treasury Directive TD P-71-10, Chapter III, Section 2, "Limited Official Use Information and Other Legends" of the Department of Treasury Security Manual. Because this document has been designated LOU, it may only be made available to those officials who have a need to know the information contained within this report in the performance of their official duties. This report must be safeguarded and protected from unauthorized disclosure; therefore, all requests for disclosure of this report must be referred to the Disclosure Section within the TIGTA's Office of Chief Counsel.

Please contact me at (202) 622-6510 if you have questions or Parker F. Pearson, Director (Small Business Compliance), at (410) 962-9637.

**The Offshore Credit Card Project Shows Promise, but Improvements Are Needed
to Ensure That Compliance Objectives Are Achieved**

Table of Contents

Background	Page 1
The Offshore Credit Card Project Is Taking an Innovative Approach in Combating Abusive Schemes Using Offshore Credit Card Accounts	Page 2
Consistency Is Needed in Assessing Penalties	Page 4
<u>Recommendation 1:</u>	Page 6
Potential Statute Expiration May Have an Adverse Impact on Resource Allocation	Page 7
<u>Recommendation 2:</u>	Page 10
<u>Recommendation 3:</u>	Page 11
A Management Information System Is Needed to Capture Results of Offshore Credit Card Project Cases to Assist in Ensuring Compliance Objectives Are Achieved	Page 11
<u>Recommendation 4:</u>	Page 13
<u>Recommendation 5:</u>	Page 14
Appendix I – Detailed Objective, Scope, and Methodology	Page 15
Appendix II – Major Contributors to This Report	Page 16
Appendix III – Report Distribution List	Page 17
Appendix IV – Management’s Response to the Draft Report	Page 18

The Offshore Credit Card Project Shows Promise, but Improvements Are Needed to Ensure That Compliance Objectives Are Achieved

Background

Congressional witnesses have estimated that 1 to 2 million taxpayers avoid \$40 to \$70 billion in taxes annually using offshore bank accounts.¹ The term “offshore” is generally used to mean a jurisdiction that offers financial secrecy laws and tax benefits in an effort to attract investments from outside its borders. To combat these abusive schemes, the Small Business/Self-Employed (SB/SE) Division initiated the Offshore Credit Card Project (OCCP) as a strategic priority for Fiscal Years (FY) 2003-2004. The SB/SE Division made a significant commitment of over 600 direct Compliance staff years² for this initiative.

In testimony before the Congress,³ the Internal Revenue Service (IRS) Commissioner described abusive schemes using offshore bank accounts as causing the largest revenue loss to the Department of the Treasury, being the hardest to detect, and undermining the fairness of the tax system. The IRS Commissioner has said that “diversion of income to offshore tax havens with strict bank secrecy laws represent [sic] a significant area of noncompliance with tax laws.”

Offshore credit cards are an easy and covert way for a taxpayer to access offshore funds. Generally, behind each offshore credit card are at least two foreign (offshore) bank accounts:

- An escrow account equal to 100 percent to 200 percent of the credit line extended.
- An account used to pay charges to the offshore credit card account.

There are valid and legal purposes for offshore bank accounts; however, some people are using them to evade taxes. Debit and credit cards have allowed offshore bankers

¹ Testimony before the U.S. Senate Finance Committee during the hearing on the nomination of Pamela F. Olson, Assistant Secretary for Tax Policy, August 1, 2002.

² A direct compliance staff year is 2,000 hours and costs approximately \$94,000. Therefore, the labor cost allocated for the initiative is over \$57 million (609 staff years x \$94,000).

³ Testimony of the Internal Revenue Service Commissioner before the U.S. Senate Finance Committee, April 11, 2002.

The Offshore Credit Card Project Shows Promise, but Improvements Are Needed to Ensure That Compliance Objectives Are Achieved

to offer easy and instantaneous access to offshore accounts without any paper trail.

Promoters openly market offshore schemes to the general public at seminars and over the Internet for fees that sometimes exceed \$3,000. The promoters include banks, accountants, trustees, lawyers, software companies, and tax haven country government officials.

We performed this audit at the SB/SE Division Headquarters Office in New Carrollton, Maryland, and visited the SB/SE Division Compliance Office in Mays Landing, New Jersey, and the Philadelphia Compliance Site in Philadelphia, Pennsylvania, from October 2002 to April 2003. The audit was conducted in accordance with *Government Auditing Standards*. Detailed information on our audit objective, scope, and methodology is presented in Appendix I. Major contributors to the report are listed in Appendix II.

The Offshore Credit Card Project Is Taking an Innovative Approach in Combating Abusive Schemes Using Offshore Credit Card Accounts

In our opinion, the OCCP reflects an innovative approach to combat tax-evasion schemes that use offshore credit card accounts. This approach aligns itself with the IRS' compliance strategy of focusing its resources on high-risk areas of noncompliance.

The IRS approach is multifaceted and includes coordinating Compliance activities with media coverage and the Criminal Investigation function to heighten taxpayer awareness. In summary, the IRS obtains cardholder and merchant credit card records to identify the taxpayer, builds cases for assignment to the Compliance field function, generates media coverage, and refers promoters for criminal investigation.

Compliance activities

In October 2000 and March and August 2002, the IRS petitioned a Federal court for authority to serve John Doe summonses⁴ on 2 major credit card companies for the

⁴ A John Doe summons is any summons that does not identify the person with respect to whose liability the summons is issued. A John Doe summons can be issued only after approval by a Federal court.

The Offshore Credit Card Project Shows Promise, but Improvements Are Needed to Ensure That Compliance Objectives Are Achieved

records of foreign bank accounts in more than 30 countries. The cardholder records obtained from the credit card companies did not include cardholder identifiers such as name or Social Security Number.

In addition to the cardholder records from the John Doe summonses, while building OCCP cases the IRS issued merchant summonses⁵ for charge card transactions, which helped identify specific taxpayers. At the time we completed our audit, the OCCP had not yet obtained the records requested in the March and August 2002 John Doe summonses.

Once the taxpayers' identities are established, examination techniques are used to determine whether a compliance issue exists. In July 2001, the IRS obtained 1.7 million records that included over 235,200 credit card numbers from the October 2000 John Doe summons. The IRS Compliance function then initiated examinations in May 2002. At the time of our review, the OCCP had developed over 2,100 cases. More than 1,740 of these cases were assigned to the IRS Compliance field function; the remaining cases were awaiting classification.

The IRS resources devoted to combating abusive tax schemes and scams (including the OCCP) significantly increased from FYs 2002 to 2003. In FY 2003, the Field Examination Plan included 609 direct staff years for the OCCP. In addition, the Plan included 396 direct staff years for other types of abusive schemes that include offshore activity.

Media coverage

Related to the OCCP, the IRS publicized the Offshore Voluntary Compliance Initiative (OVCI).⁶ The OVCI provides relief from certain penalties if taxpayers come forward and make a voluntary disclosure of their offshore activity. However, taxpayers will still have to pay taxes on unreported income, interest, and certain accuracy or

⁵ Referred to as "second level" John Doe summons.

⁶ Revenue Procedure 2003-11 (January 14, 2003).

The Offshore Credit Card Project Shows Promise, but Improvements Are Needed to Ensure That Compliance Objectives Are Achieved

delinquency penalties. Results of this initiative were still pending at the time we completed our audit.

Promoter investigation activities

To address the offshore credit card promoters, the OCCP refers information on promoters to the SB/SE Division Compliance Reporting function where promoter information on abusive schemes is collected and investigated.

Promoters lure both suspecting and unsuspecting taxpayers with the promise of lucrative tax benefits. The identification of promoters is another key to combating offshore tax evasion because gaining access to a promoter's list of investors can save the IRS resources.

While the OCCP shows promise, the IRS needs to make improvements. The improvements are needed to ensure fairness to all taxpayers, effective use of resources, and the availability of information to manage the Project.

Consistency Is Needed in Assessing Penalties

One of the IRS' Strategic Goals is to ensure that the tax law is applied fairly and uniformly to all taxpayers. The Internal Revenue Code (I.R.C.)⁷ provides for certain penalties that the IRS uses to ensure the fairness of the tax system by penalizing the noncompliant taxpayer. The IRS policy on penalty administration requires "...a penalty system that is designed to ensure consistency and accuracy of results in light of the facts of the law."

Properly and judiciously used, penalties promote voluntary compliance. The I.R.C.⁸ provides that the accuracy-related penalty be computed on the tax underpayment attributable to negligence. If a tax underpayment is attributable to a taxpayer's participation in an abusive offshore scheme and there is negligence, the revenue agent must develop the accuracy-related penalty issue. Figure 1 shows a hypothetical example of the penalties on underpayments attributable to negligence.

⁷ I.R.C. § 6662 (2001).

⁸ I.R.C. § 6662(a) (2001).

TDP 15-71

**Computer Security Vulnerabilities Vary
Among Internal Revenue Service Offices**

October 2002

Reference Number: 2003-20-019

TDP 15-71



INSPECTOR GENERAL
for TAX
ADMINISTRATION

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

October 30, 2002

MEMORANDUM FOR DEPUTY COMMISSIONER FOR MODERNIZATION &
CHIEF INFORMATION OFFICER

Pamela J. Gardiner

FROM: Pamela J. Gardiner
Acting Inspector General

SUBJECT: Final Audit Report – Computer Security Vulnerabilities Vary
Among Internal Revenue Service Offices (Audit # 200220025)

This report presents the results of our review of the effectiveness and consistency of selected computer security controls in Internal Revenue Service (IRS) field offices. In each office, we determined whether selected SANS/FBI Top Twenty vulnerabilities¹ existed. We also tested for additional vulnerabilities suggested by our contractor.² These vulnerabilities are widely known in the cyber-security industry and to hackers.

In summary, computer security controls were not implemented effectively in most of the offices we visited, and a wide range in the number of vulnerabilities existed between offices. The vulnerabilities identified could be exploited by disgruntled employees and by hackers to access data, change data, or to obtain information for a denial of service attack.³

For example, some offices installed operating systems using default settings that are well known by hackers instead of modifying the settings. A default installation would allow an anonymous user with no password to obtain a listing of user account names. Some accounts did not have a user profile which is needed to restrict access for each user. Another illustration of a potential vulnerability included accounts with passwords

¹ The SANS/FBI Top Twenty list, released on October 1, 2001, shows common security flaws that account for a majority of successful attacks. This list expands on last year's list, "Ten Most Critical Internet Security Vulnerabilities," which was released by SANS and the National Infrastructure Protection Center (NIPC). See <http://www.sans.org> for additional information.

² See Appendix IV for a general listing of vulnerabilities by category.

³ A denial of service attack occurs when an intruder takes over the resources of a system to limit access of legitimate users to the system.

that were marked "never expire" or "cannot change." Over time, the chances for disclosure or abuse of a permanent password are high.

Of the six offices we tested, San Francisco and Oakland had a higher rate of vulnerabilities for both Windows NT servers and workstations. The New Carrollton Federal Building and Atlanta had lower rates of vulnerabilities for both servers and workstations. The other offices had mixed results. Vulnerabilities were identified and recommended corrective actions were provided by the commercial software reports. Test results were provided to local IRS managers in each of the offices we visited for assessment and appropriate corrective action.

Systems administrators have the responsibility for ensuring the proper protection of system software. We contacted systems administrators for each of the offices visited to identify some of the possible causes for not implementing security controls effectively and consistently. A variety of reasons were provided including operational demands, budgetary constraints, lack of resources, and equipment being replaced or relocated.

Of particular importance, however, was the lack of computer security training. As of May 2002, none of the six systems administrators we contacted had received any security training within this calendar year, and five had not received any security training in the prior calendar year. Also, existing IRS guidance covering system administrator responsibilities does not explicitly state what responsibility they have in regard to patching software. This lack of guidance could lessen the accountability and responsibility for ensuring that IRS systems are properly protected and maintained.

