

**Improvements Are Needed to Prevent
the Potential Disclosure of
Confidential Taxpayer Information**

December 2002

Reference Number: 2003-40-022

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



DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

INSPECTOR GENERAL
for TAX
ADMINISTRATION

December 19, 2002

MEMORANDUM FOR CHIEF, COMMUNICATIONS AND LIAISON

Gordon C. Milbourn III

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

SUBJECT: Final Audit Report - Improvements Are Needed to Prevent the
Potential Disclosure of Confidential Taxpayer Information
(Audit # 200240045)

This report presents the results of our review to assess the Internal Revenue Service's (IRS) controls over the access to, disclosure of, and use of social security numbers (SSN) by third parties.

The Privacy Act¹ and other statutes regulate the government's use of SSNs. Internal Revenue Code (I.R.C.) Section (§) 6103² governs the disclosure of information contained in a tax return, including SSNs, to third parties. I.R.C. § 6103 establishes a number of requirements that must be met before this information can be disclosed. The Chairman of the House Ways and Means Subcommittee on Social Security asked the Social Security Administration Office of the Inspector General and the President's Council on Integrity and Efficiency to look at how federal agencies distribute and control SSNs.

In summary, the IRS provides information required by the Privacy Act and has established procedures to help ensure third parties, such as government agencies and private contractors, safeguard taxpayer information. In addition, the IRS conducts on-site safeguard reviews of the agencies receiving taxpayer information every 3 years, as required.

However, a review of the IRS' disclosure procedures and a judgmental sample of IRS agreements with federal and state agencies and private contractors receiving tax

¹ Privacy Act of 1974, 5 U.S.C. § 552a (1994 & Supp. IV 1998).

² I.R.C. § 6103 (2001).

information from the IRS during Calendar Year 2001 indicated the IRS needs to make improvements to its safeguard processes and procedures. Safeguards are needed to prevent the potential disclosure of taxpayer information protected by I.R.C. § 6103. In addition, federal and state agency safeguard activity reports and IRS safeguard review reports are not always timely. Procedures for disclosing federal tax information to private contractors also are not always effective.

Management's Response: The IRS agreed with the recommendations in the report. Specifically, the IRS indicated it is in the process of working with Chief Counsel on the legal implications of the transmission of taxpayer identification numbers to the Office of Child Support Enforcement (OCSE). The IRS also stated that it would examine its procedures for protecting the transmission of federal tax information and make needed changes. In addition, the IRS is in the process of revising its safeguard review process and safeguard review procedures. The IRS will also revise its internal safeguard and contract procedures, and review all applicable contractual clauses and its educational portfolio for contractors to ensure they are clear, concise, and consistent.

While the IRS agreed with the recommendations in the report, it questioned our conclusion that the transmission of Employer Identification Numbers (EIN) is not allowed under the law. We agree that the transmission of federal tax information is not prohibited under I.R.C. § 6103(l)(6)(A). However, we believe that the transmission of the EINs to the OCSE was in error and created a potential risk of disclosure, requiring the IRS to make improvements to its safeguard processes and procedures.

Copies of this report are also being sent to the IRS managers who are affected by the 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.

Improvements Are Needed to Prevent the Potential Disclosure of Confidential Taxpayer Information

Table of Contents

Background	Page 1
Significant Steps Have Been Taken to Protect Taxpayer Information	Page 2
Improvements Are Needed to Ensure Taxpayer Information Is Not Potentially Disclosed to Third Parties	Page 5
<u>Recommendations 1 through 3:</u>	Page 12
<u>Recommendations 4 and 5:</u>	Page 13
<u>Recommendation 6:</u>	Page 14
Appendix I – Detailed Objective, Scope, and Methodology	Page 15
Appendix II – Major Contributors to This Report.....	Page 18
Appendix III – Report Distribution List	Page 19
Appendix IV – Outcome Measures	Page 20
Appendix V – Laws and Regulations Governing Disclosure of Social Security Numbers	Page 22
Appendix VI – Management’s Response.....	Page 25

Improvements Are Needed to Prevent the Potential Disclosure of Confidential Taxpayer Information

Background

The Social Security Administration (SSA) created the Social Security Number (SSN) in 1936 as a means of tracking worker's earnings and eligibility for Social Security benefits. However, over the years, the SSN has become a "de facto" national identifier used by federal agencies, state and local governments, and private organizations.

The expanded use of the SSN as a national identifier provides a tempting motive for unscrupulous individuals to acquire an SSN and use it for illegal purposes. While no one can fully prevent SSN misuse, federal agencies have a responsibility to limit the risk of unauthorized disclosure of SSN information. To that end, the Chairman of the House Ways and Means Subcommittee on Social Security asked the SSA Office of the Inspector General and the President's Council on Integrity and Efficiency to look at how federal agencies distribute and control SSNs.

The Privacy Act¹ was enacted in 1974 to regulate federal agencies' collection, use, distribution, and maintenance of personal information about individuals that would include their SSNs. As part of this Act, each agency is required to disclose to the public the authority that allows the agency to ask for the information and whether supplying that information is mandatory or voluntary. Each agency is also required to explain the routine uses that may be made of the information provided.

Internal Revenue Code (I.R.C.) Section (§) 6109² requires that individual taxpayers provide their SSN when filing a tax return. Under I.R.C. § 6103,³ tax returns and return information (referred to as federal tax information or FTI), such as an individual's SSN, shall be confidential. The Internal Revenue Service (IRS) can disclose the information on a tax return to third parties only if it is authorized under the I.R.C. Certain requirements must be met and maintained before this information can be released. Unauthorized disclosures can result in criminal penalties, if

¹Privacy Act of 1974, 5 U.S.C. § 552a (1994 & Supp. IV 1998).

²I.R.C. § 6109 (2001).

³I.R.C. § 6103 (2001).