We recommend that systems administrators responsible for the equipment in the offices we tested be given security training tailored to mitigating vulnerabilities identified in the SANS/FBI Top Twenty list. An assessment of whether adequate security training has been provided to systems administrators in other offices should also be considered.

Management's Response: The Chief, Security Services, concurred with our recommendation and indicated that activities are underway to identify, define, and develop security training within the next 18 months, barring any shift of resources. Management's complete response to the draft report is included as Appendix V.

The Treasury Inspector General for Tax Administration (TIGTA) has designated this report as Limited Official Use (LOU) pursuant to Treasury Directive TD P-71-10, Chapter III, Section 2, "Limited Official Use Information and Other Legends" of the Department of Treasury Security Manual. Because this document has been designated Limited Official Use, it may only be made available to those officials who have a need to know the information contained within this report in the performance of their official duties. This report must be safeguarded and protected from unauthorized disclosure; therefore, all requests for disclosure of this report must be referred to the Disclosure Unit within the TIGTA's Office of Chief Counsel.

Copies of this report are also being sent to the IRS managers who are affected by the report recommendation. Please contact me at (202) 622-6510 if you have questions or

Scott E. Wilson, Assistant Inspector General for Audit (Information Systems Programs),
at (202) 622-8510.

Computer Security Vulnerabilities Vary Among
Internal Revenue Service Offices

Table of Contents

Background	Page 1
Security Controls Were Not Implemented Effectively and Consistently....	Page 1
<u>Recommendation 1</u>	Page 7
Appendix I – Detailed Objective, Scope, and Methodology	Page 8
Appendix II – Major Contributors to This Report	Page 10
Appendix III – Report Distribution List	Page 11
Appendix IV – Categories of Vulnerabilities	Page 12
Appendix V – Management’s Response to the Draft Report	Page 14

Computer Security Vulnerabilities Vary Among Internal Revenue Service Offices

Background

The Internal Revenue Service's (IRS) network is an outgrowth of a large number of local area networks developed and installed by data communication technicians and architects from various offices located throughout the country. Ensuring that security controls are implemented effectively and consistently in a widely dispersed organization like the IRS is clearly a challenge.

Systems administrators are charged with the responsibility to ensure proper protection and use of system software. The End User Equipment and Service Group, the Domain Infrastructure Networking Group, and the Office of Mission Assurance also share responsibility for providing guidance, testing, and implementation.

We performed this audit to meet the requirements of the IRS Restructuring and Reform Act of 1998,¹ which requires the Treasury Inspector General for Tax Administration (TIGTA) to annually assess the security of IRS technology. The audit work was performed from January through August 2002. We conducted our network vulnerability tests in Atlanta, Georgia (Summit Building); Newark, New Jersey (Broad Street); Lanham, Maryland (New Carrollton Federal Building); Philadelphia, Pennsylvania (Arch Street); and San Francisco, California (Golden Gate Avenue).

This audit was performed in accordance with *Government Auditing Standards*. Detailed information on our audit objective, scope, and methodology is presented in Appendix I. Major contributors to the report are listed in Appendix II.

Security Controls Were Not Implemented Effectively and Consistently

Computer security controls were not implemented effectively in most of the offices we visited, and a wide range in the number of vulnerabilities existed between offices. The vulnerabilities identified could be exploited to

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

Computer Security Vulnerabilities Vary Among Internal Revenue Service Offices

access data, change data, or to obtain information for use in a denial of service attack.²

For example, some offices installed operating systems using default settings that are well known by hackers instead of modifying the settings. A default installation would allow an anonymous user without a password to obtain a listing of user account names.

Some accounts did not have a user profile. User profiles provide security on network systems because they are designed to restrict access for each user. Guest accounts were usually disabled, but two instances were found where the Guest account was enabled. This would provide an intruder who logged in as Guest to have expanded access to the network.

Another illustration of a potential vulnerability included accounts with passwords that were marked "never expire" or "cannot change." Over a period of time, the chances for disclosure or abuse of a permanent password are high. A complete list of the vulnerability categories for which we tested is included in Appendix IV.

The vulnerabilities identified are exploitable from within the IRS' network. Many security experts view insider threats as the most dangerous and hardest to detect.³ The most devastating threats to security have come from individuals who were deemed trusted insiders. Additionally, should perimeter controls such as firewalls and intrusion detection systems be breached, an external hacker could take advantage of the same vulnerabilities.

We provided each office we visited the results generated by our software (Internet Security Systems (ISS)™ Internet Scanner) for assessment and corrective action as appropriate. The results included the identification and description of vulnerabilities and recommended corrective

² A denial of service attack occurs when an intruder takes over the resources of a system to limit access of legitimate users to the system.

³ For a discussion of the insider threat see the Texas A&M Research Foundation's web site at: <http://rf-web.tamu.edu/files/SECGUIDE/V1comput/Threats.htm#Threats>

Computer Security Vulnerabilities Vary Among Internal Revenue Service Offices

actions for identified vulnerabilities. Table 1 below represents the number of vulnerabilities identified by office and type of computer.⁴

Table 1. Number of Vulnerabilities by Office and Device Type

Office Location	Windows NT Servers	Windows NT Work-Stations	Unix Servers	Unix Work-stations	Routers	Web Servers
Atlanta, GA	7	55	7	N/A	1	N/A
Newark, NJ (Including Springfield)	51	19	N/A	N/A	N/A	N/A
Lanham, MD	12	21	N/A	N/A	1	8
Oakland, CA	30	45	8	7	1	11
Philadelphia, PA	25	97	7	N/A	1	3
San Francisco, CA	45	57	7	7	N/A	N/A

Prepared by: TIGTA, May 2002

N/A= Not Applicable

Approximately 87 percent of all vulnerabilities found by office are from Windows NT workstations (55 percent) and Windows NT servers (32 percent). The remaining 13 percent represent vulnerabilities in Unix-based systems, routers, and web servers. The vulnerabilities we identified were not isolated to any particular computer in the offices we visited.

The types and numbers of vulnerabilities varied widely among the offices tested

We found a wide range of vulnerabilities among the offices visited. Table 2 shows that the average number of vulnerabilities identified per Windows NT workstation ranged from 1.27 to 7.13. Table 3 shows the average number of vulnerabilities per Windows NT server varied from 1.00 to 9.00. Vulnerabilities per scan for Tables 2 and 3 were determined by dividing the number of vulnerabilities

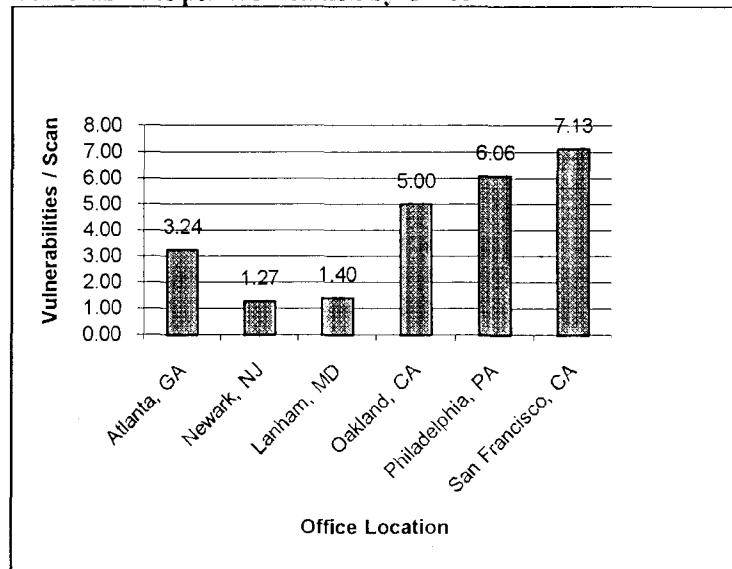
⁴ See Appendix I, Table 1 for the number of devices and types tested by location.

Computer Security Vulnerabilities Vary Among Internal Revenue Service Offices

shown in Table 1 by the number of like computers scanned shown in Appendix I.

Table 2 shows the average number of vulnerabilities for each Windows NT workstation by office location.

Table 2. Windows NT Workstations: Distribution of Unique Vulnerabilities per Workstation by Office

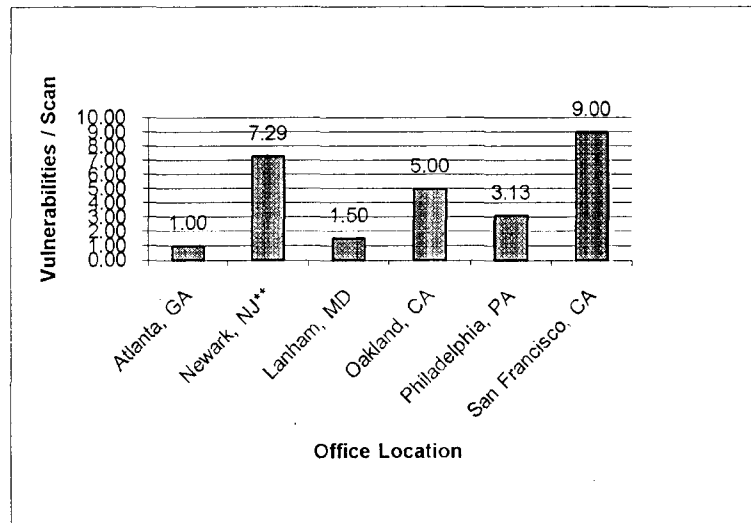


Source: TIGTA

Table 3 shows the average number of vulnerabilities for each Windows NT server by office location.

Computer Security Vulnerabilities Vary Among Internal Revenue Service Offices

Table 3. Windows NT Servers: Distribution of Unique Vulnerabilities per Server by Office



Source: TIGTA

**Servers located in Springfield, NJ

San Francisco and Oakland had a higher rate of vulnerabilities for both Windows NT servers and workstations. The New Carrollton Federal Building and Atlanta had lower rates of vulnerabilities for both servers and workstations. We attribute Atlanta's and New Carrollton's lower results to vigilant management practices. The other offices had mixed results.

The low vulnerabilities per scan for Newark Windows NT workstations can be explained because 7 of the 15 workstations tested had been updated with standard software known in the IRS as the Common Operating Environment (COE). Workstations updated with the COE had fewer vulnerabilities, which reduced the average number of vulnerabilities found per machine by office. The COE provides a means for the IRS to standardize its operating system and the various software applications on its workstations. The IRS plans to install the COE on over 100,000 workstations by 2004.

**Management Oversight of the Acceptance
Agent Program Is Needed to Assure that
Individual Taxpayer Identification Numbers
Are Properly Issued**

November 2002

Reference Number: 2003-30-020



INSPECTOR GENERAL
for TAX
ADMINISTRATION

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

November 6, 2002

MEMORANDUM FOR COMMISSIONER, LARGE AND MID-SIZE BUSINESS
DIVISION

Gordon C. Milbourn

FROM: Gordon C. Milbourn III
Acting Deputy Inspector General for Audit

SUBJECT: Final Audit Report - Management Oversight of the Acceptance Agent Program Is Needed to Assure that Individual Taxpayer Identification Numbers Are Properly Issued (Audit #200230026)

This report presents the results of our review to determine whether the Internal Revenue Service (IRS) ensures that acceptance agents¹ are complying with provisions of the Memorandum of Understanding (MOU) with the IRS for certifying the IRS' Individual Taxpayer Identification Number (ITIN) applications.

Foreign individuals are required to furnish either a Social Security Number (SSN) or an ITIN on tax returns filed after December 31, 1996. To carry out its ITIN-related responsibilities, the IRS established the Acceptance Agent Program (AAP). The IRS allows ITIN applicants to use approved acceptance agents to assist in completing the applications and reviewing the necessary documentation. An acceptance agent can be a United States or foreign individual/entity. An effectively administered AAP takes on increased importance with the national security risks now present in the United States. Because of these risks, the IRS has formed a task force to study the overall ITIN process.

In summary, the IRS has not provided an organizational commitment to the AAP to reasonably assure that expectations are established and achieved. In fact, the IRS has not determined the operating division that will be responsible for the overall ITIN process. Currently, the Large and Mid-Size Business Division has functional responsibility for managing the AAP. However, the Small Business/Self-Employed Division oversees the ITIN process, while the Wage and Investment Division processes the ITIN applications.

¹ Internal Revenue Procedure 96-52 (November 1996) provides for acceptance agents and certifying acceptance agents. Currently, the IRS uses only certifying acceptance agents.

The IRS needs to improve management controls and information to effectively manage the AAP. Since the inception of the AAP, the IRS has not performed any objective compliance reviews of the documentation maintained by the acceptance agents. IRS officials advised that they had neither sufficient management information on the number of applications certified by each agent, nor the necessary resources to properly assess the acceptance agent's compliance with documentation requirements.

Further, the IRS does not have sufficient management information concerning the characteristics of the ITIN documents submitted by acceptance agents. Consequently, the IRS has not determined whether the AAP is functioning as intended.

We recommended that the IRS ensure that the ITIN task force suggests the organizational placement of the AAP as part of its evaluation of the overall ITIN process. This evaluation should also include a requirement that the IRS function in which the AAP is eventually located establish goals, objectives, critical success factors, performance measures, and managerial accountability. To improve controls, we recommended that the acceptance agents submit copies of the applicants' supporting documents. This recommendation would: minimize the expenditure of resources since onsite visits to acceptance agents would be reduced or eliminated, provide for an objective evaluation of quality, and reduce the burden on acceptance agents by eliminating the need to maintain IRS records.

To improve program oversight, we recommended that the IRS use computer applications for management information and develop procedures for analyzing the ITIN database; require acceptance agents to certify compliance with their tax responsibilities and attest to criminal violations or professional misconduct; and require acceptance agents to reapply to the AAP on a periodic basis. We also recommended that the IRS terminate the MOU for any acceptance agent who has not certified a pre-determined number of Applications for IRS Individual Taxpayer Identification Number (Form W-7).

Management's Response: Management did not agree with our finding that the IRS has not made an organizational commitment to the AAP. In their response, management provided a historical overview of the AAP to demonstrate their commitment to and oversight of the Program.

The IRS agreed with our audit recommendations, except for Recommendation 2 that would require acceptance agents to submit to the IRS copies of the supporting documents that they reviewed. IRS management indicated it will not implement this recommendation because they believed this requirement would place an unnecessary burden on the IRS and on acceptance agents. The IRS' complete response to the draft report is included in Appendix IV.

Office of Audit Comment: Management's historical overview does not address the requirements of the General Accounting Office's (GAO) *Standards for Internal Control in the Federal Government*. These standards cite that a factor affecting the control environment is the agency's organizational structure that provides management's framework for planning, directing, and controlling operations to achieve agency objectives. A good internal control environment requires that the agency's

organizational structure clearly define key areas of authority and responsibility and establish appropriate lines of reporting. The AAP received initial management attention during implementation, but remains a program without an infrastructure that includes goals, objectives, critical success factors, performance measures, and adequate managerial oversight. With the increased concern about national security, the risks presented by the AAP are greater now than the program design ever envisioned.

Management's response to Recommendation 2 stated that the IRS reviewed documentation maintained by 25 acceptance agents during on-site visits and by correspondence. However, the IRS did not provide any documentation of any compliance checks. Moreover, the review of 25 acceptance agents over a 5-year period, from among the hundreds of acceptance agents registered with the IRS, does not provide an objective evaluation of quality. The IRS advised that additional quality reviews were not performed because they did not have sufficient management information on the number of applications certified by each agent or the necessary resources to properly assess the acceptance agents' compliance with documentation requirements. Management stated that they could not justify expending resources on acceptance agents' quality of work while they were receiving criticism for the decrease in the overall number of examinations of tax returns.

The ITIN Task Force recommendation of performing compliance-check visits for at least 20 percent of the acceptance agents will necessitate resource expenditures to perform compliance checks for over 180 of the 905 approved acceptance agents each year. We believe requiring acceptance agents to submit to the IRS copies of the supporting documents that they reviewed would reduce the use of IRS resources and better ensure that compliance resources could be focused where there is a greater risk of improprieties.

Finally, management's response stated that they analyzed the list of 276 acceptance agents that did not certify any ITINs during Calendar Year 2001. Our analysis was based on the IRS' database of acceptance agents. We provided our analysis of the data to the IRS because management had not developed any information on the characteristics of the acceptance agents. In fact, the IRS performed their analysis subsequent to the issuance of the draft report.

While we still believe that our second recommendation is worthwhile, we do not intend to elevate our disagreement concerning this matter to the Department of Treasury for resolution.

The Treasury Inspector General for Tax Administration (TIGTA) has designated this report as Limited Official Use (LOU) pursuant to Treasury Directive TD P-71-10, Chapter III, Section 2, "Limited Official Use Information and Other Legends" of the Department of Treasury Security Manual. Because this document has been designated LOU, it may only be made available to those officials who have a need to know the information contained within this report in the performance of their official duties. This report must be safeguarded and protected from unauthorized disclosure; therefore, all requests for disclosure of this report must be referred to the Disclosure Unit within the TIGTA's Office of Chief Counsel.

Please contact me at (202) 622-3837 if you have questions or Parker F. Pearson, Acting Assistant Inspector General for Audit (Small Business and Corporate Programs) at (410) 962-9637.

Management Oversight of the Acceptance Agent Program Is Needed to Assure that Individual Taxpayer Identification Numbers Are Properly Issued

Table of Contents

Background	Page 1
An Organizational Commitment Is Needed to Provide Reasonable Assurance that Goals Are Established and Achieved	Page 2
<u>Recommendation 1:</u>	Page 3
Oversight of Acceptance Agents Is Inadequate	Page 4
<u>Recommendation 2:</u>	Page 5
Management Information Is Needed to Effectively Oversee the Acceptance Agent Program	Page 7
<u>Recommendations 3 and 4:</u>	Page 11
<u>Recommendations 5 through 7:</u>	Page 12
Appendix I – Detailed Objective, Scope, and Methodology	Page 13
Appendix II – Major Contributors to This Report	Page 14
Appendix III – Report Distribution List	Page 15
Appendix IV – Management’s Response to the Draft Report	Page 16

Management Oversight of the Acceptance Agent Program Is Needed to Assure that Individual Taxpayer Identification Numbers Are Properly Issued

Background

An Internal Revenue Procedure allows an acceptance agent¹ to assist an alien or foreign individual in obtaining an Internal Revenue Service (IRS) Individual Taxpayer Identification Number (ITIN). An acceptance agent is a person or an entity who, pursuant to a written Memorandum of Understanding (MOU) with the IRS, is authorized to assist aliens and foreign individuals in obtaining ITINs. An acceptance agent can be a United States (U.S.) or foreign individual/entity. The ITIN process was implemented to facilitate return filing and improve compliance on tax returns and other documents filed by foreign individuals and aliens.

Effective for tax returns filed after December 31, 1996, foreign individuals are required to furnish either a Social Security Number (SSN) or an ITIN. Any alien, whether non-resident or resident, who is required to file or can be claimed as an exemption or dependent on a tax return, and who does not qualify for an SSN, must have an ITIN.

Foreign individuals, aliens, and their spouses and dependents apply for the ITIN using the Application for IRS Individual Taxpayer Identification Number (Form W-7). The IRS began processing Forms W-7 during July 1996.

The Form W-7 supporting documents and the ITIN constitute confidential taxpayer information. The ITIN is intended for tax purposes only and affects neither the immigration status of a foreign person nor his or her right to be legally employed in the U.S. However, while the ITIN may be used to file a tax return, it is not to be used for work purposes.

The Form W-7 and the original supporting documents² can be submitted by mail or presented directly to the IRS or to an acceptance agent. The acceptance agent submits the Form W-7 to the IRS on behalf of an applicant, without having to furnish the supporting documentary evidence. The

¹ Internal Revenue Procedure 96-52 (November 1996) provides for acceptance agents and certifying acceptance agents. Currently, the IRS uses only certifying acceptance agents.

² For example, birth records, driver's license, marriage record, etc.

Management Oversight of the Acceptance Agent Program Is Needed to Assure that Individual Taxpayer Identification Numbers Are Properly Issued

acceptance agent certifies to the IRS that the appropriate documentary evidence was reviewed and that a record of such documentation is being maintained.

We performed this audit at the Headquarters Office of the Large and Mid-Size Business (LMSB) Division in Washington, DC, and the IRS' Campus in Philadelphia, Pennsylvania. The audit was performed between May and July 2002 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.

An Organizational Commitment Is Needed to Provide Reasonable Assurance that Goals Are Established and Achieved

The IRS has not made an organizational commitment to the Acceptance Agent Program (AAP) because, subsequent to the IRS' reorganization in Calendar Year (CY) 2000, the operating division responsible for the overall ITIN process has not been determined. Currently, the LMSB Division has functional responsibility for managing the AAP. However, the Small Business/Self-Employed (SB/SE) Division oversees the ITIN process, while the Wage and Investment (W&I) Division processes the ITIN applications.

The General Accounting Office's (GAO) *Standards for Internal Control in the Federal Government* state that a factor affecting the control environment is the agency's organizational structure that provides management's framework for planning, directing, and controlling operations to achieve agency objectives. A good internal control environment requires that the agency's organizational structure clearly define key areas of authority and responsibility and establish appropriate lines of reporting.

Without an organizational commitment with management accountability and improved management and internal controls, the AAP cannot be effectively managed. The absence of this organizational commitment has left the AAP without an infrastructure that includes goals, objectives, critical success factors, performance measures, and adequate managerial oversight.

Management Oversight of the Acceptance Agent Program Is Needed to Assure that Individual Taxpayer Identification Numbers Are Properly Issued

Based on national security risks, the ITIN process is an area of vulnerability and concern. According to an article in Tax Notes Today, July 8, 2002, entitled, "National Security May Require Rethinking the ITIN," by George Guttman, the ITINs were created for a specific purpose but are being used for unintended purposes. For example, the Federal Deposit Insurance Corporation has indicated that banks may accept the ITIN to open a bank account. By opening a bank account, an individual may be able to obtain a credit card. In addition, a number of states are willing to accept an ITIN to issue a driver's license. With an accepted form of government-issued identification like an ITIN, it is easier for terrorists and their sympathizers to operate in an open society while planning hostile actions. Because of concerns about this possibility, the IRS has formed a task force to study the overall ITIN process.

Recommendation

1. The Director, International, LMSB Division, should ensure that the IRS' ITIN task force decides on the organizational placement of the AAP as part of its evaluation of the overall ITIN process. This evaluation should also include a requirement that the IRS function in which the AAP is eventually located should establish goals, objectives, critical success factors, performance measures, and managerial accountability for the Program.

Management's Response: The IRS did not agree with our finding that the IRS has not made an organizational commitment to the AAP. In their response, management provided a historical overview of the AAP to demonstrate their commitment to and oversight of the Program.

However, the IRS is implementing our recommendation. Full ownership of the ITIN process and AAP will be transferred to the W&I Division. A team of representatives from the W&I, LMSB, and SB/SE Divisions will be formed to develop an action plan to implement changes, including program goals, objectives, critical success factors, performance measures, and

Management Oversight of the Acceptance Agent Program Is Needed to Assure that Individual Taxpayer Identification Numbers Are Properly Issued

managerial accountability for the international processing programs.