Improvements Are Needed to Prevent the Potential Disclosure of Confidential Taxpayer Information

found to be willful.⁴ Taxpayers may also sue for damages.⁵ See Appendix V for a list of the laws and regulations that govern the use and disclosure of SSNs.

Taxpayers need to be assured that their tax information is protected and properly used. This assurance is vital to the success of the nation's voluntary tax system. Taxpayers must have the confidence that sensitive personal and financial information provided to the IRS is protected at all times against unauthorized use, inspection, or disclosure.

This audit was performed between February and July 2002 and included testing in the Office of Governmental Liaison and Disclosure and the Office of Procurement in the IRS' National Headquarters. The audit was conducted in accordance with *Government Auditing Standards*.

The scope of this audit was limited to those IRS procedures and the laws and regulations that govern the distribution of FTI to government agencies and private contractors. Our review did not include an assessment of the IRS' procedures for disclosing FTI to other third party entities such as tax practitioners. Detailed information on our audit objective, scope, and methodology is presented in Appendix I. Major contributors to the report are listed in Appendix II.

Significant Steps Have Been Taken to Protect Taxpayer Information

The IRS provides the information required by the Privacy Act in the individual tax return instructions. In addition, the IRS has established procedures that third parties, such as agencies and private contractors, must follow to ensure that taxpayer information is being safeguarded.

The IRS is complying with the Privacy Act

The Privacy Act requires that the IRS advise taxpayers what legal right the IRS has to ask for personal information, such as an SSN, why the IRS needs that information, and how the IRS uses the information. The IRS provides this information in the instructions for individual tax returns. The IRS also provides this information when contacting taxpayers concerning audits of their tax returns or when it

⁴ I.R.C. § 7213 (2001).

⁵ I.R.C. § 7431 (2001).

Improvements Are Needed to Prevent the Potential Disclosure of Confidential Taxpayer Information

questions taxpayers about discrepancies in the income that they reported on their tax returns.

The IRS has taken additional steps to protect the privacy of individuals' SSNs. To address a longstanding privacy concern of the Congress, the IRS removed individuals' SSNs from the peel-off labels that were contained in the tax return instruction booklets mailed to taxpayers. This change became effective for taxpayers filing their 1998 tax returns.

The IRS has also taken measures to protect the taxpayer identification numbers (TIN) of individuals who prepare tax returns (return preparers). Return preparers had been required to include their SSNs on those returns they prepared. The Congress, concerned about the potential inappropriate use of SSNs, included a provision in the IRS Restructuring and Reform Act of 1998 (RRA 98)⁶ authorizing the IRS to provide alternatives to return preparers. The IRS subsequently developed a process that allows return preparers to apply for a separate preparer taxpayer identification number (PTIN). Return preparers were able to use PTINs beginning in Tax Year 1999.

Written agreements are required from other agencies when FTI is shared

In addition to the Privacy Act, I.R.C. § 6103 governs the disclosure of information contained in a tax return, including individuals' SSNs, to other agencies and third parties. Under I.R.C. § 6103, the IRS can disclose FTI to other agencies if the agencies meet certain requirements. One of these requirements is that certain agencies must enter into a written agreement with the IRS before the information can be shared.

A review of 73 basic agreements between the IRS and agencies receiving FTI from the IRS indicated the IRS required those agencies to enter into written agreements for the sharing of FTI, as the law specifies. These agreements provided a number of procedures and safeguards the

⁶ 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.).

Improvements Are Needed to Prevent the Potential Disclosure of Confidential Taxpayer Information

agencies agreed to follow in order to receive FTI from the IRS.

The IRS helps ensure compliance by performing safeguard reviews at least every 3 years

To ensure each agency receiving FTI from the IRS is complying with the safeguarding requirements, the IRS regularly performs on-site evaluations of the agencies. IRS procedures require it to perform a safeguard review every 3 years of each agency receiving FTI. Our analysis of IRS safeguard reviews of 51 state government assistance agencies⁷ showed that the IRS performed the required reviews every 3 years for 46 (90 percent) of the 51 agencies.

The IRS has established safeguard procedures for contractors to follow to protect taxpayer information

The IRS has also established procedures to safeguard information disclosed under I.R.C. § 6103(n) to contractors for the purposes of carrying out their contracts.

Treas. Reg. § 301.6103(n)-1(d) allows the IRS to prescribe any conditions and requirements that must be followed in order to safeguard FTI. These requirements can be specified by regulation, in published rules or procedures, or in written communications. Examples of the requirements the IRS has established include:

- Contractors may use the FTI only for the sole purpose of performing the terms of the contract.
- Contractors must properly account for, store, and protect FTI in accordance with prescribed standards.
- Contractors may not subcontract any work involving FTI without prior written approval from the IRS.
- The IRS has the right to make on-site inspections of the contractor's facilities and operations in order to ensure FTI is being safeguarded.

⁷ This includes the governments of Puerto Rico and the United States (U.S.) Virgin Islands. In addition, some states have more than one government assistance agency.

Improvements Are Needed to Prevent the Potential Disclosure of Confidential Taxpayer Information

In a judgmental sample of nine contract actions⁸ where SSNs could be disclosed to the contractor, the safeguard clauses were included, as required.

The IRS' internal procedures, coupled with the requirements set forth in I.R.C. § 6103, provide some assurance that FTI was not potentially disclosed. This assurance is vital to taxpayers' compliance with the nation's voluntary tax system.

Improvements Are Needed to Ensure Taxpayer Information Is Not Potentially Disclosed to Third Parties

While the IRS is generally complying with the requirements in I.R.C. § 6103 and its own internal procedures to protect taxpayer information, it is not always following all the requirements. In some cases, the IRS' internal procedures are in conflict with the laws and regulations governing the disclosure of FTI to third parties.

Reviews of the IRS' processes and procedures for monitoring federal and state agencies and private contractors identified several areas where improvements can be made.