Office of Audit Comment: Management's response to this report disputed our conclusion concerning the IRS' organizational commitment to the AAP. The IRS' historical overview does not address the requirements of the GAO's *Standards for Internal Control in the Federal Government*. These standards cite that a factor affecting the control environment is the agency's organizational structure that provides management's framework for planning, directing, and controlling operations to achieve agency objectives. A good internal control environment requires that the agency's organizational structure clearly define key areas of authority and responsibility and establish appropriate lines of reporting. The AAP received initial management attention during implementation, but remains a program without an infrastructure that includes goals, objectives, critical success factors, performance measures, and adequate managerial oversight. With the increased concern about national security, the risks presented by the AAP now are greater than the program design ever envisioned.

Oversight of Acceptance Agents Is Inadequate

The MOU agreed to by the IRS and each of the 905³ acceptance agents includes a requirement that the IRS is entitled to review the copies of the original documents submitted by applicants to secure their ITINs. However, the IRS does not, in effect, exercise its right under the MOU to perform this review.

During CY 2001, acceptance agents certified 72,785 (6.7 percent) of the 1.08 million ITIN applications. These agents are required to send the original Form W-7 and a verification statement to the IRS, and then maintain copies of the original supporting documentation for 3 years. Since the inception of the AAP, the IRS has not performed any objective compliance reviews of the documentation maintained by the

³ As of May 28, 2002, according to IRS records, there were 908 acceptance agents (905 active and 3 terminated).

**Controls Need to Be Improved to Ensure
Accurate Direct Deposit of Tax Refunds**

May 2003

Reference Number: 2003-40-108



INSPECTOR GENERAL
for TAX
ADMINISTRATION

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

May 9, 2003

MEMORANDUM FOR COMMISSIONER, WAGE AND INVESTMENT DIVISION

Gordon C. Milbourn

FROM: Gordon C. Milbourn III
Acting Deputy Inspector General for Audit

SUBJECT: Final Audit Report - Controls Need to Be Improved to Ensure
Accurate Direct Deposit of Tax Refunds (Audit # 200240058)

This report presents the results of our review to determine the effectiveness of controls to prevent the diversion of refunds claimed on paper filed tax returns to direct deposit¹ accounts not authorized by the taxpayers.

In Tax Year (TY) 1995, the Internal Revenue Service (IRS) began to offer taxpayers who file paper tax returns the option of having their tax refunds directly deposited. To obtain a tax refund via direct deposit, the taxpayer is required to provide the Routing Transit Number, Deposit Account Number, and type of account (checking or savings) on his or her tax return. This information is necessary for the IRS to identify the specific account to which the tax refund should be deposited. The tax return instructions caution taxpayers that the IRS is not responsible for a lost tax refund if a taxpayer enters the wrong account information on the tax return.

During TY 2001,² the IRS processed over 79 million paper filed individual income tax returns, of which over 56 million had claims for tax refunds totaling approximately \$100 billion. However, control weaknesses present opportunities for tax refunds claimed on paper tax returns to be directly deposited to unauthorized bank accounts. For example, between Calendar Years

(b)(3)-26 U.S.C. 6103, (b)(7)(C)

¹ Direct deposit is an electronic transfer of a tax refund to a bank account specified by the taxpayer on the tax return, instead of the issuance of a paper refund check.

² TY 2001 tax returns were processed in the Submission Processing sites from January 1, 2002, through August 5, 2002. Submission Processing sites are the data processing arm of the IRS. The sites process paper submissions, correct errors, and forward data to the computing centers for analysis and posting to taxpayer accounts.

(b)(3) 26 U.S.C. 6103, (b)(7)(C)

Control weaknesses in both the instructions for completing the United States Individual Income Tax Return (Form 1040) and the processing procedures for when the direct deposit fields are left blank expose each of these tax refunds to the risk that an IRS employee can divert the tax refund via direct deposit to an unauthorized bank account. Furthermore, diversions of tax refunds result in taxpayers being significantly burdened, as they do not timely receive the tax refunds to which they are entitled.

Implementation of our recommendations will reduce the risk of diversion and enable detection of employees who may be involved in future improprieties. These recommendations are considered to impose the least burden on the taxpayer and are cost beneficial to the IRS. Since the initiation of the audit, IRS management has taken actions as a result of our recommendations to implement guidance to detect, deter, and refer to the TIGTA Office of Investigations potential cases of diversion of taxpayer refunds by IRS employees via direct deposit.

For the TY 2003 Filing Season,³ Form 1040 instructions should be revised to require taxpayers to line through the direct deposit fields on paper filed tax returns when they are left blank. The IRS should develop procedures to address those tax returns on which the taxpayers failed to line through blank direct deposit fields. Additionally, the IRS should work with tax software preparation companies to initiate modifications to the manner in which the direct deposit fields print out for those tax returns prepared via computer and sent to IRS as paper tax returns. These modifications should eliminate the printing of the direct deposit fields when the taxpayer elects to receive a paper tax refund check.

Management's Response: IRS management agreed with the recommendations presented in the report and will take corrective action. Specifically, the 2003 instructions for completing Form 1040 will be changed to tell taxpayers to line through the direct deposit fields on the tax return if they are not requesting a direct deposit of a refund check. In addition, Submission Processing procedures will be changed to instruct Code and Edit function employees to line through this section if a taxpayer fails to follow the instructions. Also, the IRS will contact the software developers and request that they modify their programs so that the fields do not appear or cannot be altered if a taxpayer wishes to receive a paper refund check. These changes will be effective for TY 2003.

The IRS did not agree with the potential benefits presented in the report. Specifically, the IRS believed that our calculation did not consider the fact that over 8.6 million taxpayers filing paper tax returns used direct deposit to have over \$18.3 billion deposited into their accounts. Our benefit should not include these taxpayers in the calculation. Management's complete response to the draft report is included as Appendix V.

³ The filing season is the period from January through April when most individual income tax returns are filed.

Office of Audit Comment: We appreciate management's recognition that the current procedures for direct deposit present opportunities for tax refunds claimed to be directly deposited to unauthorized bank accounts, along with their agreement to implement corrective actions, as the recommendations made in the report will substantially reduce the possibility of diversion. However, management disagreed with the potential benefits that our recommendations may have on the protection of revenue. This disagreement relates to the fact that our calculation includes tax refunds paid via direct deposit. We disagree with management's position that the benefits should be reduced by the amount of tax refunds paid via direct deposit. Our disagreement is based in the fact that control weaknesses reported present the opportunity for these tax refunds to also be potentially diverted to unauthorized bank accounts.

The TIGTA has designated this report as Limited Official Use (LOU) pursuant to Treasury Directive TD P-71-10, Chapter III, Section 2, "Limited Official Use Information and Other Legends" of the Department of Treasury Security Manual. Because this document has been designated LOU, it may only be made available to those officials who have a need to know the information contained within this report in the performance of their official duties. This report must be safeguarded and protected from unauthorized disclosure; therefore, all requests for disclosure of this report must be referred to the Disclosure Unit within the TIGTA's Office of Chief Counsel.

Copies of this report are also being sent to the IRS managers who are affected by the report recommendations. Please contact me at (202) 622-6510 if you have questions or Michael R. Phillips, Assistant Inspector General for Audit (Wage and Investment Income Programs), at (202) 927-0597.

**Controls Need to Be Improved to Ensure Accurate
Direct Deposit of Tax Refunds**

Table of Contents

Background.....	Page 1
Control Weaknesses Present Opportunities for Tax Refunds Claimed on Paper Tax Returns to Be Directly Deposited to Unauthorized Bank Accounts.....	Page 3
<u>Recommendations 1 and 2:</u>	Page 8
Appendix I – Detailed Objective, Scope, and Methodology.....	Page 9
Appendix II – Major Contributors to This Report	Page 11
Appendix III – Report Distribution List.....	Page 12
Appendix IV – Outcome Measures.....	Page 13
Appendix V – Management’s Response to the Draft Report.....	Page 15

Controls Need to Be Improved to Ensure Accurate Direct Deposit of Tax Refunds

Background

In Tax Year (TY) 1995, the Internal Revenue Service (IRS) began to offer taxpayers who file paper tax returns the option of having their tax refunds directly deposited.¹ Tax refunds paid via direct deposit provide benefits to both the taxpayer and the IRS, including:

- Faster and more convenient receipt of the tax refund.
- Security of tax refund payment – no paper check to lose.
- Reduced refund issuance cost for the IRS when compared with issuing a paper tax refund check.

To obtain a tax refund via direct deposit, the taxpayer is required to enter the Routing Transit Number, Deposit Account Number, and type of account (checking or savings) on his or her tax return. This information is necessary for the IRS to identify the specific account to which the tax refund should be deposited. The tax return instructions caution taxpayers that the IRS is not responsible for a lost tax refund if the taxpayer enters the wrong account information on the tax return.

During TY 2001, the IRS processed over 79 million paper filed individual tax returns, of which over 56 million had claims for tax refunds totaling approximately \$100 billion, as shown in the following table.

¹ Direct deposit is an electronic transfer of a tax refund to a bank account specified by the taxpayer on the tax return, instead of the issuance of a paper refund check.

Controls Need to Be Improved to Ensure Accurate Direct Deposit of Tax Refunds

Tax Refunds Issued by Type of Refund TY 2001 Paper Filed Tax Returns

Type of Refund	Refunds Issued	Dollars Refunded
Paper Check	47.7 million	\$81.3 billion
Direct Deposit	8.6 million	\$18.3 billion
Total	56.3 million	\$99.6 billion

Source: Treasury Inspector General for Tax Administration (TIGTA) Extract of TY 2001 Direct Deposit Database through June 2002 and Submission Processing Individual Master File² Refund Report through October 2002.

The IRS generally processes a paper filed tax return within 6 weeks from the date the tax return is received.

Subsequent to the 6-week period, taxpayers who do not receive their tax refunds can contact any of the various IRS Customer Service functions to inquire about their missing tax refunds. The IRS' Customer Service options include calling the

toll-free telephone service, using the automated refund inquiry system, visiting a Taxpayer Assistance Center, sending in correspondence, and contacting the Taxpayer Advocate Service.³ The identification of missing tax refunds is based solely on a taxpayer contacting the IRS, as the IRS has no process to proactively identify missing tax refunds.

Contacting the IRS through any of the above Customer Service options initiates the IRS' tax refund inquiry process. The IRS' Refund Inquiry Unit will work with the taxpayer to obtain pertinent information and perform research to determine what may have occurred with the missing tax refund. Based on the results of the Refund Inquiry Unit's research, the taxpayer could be reissued his or her tax refund or be provided with information as to why the IRS is not responsible for the missing refund. For a taxpayer who does not receive a tax refund within 45 days after the date the

² The Individual Master File is the IRS database that maintains transactions or records of individual tax accounts.

³ "Lost or stolen tax refunds" was ranked 11th out of 23 broadly defined reasons why taxpayers contacted the Taxpayer Advocate Service in Fiscal Year 2001.

Controls Need to Be Improved to Ensure Accurate Direct Deposit of Tax Refunds

IRS receives the tax return, the IRS will pay the taxpayer interest on the tax refund.

Audit testing was performed at the National Headquarters for Submission Processing (Cincinnati, Ohio, and Washington, D.C.) and the eight Submission Processing sites⁴ that accept and process paper filed individual income tax returns. Audit work was performed between June and December 2002. The audit was conducted in accordance with *Government Auditing Standards*. Detailed information on our audit objective, scope, and methodology is presented in Appendix I. Major contributors to the report are listed in Appendix II.