- Safeguard procedures do not always identify potential disclosures of data that are not authorized under I.R.C. § 6103.
- Federal and state agency safeguard activity reports (SAR) and IRS safeguard review reports (SRR) are not always timely.
- Procedures for disclosure of FTI to private contractors are not always effective.

Each of the conditions reduces the IRS' assurance that FTI, including SSNs, is being protected from potential disclosure. These conditions could also undermine taxpayers' confidence in the IRS' ability to protect the confidentiality of their personal information.

⁸ "Contract actions" refer to contracts, interagency agreements, task orders, delivery orders, purchase orders, and contract modifications.

Improvements Are Needed to Prevent the Potential Disclosure of Confidential Taxpayer Information

Safeguard procedures do not always identify potential disclosures not authorized under I.R.C. § 6103

Based upon a review of the laws and IRS procedures and discussions with officials from the U.S. Department of Health and Human Services (HHS), the Treasury Inspector General for Tax Administration (TIGTA) advised the IRS that TINs⁹ were apparently provided in error to the HHS' Office of Child Support Enforcement (OCSE). The IRS subsequently confirmed this was occurring and that it had resulted in an estimated 27.6 million TINs on Wage and Tax Statements (Form W-2) being transmitted to the OCSE between June 1997 and May 2002. Once we brought it to the IRS' attention, the IRS advised the TIGTA that it took immediate action to correct the error.

A senior IRS executive stated the following (paraphrased and summarized):

We [the IRS] estimate the transmission of 27.6 million TINs included approximately 1.1 million unique EINs. This estimate includes duplicate requests that were made, for example, to obtain updated addresses or income information, but we cannot quantify these duplications from the available data.

We also cannot ascertain precisely what ratio of SSNs to EINs was actually experienced over the last 5 years because neither the OCSE nor we retained the information transmitted. There have been wide variances in the OCSE requests, from monthly requests of 320 to almost 2 million. Consequently, an analysis of sample data, even if it were available, would not likely produce a very precise estimate.

Nevertheless, we calculated the 1.1 million unique TINs using a weighted average of the most current available census data on

⁹ The TIN may be an SSN or Employer Identification Number (EIN) issued by the IRS.

Improvements Are Needed to Prevent the Potential Disclosure of Confidential Taxpayer Information

employment by employer size (1999). This provided a rough approximation of about 25 employees per employer. On that basis, we estimate the transmission of 27.6 million TINs to OCSE over the 5-year period included approximately 1.1 million unique EINs (27.6 million/25 = 1.1 million).

The law allows the IRS to provide taxpayer information to child support enforcement agencies for the purpose of locating persons owing child support and establishing and collecting such support.¹⁰ OCSE officials advised us that the IRS provides information to them on a cartridge. The OCSE has one of their employees transport the cartridge to a Social Security Administration (SSA) facility.¹¹ The information is then downloaded from the cartridge to a designated section of a computer system and subsequently transmitted electronically to the individual child support enforcement agencies. The OCSE also advised us that it only keeps the information the IRS provides until it is assured that the data has been successfully transmitted to the individual agencies.

The I.R.C. § 6103(l)(6)(A) allows the following,

“The Secretary [of the Treasury] may, upon written request, disclose to the appropriate Federal, State, or local child support enforcement agency – (ii) available return information reflected on any return filed by, or with respect to, any individual described in clause (i) relating to the amount of such individual’s gross income (as defined in section 61) or consisting of the names and addresses of payors of such income and the names of any dependents reported on such return, but only if such return information is not reasonably available from any other source.”

¹⁰ I.R.C. § 6103(l)(6) (2001).

¹¹ The OCSE advised us that it contracts with the SSA to process the cartridges.

Improvements Are Needed to Prevent the Potential Disclosure of Confidential Taxpayer Information

Further, as stated in an October 2000 Treasury report to the Congress, “It should be noted that employer identification numbers are not included in the list of items that may be disclosed under section 6103(l)(6)(A)(ii).”¹²

We did not conduct specific testing to validate the number of TINs transmitted or to determine why this error occurred; however, tests indicate that the IRS’ current safeguard reporting and review requirements would not identify this type of error. The IRS requires agencies to file a number of safeguard reports and conducts safeguard reviews of those agencies to ensure proper steps are taken to protect FTI. These procedures do not include determining whether agencies are receiving only the FTI they are authorized to receive.

Federal and state agency SARs and IRS SRRs are not always timely

A review of a judgmental sample of federal and state agencies receiving FTI from the IRS during Calendar Year (CY) 2001 showed that agencies were not timely filing SARs with the IRS. In addition, the IRS was not timely issuing interim reports on safeguard reviews of these agencies.

The IRS requires that federal, state, and local agencies¹³ file a SAR with the IRS every year. The SAR provides information on an agency’s efforts to ensure the confidentiality of FTI received from the IRS. It also certifies that the agency is meeting its requirements to protect the information in accordance with I.R.C. § 6103.

Most agencies are required to file the SAR for the calendar year by January 31 of the following year.¹⁴ A review of a judgmental sample of 91 agencies showed that a SAR was not filed timely by 35 agencies (38 percent). For 17 of the

¹² Office of Tax Policy, Department of the Treasury, *Scope and Use of Taxpayer Confidentiality and Disclosure Provisions. Volume I: Study of General Provisions*, October 2, 2000, p. 83.

¹³ This includes governments outside the U.S., such as Guam, Puerto Rico, and the U.S. Virgin Islands.

¹⁴ State government assistance agencies are required to file SARs by September 30 for the processing year (July 1 through June 30).

Improvements Are Needed to Prevent the Potential Disclosure of Confidential Taxpayer Information

agencies, they had not filed a SAR for 2001 and it had been more than 1 year since the last one was filed.

In addition to requiring that agencies file SARs, IRS procedures require it to conduct an on-site safeguard review of each agency at least every 3 years to evaluate whether an agency complied with the legal requirements to protect the FTI it received from the IRS. The review is to include determining if:

- The information is securely stored.
- Access is restricted to only authorized employees.
- Agency employees fully understand their disclosure responsibilities and the penalties that apply for failure to protect information.