Control Weaknesses Present Opportunities for Tax Refunds Claimed on Paper Tax Returns to Be Directly Deposited to Unauthorized Bank Accounts

Controls need to be improved to ensure that tax refunds are accurately directly deposited. Specifically, between
Calendar Years,

(b)(3)-26 U.S.C. 6103,(b)(7)(C)

⁴ Submission Processing sites are located in Andover, Atlanta, Austin, Holtsville, Fresno, Kansas City, Memphis, and Philadelphia. Submission Processing sites are the data processing arm of the IRS. The sites process paper submissions, correct errors, and forward data to the computing centers for analysis and posting to taxpayer accounts.

Controls Need to Be Improved to Ensure Accurate Direct Deposit of Tax Refunds

We alerted IRS executives on June 25, 2002, to the control weaknesses in the processing of paper filed tax returns that provide opportunities for tax refunds claimed on paper filed tax returns to be directly deposited to bank accounts that were not authorized by the taxpayers. As a result of this alert, IRS management added this risk as a reportable condition to the tax processing Annual Assurance Process memorandum.⁵ Further, the Submission Processing site functions developed an action plan to determine what controls were currently in place to prevent unauthorized direct deposits.

Contributing factors

Several factors contributed to the control weaknesses we identified.

Instructions for completing the United States Individual Income Tax Return (Form 1040) do not require the taxpayer to void the direct deposit fields if the taxpayer does not use them. When the direct deposit fields are left blank, the opportunity exists for IRS employees who work in the areas that receive and open tax returns,⁶ review the tax returns for completeness,⁷ and input the information from tax returns into IRS computers⁸ to alter the fields. Specifically, the instructions do not require the taxpayer to take any preventive steps (e.g., lining through the direct deposit fields on the tax return to void them rather than leaving them blank) to ensure the fields cannot be manipulated subsequent to the filing of the tax return.

Furthermore, IRS reports indicate that approximately 48 percent of paper filed tax returns are prepared on a computer using tax preparation software packages. When these tax returns are printed, the direct deposit fields are left blank for those taxpayers who elect to receive a paper check

⁵ The Annual Assurance memorandum reports instances of waste, fraud, and abuse identified in the IRS' Submission Processing sites.

⁶ Receipt and Control function, which is responsible for handling mail.

⁷ Code and Edit function, which is responsible for marking returns for entry into IRS computer systems.

⁸ Data Transcription function, which is responsible for entering tax return data into IRS computer systems.

Controls Need to Be Improved to Ensure Accurate Direct Deposit of Tax Refunds

tax refund. As with the hand-written paper Forms 1040, the direct deposit fields on these tax returns can be altered.

Tax return processing controls do not minimize the risk of, or identify potential instances of, employee diversion of tax refunds via direct deposit to unauthorized bank accounts.

There are no controls in place to minimize the risk of, or identify potential instances of, employee impropriety via direct deposit in the areas that receive and open tax returns, review the tax returns for completeness, and input the information from tax returns into IRS computers.

Specifically, IRS procedures do not require actions to be taken upon the IRS' receipt of a paper tax return to minimize the possibility of an employee inputting unauthorized direct deposit information in fields left blank by the taxpayer.

Procedures do not provide IRS employees with guidance on identifying and referring for investigation tax returns with suspicious direct deposits. Procedures were not developed and distributed to those employees who work in the areas that receive and open tax returns, review the tax returns for completeness, and input the information from tax returns into IRS computers informing them of the need to refer cases with potentially unauthorized direct deposits to the TIGTA Office of Investigations.

When working refund inquiries, IRS employees did not consider the possibility of employee impropriety for those cases involving direct deposit. Employees in those functions that assist taxpayers who do not receive their refunds were not required to consider the possibility of employee impropriety when evaluating tax refund inquiries that involve direct deposits.

Prior to the initiation of this audit, IRS management presumed that most unauthorized direct deposit refunds were the result of IRS processing errors.⁹ The IRS' position has been that in the case of direct deposits, the taxpayer has the burden to show that the tax refund was deposited to an

⁹ Processing errors may include erroneously entering the direct deposit data from another taxpayer's tax return or transposition of numbers in the direct deposit fields.

TD P 15-71

**Increased Taxpayer Awareness and Improved
Guidance Are Needed to Ensure Accurate
Direct Deposit of Tax Refunds Claimed on
E-Filed Tax Returns**

October 2003

Reference Number: 2004-40-016

TD P 15-71



INSPECTOR GENERAL
for TAX
ADMINISTRATION

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

October 31, 2003

MEMORANDUM FOR COMMISSIONER, WAGE AND INVESTMENT DIVISION

Gordon C. Milbourn III

FROM: Gordon C. Milbourn III
Assistant Inspector General for Audit (Small Business and
Corporate Programs)

SUBJECT: Final Audit Report - Increased Taxpayer Awareness and
Improved Guidance Are Needed to Ensure Accurate Direct
Deposit of Tax Refunds Claimed on E-Filed Tax Returns
(Audit # 200340029)

This report presents the results of our review of the direct deposit of tax refunds claimed on electronically filed (*e-filed*) tax returns. The overall objective of this review was to determine the effectiveness of controls to prevent the diversion of tax refunds claimed on *e-filed* tax returns to direct deposit¹ bank accounts not authorized by the taxpayers.

The Internal Revenue Service's (IRS) Electronic Filing (*e-file*) Program offers taxpayers an alternative to filing a traditional paper tax return. The *e-file* Program enables taxpayers to send their tax returns to the IRS in an electronic format via an IRS authorized *e-file* Provider.² *E-file* Providers can transmit tax returns they prepared and/or transmit tax returns prepared by taxpayers. *E-file* Providers include individuals or organizations that serve as volunteers in IRS-sponsored programs such as the Volunteer Income Tax Assistance (VITA) and Tax Counseling for the Elderly (TCE) Programs.³ As of July 2003, there were 154,468⁴ IRS-authorized *e-file* Providers.

¹ Direct deposit is an electronic transfer of a tax refund to an account specified by the taxpayer.

² For the purpose of this report, authorized *e-file* Providers include individuals or businesses that prepare tax returns and transmit the tax returns electronically to the IRS, or individuals or businesses that electronically transmit tax returns to the IRS from taxpayers who elect to prepare their own tax returns. This does not include TeleFile tax returns where taxpayers can *e-file* their tax returns using a telephone.

³ The VITA and TCE Programs provide free tax return preparation including *e-filing*.

⁴ The IRS provided this figure, and we did not validate it. However, it is overstated, as *e-file* Providers can be authorized to transmit *e-filed* tax returns to more than one Electronic Individual Return Submission Processing Site.

Since 1988, the IRS has offered taxpayers who *e-file* the option of having their tax refunds directly deposited. To obtain a tax refund via direct deposit, taxpayers are required to provide on their tax returns the Routing Transit Number, Deposit Account Number, and type of account (checking or savings) to which the refunds will be deposited. The tax return instructions caution taxpayers that the IRS is not responsible for a lost tax refund if the taxpayer enters the wrong account information on the tax return. During the 2002 Filing Season,⁵ the IRS processed over 39 million *e-filed* individual income tax returns, prepared and/or transmitted by an *e-file* Provider, that had claims for tax refunds totaling approximately \$90 billion, with approximately 30 million of the tax refund claims (for approximately \$75 billion) paid via direct deposit.

Opportunities exist for *e-file* Providers to change or add direct deposit account numbers on a taxpayer's tax return prior to *e-filing* the tax return to the IRS. This impropriety can result in a tax refund claimed on an *e-filed* tax return being directly deposited to a bank account not authorized by the taxpayer. For example,

[REDACTED] In another case, [REDACTED] (b)(3);26 U.S.C. 6103 (b)(7)(C) [REDACTED]

A number of factors contribute to the weaknesses identified. One is that the instructions for completing the United States (U.S.) Individual Income Tax Return (Form 1040) do not require the taxpayer to void the direct deposit field on the tax return if he or she wants to receive a paper tax refund check. In addition, cautionary information and/or educational efforts have not been provided or undertaken to increase taxpayers' awareness of the need to obtain and retain copies of their tax returns and signature authorization documents, as well as to ensure the accuracy of direct deposits. Further, refund inquiry guidance does not contain specific steps to be followed to validate a taxpayer's intention when a tax refund is inaccurately directly deposited, and specific legal guidance does not exist regarding erroneous direct deposits for *e-filed* tax returns.

Implementation of our recommendations will reduce the risk of tax refunds claimed on *e-filed* tax returns being diverted to unauthorized bank accounts. Additionally, our recommendations will improve the consistency with which taxpayers are treated when their tax refunds are inaccurately directly deposited. We recommended that the Commissioner, Wage and Investment (W&I) Division, add a cautionary statement on *e-file* signature authorization forms⁶ alerting taxpayers to the importance of accurately providing direct deposit bank account information and retaining copies of their tax returns; undertake educational efforts to increase taxpayer and *e-file* Provider awareness of the importance of taxpayers obtaining and retaining copies of tax returns;

⁵ The period from January through mid-April when most individual income tax returns are filed.

⁶ Signature authorization forms are required to authenticate the electronic tax return and provide certification that the return is true, correct, and complete. These forms include the U.S. Individual Income Tax Declaration for an IRS *e-file* Return (Form 8453) and the IRS *e-file* Signature Authorization (Form 8879).

and provide adequate resources to volunteer sites to ensure copies of tax returns are provided to taxpayers who use these services. We further recommended that the Commissioner, W&I Division, revise refund inquiry guidance, and explore whether a legislative change to address the IRS' authority to reissue a taxpayer's tax refund in the event of theft via direct deposit is appropriate.

Management's Response: Management agreed to implement the majority of our recommendations, which will reduce the risk of tax refunds claimed on *e-filed* tax returns being diverted to unauthorized bank accounts and improve the consistency with which taxpayers are treated when their tax refunds are inaccurately direct deposited. Specifically, the IRS is adding a statement to the IRS *e-file* Signature Authorization (Form 8879) to remind taxpayers that they should get a copy of their return. The IRS will develop messages for filing season and practitioner communications and will advise taxpayers of the need to retain copies of returns and signature forms in national print and broadcast media in the 2004 *e-file* marketing campaign. To ensure volunteer tax preparation sites provide copies of returns to taxpayers, the IRS will include the requirement in guidance provided to volunteers and site coordinators when establishing volunteer sites and include the requirement as part of the volunteer training. The IRS revised guidance to instruct employees to obtain copies of the taxpayer's return and compare it with the electronically transmitted data. The IRS will work with the National Taxpayer Advocate to determine if current procedures for forged checks could be applied when a theft of a direct deposit has been verified.

Management disagreed with our recommendation to add a cautionary statement to the U.S. Individual Income Tax Declaration for an IRS *e-file* Return (Form 8453). Management cited that the *e-file* Provider signs a statement on the Form 8453 agreeing to provide the taxpayer with copies of all forms and information filed with the IRS. Taxpayers sign Form 8453 declaring that the information given to the *e-file* Provider agrees with the electronic return; therefore, the taxpayer would have reviewed the direct deposit information for accuracy and would receive a copy of the Form 8453 showing the direct deposit information.

In addition, management acknowledges the outcome measure we reported as being "potential" revenue protection; however, they do not believe that our outcome measure reflects a realistic representation of the risk associated with improprieties by *e-file* Providers. Further, management indicated that they realize that there are risks associated with direct deposit; however, existing safeguards minimize these risks. Management's complete response to the draft report is included as Appendix V.

Office of Audit Comment: While we still believe our recommendation regarding the inclusion of a cautionary statement on Form 8453 is worthwhile, we do agree that improved safeguards will minimize the risk of improprieties by *e-file* Providers. We do not intend to elevate our disagreement concerning this matter to the Department of Treasury for resolution.

As we indicated in our audit report, the outcome is provided in quantifiable terms to demonstrate the value that our audit recommendations will have on tax administration

and business operations and to show the number of taxpayers who are potentially at risk when filing an electronic tax return with the assistance of an *e-file* Provider and the estimated refund dollars claimed.

The Treasury Inspector General for Tax Administration (TIGTA) has designated this report as Limited Official Use (LOU) pursuant to Treasury Directive TD P-71-10, Chapter III, Section 2, "Limited Official Use Information and Other Legends" of the Department of Treasury Security Manual. Because this document has been designated LOU, it may only be made available to those officials who have a need to know the information contained within this report in the performance of their official duties. This report must be safeguarded and protected from unauthorized disclosure; therefore, all requests for disclosure of this report must be referred to the Disclosure Section within the TIGTA's Office of Chief Counsel.

Please contact me at (202) 622-6510 if you have questions or Michael R. Phillips, Assistant Inspector General for Audit (Wage and Investment Income Programs), at (202) 927-0597.

**Increased Taxpayer Awareness and Improved Guidance Are Needed to Ensure Accurate
Direct Deposit of Tax Refunds Claimed on E-Filed Tax Returns**

Table of Contents

Background.....	Page 1
Opportunities Exist for E-File Providers to Change or Add Direct Deposit Account Numbers on a Taxpayer's Tax Return Prior to E-Filing.....	Page 3
<u>Recommendation 1:</u>	Page 8
<u>Recommendations 2 and 3:</u>	Page 9
<u>Recommendation 4:</u>	Page 10
Appendix I – Detailed Objective, Scope, and Methodology	Page 11
Appendix II – Major Contributors to This Report	Page 13
Appendix III – Report Distribution List.....	Page 14
Appendix IV – Outcome Measures.....	Page 15
Appendix V – Management's Response to the Draft Report.....	Page 18

Increased Taxpayer Awareness and Improved Guidance Are Needed to Ensure Accurate Direct Deposit of Tax Refunds Claimed on E-Filed Tax Returns

Background

The Internal Revenue Service's (IRS) Electronic Filing (*e-file*) Program offers taxpayers an alternative to filing a traditional paper tax return. The *e-file* Program enables taxpayers to send their tax returns to the IRS in an electronic format via an IRS-authorized *e-file* Provider.¹ *E-file* Providers can transmit tax returns they prepared and/or transmit tax returns prepared by taxpayers. *E-file* Providers include individuals or organizations that serve as volunteers in IRS-sponsored programs such as the Volunteer Income Tax Assistance (VITA) and Tax Counseling for the Elderly (TCE) Programs.² As of July 2003, there were 154,468³ IRS-authorized *e-file* Providers.

Since 1988, the IRS has offered taxpayers who *e-file* the option of having their tax refunds directly deposited.⁴ Tax refunds paid via direct deposit provide benefits to both the taxpayer and the IRS, including:

- Faster and more convenient receipt of the tax refund.
- Security of tax refund payment – no paper check to lose.
- Reduced tax refund issuance cost for the IRS when compared with issuing a paper tax refund check.

To obtain a tax refund via direct deposit, the taxpayer is required to provide on the tax return the Routing Transit Number, Deposit Account Number, and type of account (checking or savings) to which the refund will be deposited. The tax return instructions caution the taxpayer that the IRS

¹ For the purpose of this report, authorized *e-file* Providers include individuals or businesses that prepare tax returns and transmit the tax returns electronically to the IRS, or individuals or businesses that electronically transmit tax returns to the IRS from taxpayers who elect to prepare their own tax returns. This does not include TeleFile tax returns where taxpayers can *e-file* their tax returns using a telephone.

² The VITA and TCE Programs provide free tax return preparation including *e-filing*.

³ The IRS provided this figure, and we did not validate it. However, it is overstated, as *e-file* Providers can be authorized to transmit electronically filed tax returns to more than one Electronic Individual Return Submission Processing Site.

⁴ Direct deposit is an electronic transfer of a tax refund to an account specified by the taxpayer.

Increased Taxpayer Awareness and Improved Guidance Are Needed to Ensure Accurate Direct Deposit of Tax Refunds Claimed on E-Filed Tax Returns

is not responsible for a lost tax refund if the taxpayer enters the wrong account information on the tax return.

During the 2002 Filing Season,⁵ over 39 million electronically filed (*e-filed*) tax returns were prepared and/or transmitted by an *e-file* Provider and had claims for tax refunds totaling approximately \$90 billion. Approximately 30 million of the tax refund claims (for approximately \$75 billion) were paid via direct deposit.

Tax Refunds Issued During 2002 Filing Season by E-File Providers

Type of Tax Refund	Volume of Tax Refunds Issued	Dollars Claimed in Tax Refunds
Paper Check	9,655,103	\$14,735,202,248
Direct Deposit	29,923,547	\$75,350,244,407
Total	39,578,650	\$90,085,446,655

Source: Wage and Investment Division Electronic Tax Administration Final Tax Year 2001 National Service Center Report Through October 20, 2002, and IRS personnel.

The IRS generally processes an *e-filed* tax return and issues the tax refund within 3 weeks from the date the tax return is received. Subsequent to the 3-week period, taxpayers who do not receive their tax refunds can contact any of the various IRS Customer Service functions to inquire about their missing tax refunds. The IRS' Customer Service options include calling the toll-free telephone service, using the automated tax refund inquiry system, visiting a Taxpayer Assistance Center, sending in correspondence, and contacting the Taxpayer Advocate Service.⁶ The identification of missing tax refunds is based solely on taxpayers contacting the IRS, as the IRS has no process to proactively identify missing tax refunds.

Contacting the IRS through the above Customer Service options initiates the IRS' tax refund inquiry process. The

⁵ The period from January through mid-April when most individual tax returns are filed.

⁶ "Lost or stolen refunds" was ranked 8th of 25 reasons why taxpayers contacted the Taxpayer Advocate Service for Fiscal Year 2002, based on the Taxpayer Advocate Management Information System receipts from October 1, 2001, to September 30, 2002.

Increased Taxpayer Awareness and Improved Guidance Are Needed to Ensure Accurate Direct Deposit of Tax Refunds Claimed on E-Filed Tax Returns

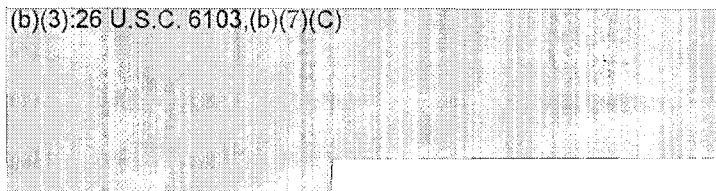
IRS' Refund Inquiry Unit will work with the taxpayers to obtain pertinent information and perform research to determine what may have happened to the missing refunds.

Audit work was performed at the National Headquarters for Electronic Tax Administration (Washington, D.C.) and the five Electronic Individual Return Submission Processing Sites⁷ that accept and process *e-filed* individual income tax returns. Audit work was performed from October 2002 through June 2003 in accordance with *Government Auditing Standards*. Detailed information on our audit objective, scope, and methodology is presented in Appendix I. Major contributors to the report are listed in Appendix II.

Opportunities Exist for E-File Providers to Change or Add Direct Deposit Account Numbers on a Taxpayer's Tax Return Prior to E-Filing

Opportunities exist for *e-file* Providers to change or add direct deposit account numbers on a taxpayer's tax return prior to *e-filing* the tax return with the IRS. This impropriety can result in tax refunds claimed on *e-filed* tax returns being directly deposited to bank accounts not authorized by the taxpayers. Specifically, instances have occurred where *e-file* Providers and volunteers participating in the IRS' VITA Program have altered direct deposit information on *e-file* tax returns prior to transmitting the tax returns to the IRS. These alterations, whether intentional or inadvertent, have resulted in tax refunds being directly deposited to bank accounts not authorized by the taxpayers. For example:

- (b)(3), 26 U.S.C. 6103, (b)(7)(C)



- (b)(3), 26 U.S.C. 6103, (b)(7)(C)



⁷ Electronic Individual Return Submission Processing Sites are located at the Andover, Massachusetts; Austin, Texas; Cincinnati, Ohio; Memphis, Tennessee; and Ogden, Utah IRS campuses. The campuses are the data processing arms of the IRS; they process submissions, correct errors, and forward data to the computing centers for analysis and posting to taxpayer accounts.

Increased Taxpayer Awareness and Improved Guidance Are Needed to Ensure Accurate Direct Deposit of Tax Refunds Claimed on E-Filed Tax Returns

(b)(3);26 U.S.C. 6103,(b)(7)(C)

Furthermore, the IRS policy is not consistent in how it resolves stolen tax refund checks and fraudulently diverted direct deposits of tax refunds. In situations that involve inaccurate direct deposits, the burden is on the taxpayer to show that the refund was deposited to a bank account *other* than the bank account he or she designated on the tax return. An IRS Chief Counsel Advice⁸ dated September 6, 2002, stated that in the context of direct deposit, the IRS satisfies its burden of proof by showing that the tax refund was sent to the bank account designated on the tax return. If the taxpayer does not show that the tax refund was deposited to an account other than the bank account he or she designated on the return, then the IRS does not have authority to replace the incorrectly deposited tax refund.

This advice differs significantly from the IRS' policy related to stolen tax refund checks. For example, if a taxpayer's tax refund check is stolen, the IRS will reissue the refund. In comparison, if a tax refund is fraudulently directly deposited to an unauthorized bank account, in most cases the IRS will not reissue the tax refund. The IRS' position is that the tax refund was deposited to the account specified on the tax return. This does not take into account possible manipulation of the direct deposit information prior to the tax return being transmitted to the IRS.

In many cases involving theft of tax refunds via direct deposit, the IRS functions assisting a taxpayer with a tax refund inquiry may obtain a legal opinion from the IRS Chief Counsel to determine if the IRS has the authority to replace the taxpayer's tax refund. Varied responses have been received and have led to inconsistent treatment of taxpayers even when the circumstances involved in the cases are identical. For example, one taxpayer could be

⁸ A Chief Counsel Advice is written advice or instruction prepared by the Office of Chief Counsel that is issued to IRS employees. It conveys legal interpretation of internal revenue law either in general or as applied to specific taxpayers or groups of specific taxpayers.

TD P 15-71

**Persistent Physical Security Vulnerabilities
Should Be Corrected to Better Protect
Facilities and Computer Resources**

July 2001

Reference Number: 2001-20-108

TD P 15-71



INSPECTOR GENERAL
for TAX
ADMINISTRATION

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

July 23, 2001

MEMORANDUM FOR DEPUTY COMMISSIONER FOR MODERNIZATION &
CHIEF INFORMATION OFFICER

A handwritten signature in cursive script, reading "Pamela J. Gardiner", is positioned above the "FROM:" line.

FROM: Pamela J. Gardiner
Deputy Inspector General for Audit

SUBJECT: Final Audit Report - Persistent Physical Security Vulnerabilities
Should Be Corrected to Better Protect Facilities and Computer
Resources

This report presents the results of our review of physical security at five Internal Revenue Service (IRS) facilities. In summary, we found security weaknesses that could allow an intruder easy access to IRS facilities and computer resources. Many of the weaknesses have persisted even though previously identified.

We recommended that the Chief, Agency-Wide Shared Services (AWSS), the Deputy Commissioner for Modernization & Chief Information Officer, and functional managers should coordinate efforts to improve employee security awareness. Management should provide the funds necessary to correct the specific security weaknesses we identified. The AWSS should also coordinate with the General Services Administration to ensure security weaknesses in multi-tenant buildings are corrected when identified.

Management agreed with our recommendations. However, regarding the control of equipment and data used in the Volunteer Income Tax Assistors program, they questioned the validity of the specific methods recommended. In those instances, we provided comments to clarify our position concerning the implementation of controls. Management's written response discusses several corrective actions that will improve the reported conditions. Their comments have been incorporated into the report where appropriate, and the full text of their comments is included as an appendix.