After the review, the IRS is to meet with the agency to discuss concerns and deficiencies, and an interim SRR is to be issued within 45 calendar days of the review. The IRS advised us that it requests that the agency begin taking action to correct any deficiencies identified at this meeting rather than waiting for the interim SRR to be issued.

The interim report serves as a record of deficiencies that are to be formally addressed by the agency. The agency is given an opportunity to respond to the interim SRR. The reviewed agency's comments and the IRS' response are incorporated into the SRR, and a final report is issued.

A review of a judgmental sample of 96 agencies indicated the IRS did not timely issue interim SRRs in 58 (60 percent) of the agencies reviewed. A separate analysis of the 52 government assistance agencies included in the 96 agencies reviewed showed that issuance of interim SRRs took an average of 139 days and ranged from 4 days to 672 days.

The law allows the IRS to discontinue sharing information with an agency if proper safeguards are not in place.¹⁵ The SRR serves as a written record supporting such a decision. These reports also provide the foundation for the IRS'

¹⁵ I.R.C. § 6103(p)(4) (2001).

Improvements Are Needed to Prevent the Potential Disclosure of Confidential Taxpayer Information

annual report to the Congress summarizing whether agencies are providing the proper safeguards to protect taxpayer information. Without the timely issuance of safeguard reports, the Congress may not be receiving an adequate assessment of the IRS' protection of taxpayer information.

The IRS does not have adequate staffing to effectively implement all the safeguard procedures required by I.R.C. § 6103. The IRS' Headquarters Safeguard Office has a staff of 8 employees¹⁶ who are responsible for ensuring 185 agencies comply with the safeguarding requirements.¹⁷ This includes reviewing SARs and procedure reports and performing safeguard reviews of each of the agencies. This Office also has the responsibility for inspections and safeguard reviews for some of the private contractors, as well as oversight responsibility for the safeguard review program nationwide.

Procedures for disclosure of FTI to private contractors are not always effective

A review of the laws, regulations, IRS' internal procedures, and corresponding publications indicated that the IRS does not have clear and consistent procedures to ensure that FTI provided to private contractors by the IRS was properly protected.

- The IRS is required to inspect the facilities of *major* contractors who receive confidential FTI if certain other criteria are met. However, the IRS does not define what would cause a contractor to be considered a major contractor. A limited review of nine contract actions where the contractors were authorized to receive SSNs during CY 2001 showed the IRS had not performed any inspections of contractor facilities for two contract actions that should have been considered significant or major (considering the number of SSNs that were being provided to the contractors). In CY 2001, the IRS provided a total of over 200,000 SSNs in these

¹⁶ Four contractors from a private company provide additional assistance for a portion of the safeguard reviews.

¹⁷ The IRS provided these data; we did not validate their accuracy.

Improvements Are Needed to Prevent the Potential Disclosure of Confidential Taxpayer Information

2 contract actions.¹⁷ The SSNs were submitted to the contractors who in turn provided electronic information on those taxpayers that the IRS needed. The IRS did not inspect the facilities and, therefore, has no assurance that the contractors adhered to the safeguard clauses to protect taxpayer SSNs.

- Using I.R.C. § 6103(p)(4) as criteria for its safeguard procedures, the IRS requires contractors to securely store and restrict access to information in order to receive FTI. However, this provision of the law does not apply to private contractors unless it was specifically written into the terms of the contract. The IRS Acquisition Procedure does not require that all the elements of I.R.C. § 6103(p)(4) be in the contract.

This discrepancy resulted in the inconsistent treatment of contractors. For example, the IRS recommended in a SRR that a contractor prepare safeguard procedure and activity reports in accordance with I.R.C. § 6103(p)(4). The contractor notified the IRS that it was not required to comply since this was not part of the contract with the IRS. The IRS agreed and revised its recommendation. However, other contractors are complying with I.R.C. § 6103(p)(4) regardless of whether it was specifically included in the wording of their contract.

- The IRS' safeguarding procedures treat private contractors and agencies similarly. The IRS referred private contractors to *Tax Information Security Guidelines for Federal, State, and Local Agencies* (Publication 1075) for guidance on what should be included in a SAR. However, the most current version, published in June 2000, provides details only on the requirements of I.R.C. § 6103(p)(4) for agencies in most sections of the publication. It does not include contractors in these sections.

Treas. Reg. § 301.6103(n)-1(d) states that those authorized to receive confidential return information must comply with all applicable conditions and requirements prescribed by the IRS for the purposes of protecting the confidentiality of returns and return information and preventing disclosures of

Improvements Are Needed to Prevent the Potential Disclosure of Confidential Taxpayer Information

returns or return information. In addition, the Congress is considering new laws to require federal and state agencies to conduct annual on-site reviews of all contractors working for those agencies that receive FTI. Under proposed legislation, each agency will be required to furnish the IRS with a report of its findings in these reviews and annually certify that all contractors are in compliance with the requirements to safeguard taxpayer information.

Recommendations

The Chief, Communications and Liaison, should:

1. Consult with the Office of Chief Counsel to determine the legal implications of the IRS' transmission of TINs to the OCSE.

Management's Response: The IRS agreed with the recommendation and has already contacted Chief Counsel. Chief Counsel will determine the implications of the information set forth in this report. Additional factual development is ongoing, as is Counsel's consideration of applicable law. Once the IRS receives a response from Counsel, it will determine if any further action is necessary.

2. Evaluate the safeguard procedures to ensure the procedures address the content as well as the security of information shared under I.R.C. § 6103.

Management's Response: The IRS agreed with the recommendation and has initiated several activities that it believes will address this issue as it relates to authorized government FTI recipients, such as OCSE. The IRS plans to examine its procedures to prevent inadvertent transmissions and readily detect such occurrences of inadvertent transmissions.