The Treasury Inspector General for Tax Administration (TIGTA) has designated this report as Limited Official Use (LOU) pursuant to Treasury Directive TD P-71-10,

Chapter III, Section 2, "Limited Official Use Information and Other Legends" of the Department of Treasury Security Manual. Because this document has been designated LOU, it may only be made available to those officials who have a need to know the information contained within this report in the performance of their official duties. This report must be safeguarded and protected from unauthorized disclosure; therefore, all requests for disclosure of this report must be referred to the Disclosure Unit within the TIGTA's Office of Chief Counsel.

Please contact me at (202) 622-6510 if you have questions, or Scott E. Wilson, Assistant Inspector General for Audit (Information Systems Programs) at (202) 622-8510.

**Persistent Physical Security Vulnerabilities Should Be
Corrected to Better Protect Facilities and Computer Resources**

Table of Contents

Executive Summary	Page	i
Objective and Scope	Page	1
Background	Page	1
Results	Page	3
Controls Were Not Always Sufficient to Prevent Unauthorized Access to Buildings and Computer Resources	Page	3
Security of Laptop Computers Needs Improvement to Deter Theft and to Protect Taxpayer Data	Page	10
Conclusion	Page	14
Appendix I – Detailed Objective, Scope, and Methodology	Page	15
Appendix II – Major Contributors to This Report	Page	17
Appendix III – Report Distribution List	Page	18
Appendix IV – Examples of Security Vulnerabilities	Page	19
Appendix V – Management’s Response to the Draft Report	Page	22

Persistent Physical Security Vulnerabilities Should Be Corrected to Better Protect Facilities and Computer Resources

Executive Summary

In recent months, certain federal agencies have incurred very damaging security breaches that can be traced to physical security weaknesses. These breaches may have caused the unauthorized disclosure of sensitive documents and data. Inadequate physical security could also lead to the loss of property and to the disruption of critical services.

With the emphasis on customer service, telecommunications advances, and the wide use of laptop computers, taxpayer data are much more accessible in the Internal Revenue Service (IRS) workplace. This new accessibility has also brought greater challenges for physically securing the data. While it is still more critical to provide physical security at major processing centers, employees (and intruders) can now access vast amounts of sensitive data at IRS offices and even small posts of duty.

We conducted this review to determine whether the IRS has adequate physical security controls to safeguard computer resources and data from the threat of misuse, loss, and damage. The Treasury Inspector General for Tax Administration and the General Accounting Office have conducted several physical security tests in recent audits. For this audit, we reviewed a computing center and four other offices to make our assessments.

Results

Over the past several years, IRS management has been implementing a strategic plan to methodically assess and improve physical security. As a result, security has been significantly improved at many IRS sites. In spite of these efforts, IRS facilities remain vulnerable to intruders, explosive attacks, theft of computer resources, and unauthorized disclosure of taxpayer data even in those offices where IRS has completed vulnerability assessments and improvements. Also, controls over laptop computers taken out of IRS facilities were weak.

The IRS has adequate policies and procedures for physical security. The procedures related to the issues in this report were not implemented, we believe, due to a lack of attention to security controls, insufficient security reviews, funding limitations, and ineffective coordination with the General Services Administration (GSA) at multi-tenant locations.

Controls Were Not Always Sufficient to Prevent Unauthorized Access to Buildings and Computer Resources

While we recognize the difficulty in preventing access to a determined, experienced intruder, the IRS could strengthen controls to prevent most unauthorized accesses. For

Persistent Physical Security Vulnerabilities Should Be Corrected to Better Protect Facilities and Computer Resources

example, there were numerous perimeter security vulnerabilities at various building entry points, including loading dock areas. Perimeter doors were left propped open, unlocked, or unguarded. Security gates were unlocked and perimeter fencing was in need of maintenance. And, several opportunities existed for bomb-laden vehicles to park near IRS facilities without detection. In addition, access cards and identification badges were not properly controlled increasing the risk they could be used to gain unauthorized access to IRS facilities.

Security of Laptop Computers Needs Improvement to Deter Theft and to Protect Taxpayer Data

Technology advances have enabled users to store large amounts of data on laptop computers. These computers enable users to take vast amounts of sensitive data outside the perimeter of IRS facilities and the confines of secure computer rooms. The portability of laptops greatly increases the risk that these computers could be lost or stolen. Based on poor inventory practices at the offices we visited, we could not determine if all laptops were accounted for. In addition, laptops were not properly secured after hours at one location.

Also, taxpayer information stored on approximately 5,000 laptops used by volunteer tax assistants was vulnerable to unauthorized disclosure. Systems used by these volunteers were not password protected, data were not encrypted, and taxpayer information was not removed from the hard drives of the laptops when no longer needed.

Summary of Recommendations

The Chief Agency-Wide Shared Services (AWSS) and functional managers should coordinate efforts to improve employee security awareness. Management should provide the funds necessary to correct the specific security weaknesses we identified. The AWSS should also coordinate with the GSA to ensure security weaknesses in multi-tenant buildings are corrected when identified. Management should develop procedures to ensure that volunteer tax assistants regularly remove taxpayer data from the hard drives of laptop computers and that the volunteers return the laptops to the IRS at the end of the filing season.

Management's Response: Management agreed with our findings and recommendations and provided specific actions aimed at increasing the security awareness of functional managers. The AWSS has implemented a Security Survey and Risk Assessment Program for all IRS facilities. This program should identify facility threats and weaknesses by applying a uniform risk assessment methodology to all facilities, and improve coordination with the GSA to resolve security vulnerabilities in multi-tenant buildings.

**Persistent Physical Security Vulnerabilities Should Be
Corrected to Better Protect Facilities and Computer Resources**

Management characterized our recommendations to assign accountability over laptop computers and taxpayer data used in the Volunteer Income Tax Assistor (VITA) program as not practical and not cost effective. The Director, Stakeholder Partnership, Education and Communication (SPEC), who is responsible for the VITA program, stated that SPEC territory managers are assigned the responsibility and accountability over laptops, and the Director is exploring methods of protecting data generated during the return filing process.

The Director indicated that returning the laptops to the IRS at the end of the filing season would not be practical and contravenes the Congressional mandate to increase the number of electronically filed returns. The Director further asserted that one of our recommendations would jeopardize the entire VITA program.

Office of Audit Comment: We agree with assigning accountability for VITA laptops to the SPEC territory managers. We also agree that SPEC managers should ensure that the VITA site coordinators reinforce the message to protect taxpayer data and government computers. However, the Director, SPEC, appears to be abdicating responsibility for safeguarding the laptops during the 8-month period between filing seasons. We believe the risk of theft or loss of taxpayer data and government equipment justifies the cost of controlling these assets. We also believe that the need to safeguard these assets does not contravene the Congressional mandate to increase the number of electronically filed returns.

In our opinion, management's assertion that our recommendation would jeopardize the VITA program is unreasonable. However, the alternatives management is exploring to protect taxpayer data on VITA laptop computers have merit. Our concern is that the implementation date for protecting taxpayer data on laptops is July 2002, meaning that the IRS will go through another filing season with the unnecessary risk of losing or compromising taxpayer data. In our opinion, corrective actions can and should be taken before January 2002.

Persistent Physical Security Vulnerabilities Should Be Corrected to Better Protect Facilities and Computer Resources

Objective and Scope

Our overall objective was to evaluate physical security controls over computer resources and data.

Our overall objective was to determine whether the Internal Revenue Service (IRS) had effective physical security controls to safeguard computer resources and data from the threat of misuse, loss, and damage.

We evaluated the IRS' compliance with requirements and guidelines issued by the IRS, the U.S. General Accounting Office (GAO) and the National Institute of Standards and Technology. Our review of controls included observation, interviews with both Information Technology Services (ITS) and Agency-Wide Shared Services (AWSS) personnel, and testing exterior and interior entry controls.

We performed this audit between October 2000 and December 2000 at the Tennessee Computing Center, and the Dallas, Phoenix, and two Manhattan offices. The audit was performed in accordance with *Government Auditing Standards*.

At each of the sites we visited, we evaluated the security of the building's perimeter and entrances, the security environment inside the building, and access to the computer and telecommunications equipment rooms. Details of our audit objective, scope, and methodology are presented in Appendix I. Major contributors to this report are listed in Appendix II.

Background

Effective physical security controls are essential to protecting computer systems, data and personnel.

Physical security controls provide for the protection of property, personnel, computer systems, and data, against unauthorized access, damage, sabotage, or other illegal or criminal acts. Certain federal agencies have recently incurred very damaging security breaches that can be traced to physical security weaknesses. These breaches may have led to the loss of property, the disruption of services and functions, and the unauthorized disclosure of sensitive documents and data.

Persistent Physical Security Vulnerabilities Should Be Corrected to Better Protect Facilities and Computer Resources

With the emphasis on customer service, telecommunications advances, and the wide use of laptop computers; taxpayer data are much more accessible in the IRS workplace. This new accessibility has also brought greater challenges for physically securing the data.

Physical security controls at the IRS have been the subject of numerous reviews.

The Treasury Inspector General for Tax Administration (TIGTA), the GAO and the IRS Office of Security Evaluation and Oversight (SEO) have reported on IRS physical security controls. The TIGTA has, most recently, included this subject in overall security reviews at three former district offices,¹ and identified several weaknesses. The GAO has been reporting for several years on computer security at the IRS. The Office of SEO regularly conducts reviews to ensure that IRS offices are in compliance with physical security standards and requirements. The IRS is also in the process of conducting vulnerability assessments and security surveys at its facilities, many of which have been completed. For this audit, we chose locations to complement the prior audit work.

Results

A lack of emphasis on physical security policies and procedures could allow intruders easy access to IRS facilities and computer resources.

IRS facilities remain vulnerable to intruders, explosive attacks, theft of computer resources, and unauthorized disclosure of taxpayer data. We identified several security weaknesses at the computing center and four other offices that could allow an intruder easy access to IRS facilities and computer resources. Specific examples of these conditions, where they were found, and the related causes are presented in Appendix IV.

¹ *Computer Security Controls Should Be Strengthened in the Houston District*, (Reference Number 2000-20-106, dated July 2000); *Computer Security Controls Should Be Strengthened in the Former Brooklyn District*, (Reference Number 2001-20-020, dated November 2000); *Computer Security Controls Should Be Strengthened in the Former Northern California District*, (Reference Number 2001-20-036, dated January 2001).

Persistent Physical Security Vulnerabilities Should Be Corrected to Better Protect Facilities and Computer Resources

Also, data on laptop computers could be better protected from theft and unauthorized disclosure.

The IRS has adequate policies and procedures for physical security. The procedures related to the issues in this report were not implemented for several reasons. Security policies and procedures have long been emphasized at the computing centers to a greater extent than at smaller offices, because of the amount and type of data physically stored there. Although employees (and intruders) at the smaller offices now have access to the same data via telecommunications, security at these facilities has not been emphasized to the same degree.

We also attributed the weaknesses we identified at all sites to insufficient security reviews by on-site physical security personnel, a lack of funding allocated for security improvements, and the need for improved coordination with the General Services Administration (GSA) at multi-tenant locations. Many of the conditions we noted had been identified in prior reviews but had not been corrected.

Controls Were Not Always Sufficient to Prevent Unauthorized Access to Buildings and Computer Resources

The first line of defense in protecting a facility and the resources within from intruders and building attacks are the security controls placed at the property line and building perimeter. While we recognize the difficulty in preventing access to a determined, experienced intruder, the IRS could strengthen controls to prevent most unauthorized accesses. We noted the following conditions.