3. Evaluate whether staffing levels are sufficient to ensure that third parties receiving FTI from the IRS are in compliance with the safeguarding requirements.

Management's Response: The IRS acknowledged that without additional staff or a change in its approach to safeguard reviews, the existing workload exceeds the capacity of the Safeguard Office. In a June 2001 report, an

Improvements Are Needed to Prevent the Potential Disclosure of Confidential Taxpayer Information

outside contractor benchmarking the safeguard program recommended that the safeguard review approach be modified to prioritize the agency review schedule based on the relative risk level assigned to each agency. As a result, in 2002 the IRS engaged an outside contractor to develop risk assessment guidelines for site selection and to begin building a foundation for self-certification, third party certification, or other best practice methodology.

4. Revise the IRS safeguard procedures to provide specific criteria on which contractors should have their facilities inspected and to ensure that these inspections are made.

Management's Response: The IRS agreed with the recommendation that the safeguard procedures be revised to provide more specific criteria. It is in the process of revising its Internal Revenue Manual, and will review the current methodology for contractor inspection and explore the feasibility of contractor selection for more detailed safeguard reviews based upon the relative risk level assigned to the contractor. The IRS will review the contractors the TIGTA identified and take appropriate corrective action when necessary.

5. Work with the Office of Procurement to revise internal safeguard and contract procedures to ensure they are in agreement and are in compliance with the appropriate laws concerning private contractors.

Management's Response: The IRS agreed with the recommendation and plans to work with Agency-Wide Shared Services, Office of Procurement, to revise internal safeguard and contract procedures to ensure they comply with the appropriate laws concerning private contractors.

The IRS has identified business needs that it can integrate into its recent web systemic applications and procedures in its contracting functions. The Office of Governmental Liaison and Disclosure will focus on enhancements and improvements to revise and upgrade internal safeguard contract provisions for the Office of Procurement contractors.

Improvements Are Needed to Prevent the Potential Disclosure of Confidential Taxpayer Information

6. Provide clear guidance to private contractors on the safeguard requirements and their responsibilities under those requirements.

Management's Response: The IRS will review all of the applicable contractual clauses and its educational portfolio to ensure they are clear, concise, and consistent.

Improvements Are Needed to Prevent the Potential Disclosure of Confidential Taxpayer Information

Appendix I

Detailed Objective, Scope, and Methodology

The overall objective of this review was to assess the Internal Revenue Service's (IRS) controls over the access to, disclosure of, and use of social security numbers (SSN) by third parties. To accomplish our objective, we:

- I. Determined whether the IRS made legal and informed disclosures of SSNs to governmental agencies.
 - A. Interviewed officials from the IRS Office of Governmental Liaison and Disclosure to determine if the IRS provided SSNs to agencies and what controls or safeguards existed to ensure that only authorized SSNs were provided and that those SSNs were adequately protected.
 - B. Reviewed income tax laws, Treasury Regulations, IRS tax forms and publications, and IRS procedures to understand the provisions that allow for disclosures of SSNs and how the IRS informed the public as required by law.
 - C. Reviewed 73 of the 88 written agreements between the IRS and state and local tax agencies¹ that the law requires² before the IRS can provide federal tax information (FTI) to these agencies, to determine that safeguards were included in those agreements that ensured FTI, including SSNs, was protected. We determined that review of the remaining 15 agreements was unnecessary.
 - D. Selected a judgmental sample of 96 state agencies³ from the 115 agencies that receive FTI to administer either child support enforcement or government assistance programs to determine if agencies were filing timely safeguard activity reports (SAR) and to determine if the IRS issued timely safeguard review reports (SRR).

The sample included all 60 government assistance agencies. The remaining 36 agencies represented the state agencies assigned to the IRS Headquarters Safeguard Office at the time of our on-site visit. We reviewed documentation to assess the timeliness of SARs for 82 of the agencies sampled. We excluded 14 agencies not receiving tax return information at the time of our review because they had not met all of the legal requirements. We determined the timeliness of the interim SRRs in 88 of the agencies sampled. We excluded eight agencies as we did not have sufficient information to determine if the SRRs were timely. We also

¹ Includes the governments of Puerto Rico and the United States (U.S.) Virgin Islands.

² Internal Revenue Code Section 6103(d)(1) (2001).

³ Includes the governments of Guam, Puerto Rico, and the U.S. Virgin Islands.

Improvements Are Needed to Prevent the Potential Disclosure of Confidential Taxpayer Information

determined whether safeguard reviews were being performed every 3 years for 51 of the 60 government assistance agencies. We were not able to review sufficient documentation to make a determination for nine of the agencies.

- E. Selected a judgmental sample of 9 federal agencies from the 39 different federal agencies that receive FTI under various provisions of I.R.C. § 6103 to determine if those agencies were filing timely SARs and to determine if the IRS was performing timely safeguard reviews. We limited the sample to nine agencies due to limited audit resources.

The sample was selected based upon either the number of disclosures of FTI an agency received annually, or because it was one of the federal agencies whose Inspector General was part of the President's Council on Integrity and Efficiency. The original sample consisted of 12 federal agencies. We subsequently eliminated three of the federal agencies from this sample because we determined that the agency did not actually receive individuals' SSNs from the IRS, the agency received individuals' SSNs under the provision for contractors that was tested under Sub-Objective II, or the agency no longer receives a significant number of individuals' SSNs. We were also unable to determine if the interim SRRs were timely for one of the remaining nine agencies because we did not have sufficient documentation to make that determination.

- II. Determined whether the IRS has appropriate controls over contractors' access to and use of SSNs.

- A. Interviewed officials from the IRS Offices of Governmental Liaison and Disclosure and Procurement to determine if SSNs were provided to private contractors, what laws allowed for such disclosures, and what procedures existed to ensure that SSNs are safeguarded.
- B. Reviewed income tax laws, Treasury Regulations, and IRS publications and procedures to understand the provisions that allow for disclosures of SSNs to contractors.
- C. Reviewed a judgmental sample of nine contract actions⁴ for private contractors where the contract allowed for SSNs to be provided to the contractors to determine if the proper safeguard clauses were included in the contracts. Additional contract actions were not selected due to audit staff availability.

The IRS Office of Procurement provided us with the universe of 37 contract actions made during Calendar Year 2001 where the private contractor was authorized to

⁴ "Contract actions" refer to contracts, interagency agreements, task orders, delivery orders, purchase orders, and contract modifications.

Improvements Are Needed to Prevent the Potential Disclosure of Confidential Taxpayer Information

- receive SSNs as part of the contract action.⁵ Some of the private contractors were represented on more than one contract action. For the purposes of our sample, a contractor was selected only once. In addition, we selected our sample to include those contract actions where the potential for a large number of SSN disclosures appeared to exist. One contract action was selected because the responsibility in the IRS for executing it existed outside the IRS National Headquarters.
- D. Reviewed IRS SRRs for four private contractors to determine whether the IRS was monitoring contractor compliance with the safeguarding requirements and whether the IRS was correctly and consistently ensuring compliance. This represented the entire population of SRRs for private contractors at the IRS Headquarters Safeguard Office available for review at the time of our on-site visit.

⁵ This information was not validated.

**Improvements Are Needed to Prevent the Potential Disclosure
of Confidential Taxpayer Information**

Appendix II

Major Contributors to This Report

Michael R. Phillips, Assistant Inspector General for Audit (Wage and Investment Income Programs)

Augusta R. Cook, Director

Deann L. Baiza, Audit Manager

John L. Hawkins, Senior Auditor

Alan D. Lund, Senior Auditor

Robert A. Baker, Auditor

Improvements Are Needed to Prevent the Potential Disclosure of Confidential Taxpayer Information

Appendix III

Report Distribution List

Acting Commissioner N:C
Deputy Chief, Communications and Liaison CL
Director, Business Systems Development M:I:B
Director, Disclosure CL:D
Director, Governmental Liaison CL:GL
Director, Office of Security M:S
Director, Procurement A:P
Chief Counsel CC
National Taxpayer Advocate TA
Director, Legislative Affairs CL:LA
Director, Office of Program Evaluation and Risk Analysis N:ADC:R:O
Office of Management Controls N:CFO:F:M
Audit Liaisons:
 Deputy Commissioner for Modernization & Chief Information Officer M:R:PM:PO
 Chief, Agency-Wide Shared Services A:P
 Chief, Communications and Liaison CL

Improvements Are Needed to Prevent the Potential Disclosure of Confidential Taxpayer Information

Appendix IV

Outcome Measures

This appendix presents detailed information on the measurable impact that our recommended corrective actions will have on tax administration. These benefits will be incorporated into our Semiannual Report to the Congress.

Type and Value of Outcome Measure:

- Taxpayer Privacy and Security – Potential; 1.1 million taxpayer identification numbers (TIN¹) transmitted by the Internal Revenue Service (IRS) to the Office of Child Support Enforcement (OCSE)² for employers who reported wages paid to persons who owe child support payments. These TINs are potential disclosures not authorized under Internal Revenue Code (I.R.C.) § 6103 disclosures (see page 6).

Methodology Used to Measure the Reported Benefit:

The IRS Office of Governmental Liaison provided us with the number of TINs transmitted to the OCSE. For these transmissions, the TINs were EINs. The total represents the population of EINs on Wage and Tax Statements (Form W-2) that were transmitted to the OCSE from June 1997 through May 2002.³

The IRS advised us that it estimates the transmission of 27.6 million TINs included approximately 1.1 million unique EINs. This estimate includes duplicate requests that were made, for example, to obtain updated addresses or income information, but we cannot quantify these duplications from the available data. The IRS also cannot ascertain precisely what ratio of SSNs to EINs was actually experienced over the last 5 years because neither the OCSE nor the IRS retained the information transmitted. There have been wide variances in the OCSE requests, from monthly requests of 320 to almost 2 million. Consequently, an analysis of sample data, even if it were available, would not likely produce a very precise estimate.

Nevertheless, the IRS advised us that it calculated the 1.1 million unique TINs using a weighted average of the most current available CENSUS data on employment by employer size (1999). This provided a rough approximation of about 25 employees per employer. On that basis, the IRS estimates the transmission of 27.6 million TINs to OCSE over the 5-year period included approximately 1.1 million unique EINs (27.6 million/25 = 1.1 million).

¹ The TIN may be a Social Security Number (SSN), or an Employer Identification Number (EIN) issued by the IRS.

² The OCSE is part of the United States Department of Health and Human Services.

³ This information was not validated.

Improvements Are Needed to Prevent the Potential Disclosure of Confidential Taxpayer Information

The IRS advised us that the error was corrected in June 2002. The law allows for the names and addresses of employers to be provided. However, the law does not allow for the EINs to be provided.⁴

Type and Value of Outcome Measure:

- Reliability of Management Information – Potential; 210,017 SSNs disclosed to 2 private contractors without any verifications made by the IRS that those contractors were protecting this information against potential unauthorized disclosures (see page 10).
- Methodology Used to Measure the Reported Benefit:

The IRS provided us with the number of SSNs that were disclosed by the IRS to two private contractors that had contracts with the IRS during Calendar Year 2001 to provide electronic information.³ The IRS submitted the SSNs to the contractors who in turn provided electronic information on those taxpayers that the IRS needed. Since those contracts were awarded, the IRS has not made any on-site visits to inspect those facilities and determine whether the contractors are protecting the taxpayers' SSNs to ensure against any potential unauthorized disclosures of this sensitive information.

⁴ I.R.C. § 6103(l)(6) (2001).