Facilities were vulnerable to explosive attacks

The Consolidated Physical Security Standards for IRS Facilities (CPSS) provides a set of minimum physical security standards. The CPSS states that receptacles that could conceal explosives should be kept away from the

**Computer Security Controls Should Be
Strengthened in the Former Brooklyn District**

DRAFT



INSPECTOR GENERAL
for TAX
ADMINISTRATION

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

October 25, 2000

Response Date
November 24, 2000

MEMORANDUM FOR CHIEF INFORMATION OFFICER

FROM:

Scott E. Wilson

A handwritten signature of Scott E. Wilson in cursive script.

Associate Inspector General for Audit (Information Systems
Programs)

SUBJECT:

Draft Audit Report – Computer Security Controls Should Be
Strengthened in the Former Brooklyn District

Attached for your review and comments are two copies of the subject draft audit report. In summary, steps should be taken to strengthen the former Brooklyn District's controls to guard against and detect inappropriate accesses. Specifically, the Internal Revenue Service (IRS) can improve security controls over information systems in the following three areas: user account management, security surveillance, and physical security.

We would appreciate receiving your written response to the findings and recommendations in this draft report within 30 calendar days from the date of this memorandum. We are also providing copies of the report to the IRS managers who are affected by the report recommendations.

The Treasury Inspector General for Tax Administration (TIGTA) has designated this report as Limited Official Use (LOU) pursuant to Treasury Directive TD P-71-10, Chapter III, Section 2, "Limited Official Use Information and Other Legends" of the Department of Treasury Security Manual. Because this document has been designated LOU, it may only be made available to those officials who have a need to know the information contained within this report in the performance of their official duties. This report must be safeguarded and protected from unauthorized disclosure; therefore, all requests for disclosure of this report must be referred to the Disclosure Unit within the TIGTA's Office of Chief Counsel.

Please contact me at (202) 622-8510 if you have questions, or your staff may contact Steve Mullins at (925) 210-7024.

Attachments (2)

Draft

**Computer Security Controls Should Be
Strengthened in the Former Brooklyn District**

Table of Contents

Executive Summary	Page	i
Objective and Scope	Page	1
Background	Page	1
Results	Page	3
User Account Management	Page	3
Security Surveillance	Page	6
Physical Security	Page	7
Conclusion	Page	8
Appendix I - Detailed Objective, Scope, and Methodology	Page	9
Appendix II - Major Contributors to This Report	Page	13
Appendix III - Report Distribution List	Page	14

Draft

**Computer Security Controls Should Be
Strengthened in the Former Brooklyn District****Executive Summary**

Advances in information technology have caused the daily activities of the Internal Revenue Service (IRS) to become increasingly automated and inter-linked. These advances, while improving efficiency, have also increased the risk that hackers or dishonest employees could misuse taxpayer data. Malicious acts by employees present an even greater risk since they already have access to data via networks. The former Brooklyn District had over 1,000 employees connected to its local area network (LAN). On October 1, 2000, the Brooklyn District was realigned as part of the IRS' organizational modernization.

The overall objective of this review was to determine whether the former Brooklyn District had effective security controls over its computer systems to safeguard information against unauthorized access or use, disclosure, damage, modification, and loss. We reviewed controls over the former District's LAN with emphasis on the Taxpayer Advocate Management Information System (TAMIS)¹ to demonstrate the impact of security weaknesses. This review was part of a series of reviews initiated to assess the overall effectiveness of security controls over the IRS' information systems.

Results

The former District had various computer security controls in place which reduce the risk, to some degree, of unauthorized access and destruction of data. For example, logical access controls, such as user identification and passwords, were properly set up at the minicomputer and LAN level. Also, logical access to data on sensitive systems, such as the TAMIS, was correctly limited, and physical security was generally sufficient. However, additional steps in the following areas can further strengthen the computer security program:

User Account Management

LAN and TAMIS user accounts were not always cancelled when employees transferred or left the IRS. In addition, current employees were given unneeded access to the TAMIS, thus increasing the risk of unauthorized access to taxpayer information on the system. However, we did not identify any inappropriate activity by any of these users.

In addition, special capabilities to research the TAMIS had been granted to all TAMIS users, most of whom had no need for it. Those employees had the capability to browse data for over one million taxpayers without detection. We were unable to determine if such browsing occurred because controls were insufficient to detect this activity.

¹ The TAMIS is an automated system for processing and controlling Taxpayer Advocate Service cases.

Draft

Computer Security Controls Should Be Strengthened in the Former Brooklyn District

Security Surveillance

There was no documented monitoring of the TAMIS system or the LAN to identify who was logging on or what they did. While audit trails² were run on minicomputers, the TAMIS database application, and the LAN to detect improper system activity, there was no indication they had been reviewed. Essentially, the former District did not use audit trails to detect improper activity on its computer systems.

Physical Security

In general, physical security was sufficient to protect computer systems from damage or unauthorized access, and environmental controls were adequate in protecting taxpayer data. However, one concern was that the Information Systems (IS) Division is housed on a floor that is regularly accessed by taxpayers visiting a Collection Division interview unit, and we noted that keypads used to access this area were not shielded to prevent observation of the security code. A similar finding was reported by the National Headquarters Security, Evaluation & Oversight function during a district security review in 1998. We suggest using shields to increase access protection to the area.

Summary of Recommendations

The Chief Information Officer and the appropriate IRS operations executives need to take steps to address the specific weaknesses identified in this report. Actions management should take include: allowing only appropriate system permissions and annually reviewing employee access privileges; ensuring system access is promptly removed for departing employees; and training responsible employees on performing audit trail reviews.

² Audit trails are a control for detecting improper activity on computer systems. Generally, they should show who took the action, what they did, where they did it, and when.

Draft

Computer Security Controls Should Be Strengthened in the Former Brooklyn District

Objective and Scope

Our objective was to determine whether the former Brooklyn District had effective security controls over its computer systems to safeguard information against unauthorized access or use, disclosure, damage, modification, and loss.

The overall objective of this review was to determine whether the Internal Revenue Service's (IRS) former Brooklyn District had effective security controls over its computer systems to safeguard information against unauthorized access or use, disclosure, damage, modification, and loss.

We visited the District from April to June 2000. Over 1,000 employees have access to the former District's local area network (LAN), approximately 30 of whom have access to taxpayer information through the Taxpayer Advocate Management Information System (TAMIS).¹ We selected and reviewed TAMIS controls to demonstrate the impact of security weaknesses.

During our visit, we reviewed user account management, security surveillance, physical security, and logical access controls for the LAN, minicomputers, and the TAMIS. We performed this review 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

The purpose of computer security is to protect an organization's valuable resources, such as information, hardware, and software. Through the selection and application of appropriate safeguards, security helps the organization meet its mission by protecting its physical and financial resources, reputation, legal position, employees, and other tangible and intangible assets.

¹ The TAMIS is an automated system for processing and controlling Taxpayer Advocate Service cases.

Draft

Computer Security Controls Should Be Strengthened in the Former Brooklyn District

Physical and logical access controls, restricting users' privileges, and monitoring system activity are all tools to help ensure adequate security.

The IRS, along with other high-profile government agencies and corporations, is at risk of outsiders' efforts to break into its computer systems. Advances in information technology have caused the daily activities of the IRS to become increasingly automated and inter-linked. These advances, while improving efficiency, have also increased the risk that hackers or dishonest employees could misuse taxpayer data. Malicious acts by employees present an even greater risk since they already have access to networks, in addition to being physically located where the computers are housed.

Achieving adequate security depends on properly applying several types of controls. These can be categorized into the following four groups:

- User Account Management – Manual processes to grant computer access privileges. Access should be granted to only those employees who need it to perform their official duties.
- System Security Surveillance – Processes to log and monitor computer system activities for indications of security violations as well as to timely respond to such incidents.
- Physical Security – Controls to limit physical access to computer system components (workstations, servers, and networks) to only those who are authorized and to provide a suitable physical environment which protects computer system components from man-made and natural hazards.
- System Logical Access – Computer system controls, such as password verification, to restrict access to computing resources.

The Congress recognized the significance of maintaining adequate information system security in the IRS Restructuring and Reform Act of 1998.² This law directs the Treasury Inspector General for Tax Administration (TIGTA) to report to the Congress an assessment of the

² Pub. L. No. 105-206, 112 Stat. 685.

Draft

Computer Security Controls Should Be Strengthened in the Former Brooklyn District

adequacy and security of the IRS' information technology. This report is part of TIGTA's effort to provide that assessment.

Results

Although various controls in place reduced risks to some degree, additional steps can strengthen the computer security program.

The former Brooklyn District has various computer security controls in place which reduce the risk, to some degree, of unauthorized access and destruction of data. For example, logical access controls, such as user identification and passwords, were properly set up at the minicomputer and LAN level. Logical access to data on sensitive systems, such as the TAMIS, was correctly limited, and physical security was generally sufficient.

However, additional steps can strengthen the computer security program. User accounts were assigned to employees who did not need access to the LAN and the TAMIS. In addition, security surveillance was not sufficient to detect improper computer activity. While physical security was sufficient, we noted one weakness that should be corrected. These conditions increase the risk that sensitive taxpayer data could be improperly disclosed or misused, possibly to commit fraud or other crimes.

User Account Management

Managers should restrict access to computer data to only those users who need it to carry out their duties. Because employees' responsibilities often change, managers should periodically check to ensure that access to taxpayer data is proper, based on employees' current assignments. Employees must be removed promptly from systems and applications which they do not need to access.

Users were given unneeded access to the LAN and the TAMIS.

Twenty-four employees who separated from the District between April 1999 and March 2000, continued to have access to the LAN. Access was also not cancelled for

Draft

Computer Security Controls Should Be Strengthened in the Former Brooklyn District

12 TAMIS users when they left the IRS or transferred to other functions. Some managers were not aware that a form was required to cancel employees' accesses. Other managers were not aware that their employees had access.

In addition, managers erroneously assigned TAMIS user accounts to 19 of the 40 users who did not need access to the system. None of the 19 had ever logged on to the system for periods up to 4 years. Managers did not detect the unneeded access privileges because the required annual certification reviews were not performed.

However, we did not identify any inappropriate activity by any of these employees.

In some instances, TAMIS managers did not timely re-assign the separating employees' workloads. They erroneously believed that the user accounts could not be cancelled as long as inventory was still assigned. The local Taxpayer Advocate is now aware that inventories of separating employees should be reassigned and user accounts cancelled as soon as employees no longer require access.

During our review of who had the ability to use the query capability of the system, we determined that all TAMIS users, regardless of permission level, could use query software through the TAMIS menu. This software enables users to research the database and create customized reports. It can be used when regular reports do not provide the required data.

Query software gives users access to personal information for over one million taxpayers on the TAMIS. Most of the users having this access did not need it, in our opinion.

The software also enables users to browse the personal information of over one million taxpayers, allowing the possibility of illegal activity. Managers did not give adequate weight to this risk by allowing employees this capability. We believe that most of the users had no need for this application.

Draft

Computer Security Controls Should Be Strengthened in the Former Brooklyn District

It is especially critical to limit and monitor the use of query software because managers have no audit trails³ to detect unauthorized use. The TAMIS application does not capture query software activity, and the operating system captures only system-level activity, such as when a user enters or exits the software. Because of the insufficient audit trail information, we were unable to detect whether any inappropriate usage of query software occurred.

Recommendations

The Chief Information Officer, in conjunction with the appropriate IRS operations executives, should:

1. Develop procedures to ensure that all managers annually review employee access to information systems and certify that the access and permissions are appropriate.
2. Remind managers of requirements for removing access privileges for departing employees.
3. Revise the current TAMIS so that query software capability is restricted only to those needing such access. Ensure that annual reviews of user account access and permissions include query software access.

³ Audit trails are a control for detecting improper activity on computer systems. Generally, they should show who took the action, what they did, where they did it, and when.