Improvements Are Needed to Prevent the Potential Disclosure of Confidential Taxpayer Information

Appendix V

Laws and Regulations Governing Disclosure of Social Security Numbers

This listing provides a description of the Internal Revenue Code (I.R.C.) sections that define tax returns and return information, including Social Security Numbers (SSN), as confidential. Also provided is a description of other laws that restrict the disclosure of SSNs. While this listing provides many of the major laws and regulations governing disclosures of SSNs by the Internal Revenue Service (IRS), it is not a complete listing.

I.R.C. § 6103(a) (2002) – Defines tax returns and return information as *confidential* unless otherwise authorized by the I.R.C.

I.R.C. § 6103(b) (2001) – Defines return information to include the “taxpayer’s identity.” “Taxpayer’s identity” is defined to include the taxpayer’s name, mailing address, and taxpayer identifying number.

I.R.C. § 6109 (2001) – Requires individuals to provide their Taxpayer Identification Number (TIN) when filing a tax return. This section generally defines this identifying number as the SSN for individuals.

I.R.C. § 6103(d) (2001) – Provides that return information can be disclosed to state taxing agencies and state and local law enforcement agencies that assist in the administration of state tax laws.

I.R.C. § 6103(l)(6) (2001) – Provides that return information pertaining to an individual’s income can be disclosed to federal, state, and local child support enforcement agencies in order to establish or enforce child support obligations for that individual.

I.R.C. § 6103(l)(7) (2001) – Provides that return information pertaining to an individual’s unearned income¹ can be disclosed to federal, state, and local agencies that administer various welfare and other types of government assistance programs in order to determine either eligibility for, or the correct amount of, benefits under these assistance programs.

I.R.C. § 6103(n) (2001) – Provides that return information may be disclosed to any person, such as private contractors, to the extent necessary for various activities for tax administration purposes. This would include activities such as processing and storage of tax returns and maintenance, repair, and testing of equipment.

¹ This would include income such as interest, dividends, and pensions.

Improvements Are Needed to Prevent the Potential Disclosure of Confidential Taxpayer Information

I.R.C. § 6103(p)(4) (2001) – Provides that certain safeguards must be complied with as a condition for receiving return information under various provisions of I.R.C. § 6103. This subsection of I.R.C. § 6103 applies to federal, state, and local agencies that receive tax return information. However, it does not apply to disclosures provided for by I.R.C. § 6103(n).

Treas. Reg. § 301.6103(n)-1(d) – Authorizes the IRS to prescribe any conditions or requirements that must be met by persons receiving return information under I.R.C. § 6103(n) for the purposes of protecting the confidentiality of such information.

Treas. Reg. § 301.6109-1(a)(1)(ii)(C)-(D) – Requires that Employer Identification Numbers are used as the TINs when businesses such as corporations and partnerships file tax returns or other required statements.

I.R.C. § 7213 (2001) – Provides that unauthorized disclosures of returns or return information that are found to be willful are a felony that can result in a fine not exceeding \$5,000, or imprisonment of not more than 5 years, or both. This provision applies to any federal employee and to state agency employees receiving tax information under certain provisions of I.R.C. § 6103. It also applies to any person receiving returns or return information under I.R.C. § 6103(n).

I.R.C. § 7431 (2001) – Provides that if any officer or employee of the United States (U.S.) either knowingly, or by reason of negligence, inspects or discloses any returns or return information of a taxpayer in violation of any provision of I.R.C. § 6103, such taxpayer may bring a civil action for damages against the U.S. The damages are at least \$1,000 per unauthorized disclosure plus the cost of the action and, in some cases, attorneys' fees.

Privacy Act of 1974² – Regulates the collection, use, distribution, and maintenance of personal information, such as the person's identifying number, that is maintained in a "system of records"³ by federal agencies. One section of this Act requires those agencies requesting SSNs to inform individuals as to whether providing this information is voluntary or mandatory, the legal authority for requesting the SSNs, and how this information will be used.⁴

Computer Security Act of 1987⁵ – Requires federal agencies to identify their systems that contain or process sensitive unclassified information.

² Privacy Act of 1974, 5 U.S.C. § 552a (1994 & Supp. IV 1998).

³ A system of records is defined as a group of records under an agency's control from which information is retrieved by the individual's name or some other identifier assigned to that individual, such as an SSN.

⁴ 5 U.S.C. § 552a(e)(3) (1994 & Supp. IV 1998).

⁵ Pub. L. No. 100-235, 101 Stat. 1724 (1988).

Improvements Are Needed to Prevent the Potential Disclosure of Confidential Taxpayer Information

Office of Management and Budget Circular A-130, Management of Federal Information Resources, Appendix III – States, in part, that it is an agency’s responsibility to develop management controls to safeguard personal, proprietary, and other sensitive data in information systems.

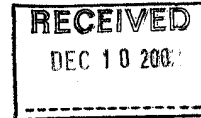
Improvements Are Needed to Prevent the Potential Disclosure of Confidential Taxpayer Information

Appendix VI

Management's Response



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



December 10, 2002

MEMORANDUM FOR DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM:

David R. Williams 
Chief Communications and Liaison

SUBJECT:

Management Response to Audit Report # 200240045
Improvements Are Needed to Ensure Taxpayer
Information Is Not Improperly Disclosed to Third Parties

Your report on the transmission of tax information to federal and state agencies will help us in our ongoing effort to improve our procedures for protecting taxpayer privacy. Since assuming responsibility for the IRS disclosure program, I have devoted considerable time to developing new business processes and procedures that will 1) better ensure that we share only tax information that is authorized by law; 2) streamline our reviews and activities to improve their efficiency and timeliness; and, 3) proactively manage our data sharing program with private contractors. Your analysis not only reinforces these priorities, but provides useful recommendations for improvements. However, they must be viewed within the proper context.

One area you highlight is the transmission of data to the Federal Office of Child Support Enforcement (OCSE). All of America shares your concern about potential misuse of SSN information. And let me stress that we believe that at no time in this particular data exchange between government agencies was an individual taxpayer's SSN placed at risk. The SSN portion of the exchange was safeguarded.

Your conclusion that the transmission of EINs is not allowed under the law raises questions that I wish to explore. Indeed, I want to determine whether your reading of the law is correct. Thus, consistent with your recommendation, I have asked the IRS Office of Chief Counsel to review the legal implications of these transmissions including whether these transmissions were, in fact, allowed under the law.

Preliminarily, Counsel notes that the words of the applicable law are susceptible to more than one interpretation and they are closely examining the legislative and administrative background before they advise me whether they agree with your

Improvements Are Needed to Prevent the Potential Disclosure of Confidential Taxpayer Information

2

conclusion. What I can conclude, however, is that employer EINs ended up in the hands of the state and local child support enforcement agencies who were authorized to receive them.

While Counsel continues its review of the legal implications of these transmissions, the discussion provided me an opportunity to closely examine our role in helping locate individuals who may owe child support. The IRS is committed to preserving taxpayer confidentiality because we realize the critical role it plays in effective tax administration. We also recognize the enormous benefits that can come from the exchange of information with agencies like the OCSE. It is because of these benefits that Congress authorized this and other data exchanges.

As we move to carry out congressional mandates on data sharing, we are mindful that the demand for authorized federal tax information has grown substantially. To manage this increase, we have aggressively enhanced disclosure awareness training agency-wide and increased training for our disclosure employees. We have also implemented both quantitative and qualitative performance measures, and have established goals for further improvements. In addition, we are building the foundation to improve our ability to perform computer security reviews. Finally, we are reengineering our business processes to better manage IRS data sharing activities.

Your findings and recommendations will be helpful to us. Despite a strong program, we can always make further improvements to prevent unauthorized transmissions to third parties. I believe the implementation of these recommendations will further ensure taxpayer privacy.

I have attached a detailed response outlining the corrective actions IRS will take to address your recommendations.

Attachment

Improvements Are Needed to Prevent the Potential Disclosure of Confidential Taxpayer Information

Attachment

Recommendation 1

Consult with the Office of Chief Counsel to determine the legal implications of the IRS' transmission of TINs (employer EINs) to the OCSE.

Assessment of Cause

The circumstance relating to this particular situation was the result of an inadvertent programming error.

Corrective Action

I agree with this recommendation and have already contacted Chief Counsel. Chief Counsel will determine the implications of the information set forth in the Report. Additional factual development is ongoing, as is Counsel's consideration of applicable law. Once we receive a response from Counsel we will determine if any further action is necessary.

Implementation Date

Proposed Date: March 31, 2003

Responsible Official

Deputy Director, Governmental Liaison and Disclosure

Corrective Monitoring Plan

GLD will develop an action plan and monitor it monthly.

Recommendation 2

Evaluate the Safeguard procedures to ensure the procedures address the content as well as the security of information shared under IRC 6103.

Assessment of Cause

Current procedures do not require final content testing or a verification that the information sent was only that which was requested.

Corrective Action

We agree with this recommendation and have initiated several activities that we believe will address this issue as it relates to authorized government FTI recipients, such as OSCE. We plan to examine our procedures to prevent inadvertent transmissions and readily detect such occurrences of inadvertent transmissions.

Improvements Are Needed to Prevent the Potential Disclosure of Confidential Taxpayer Information

2

As preventative measures, we plan to assess and revise the disclosure awareness training provided to the information technology staff to ensure they thoroughly understand their responsibilities. We have implemented additional testing measures for data transmitted to these authorized agencies.

To better detect possible disclosures we plan to implement two additional operational procedures. First, as part of our safeguard review we will require a verification of information authorized to be disclosed against information actually received. Second, we will modify our procedures to ask all FTI recipients to notify us if they receive information beyond that which was authorized.

Implementation Date

Proposed Date: June 30, 2003

Responsible Official

Deputy Director, Governmental Liaison and Disclosure

Corrective Monitoring Plan

GLD will develop an action plan and monitor it monthly.

Recommendation 3

Evaluate whether staffing levels are sufficient to ensure that third parties receiving Federal tax information from the IRS are in compliance with the safeguarding requirements.

Assessment of Cause

Based on current practices, the safeguard workload is beyond staff resources.

Corrective Action

Without additional staff or a change in our approach to safeguard reviews, we acknowledge that the existing workload exceeds the capacity of the Safeguard Office. In a June 2001 report, by an outside contractor benchmarking the safeguard program, the contractor recommended that the safeguard review approach be modified to prioritize the agency review schedule based on the relative risk level assigned to each agency. As a result, in 2002 we engaged an outside contractor to develop risk assessment guidelines for site selection and to begin building a foundation for self-certification, third party certification, or other best practice methodology.

Implementation Date

Proposed Date: June 30, 2003

Improvements Are Needed to Prevent the Potential Disclosure of Confidential Taxpayer Information

3

Responsible Official

Deputy Director, Governmental Liaison and Disclosure

Corrective Monitoring Plan

GLD will develop an action plan and monitor it monthly.

Recommendation 4

Revise the IRS safeguard procedures to provide specific criteria on which contractors should have their facilities inspected and to ensure that these inspections are made.

Assessment of cause

IRS had procedures in place, but they need to be clarified.

Corrective Action

We agree with the recommendation that IRS safeguard procedures be revised to provide more specific criteria. We are in the process of revising our IRM and will review the current methodology for contractor inspection and explore the feasibility of contractor selection for more detailed safeguard reviews based upon the relative risk level assigned to contractors. We will review the contractors TIGTA identified and take appropriate corrective action when necessary.

Implementation Date

Proposed Date: June 30, 2003

Responsible Official

Deputy Director, Governmental Liaison and Disclosure

Corrective Monitoring Plan

GLD will develop an action plan and monitor it monthly.

Recommendation 5

Work with the Office of Procurement to revise internal safeguard and contract procedures to ensure that they are in agreement and are in compliance with the appropriate laws concerning private contractors.

Assessment of Cause

Staff who are involved in contracting, in all parts of the IRS, are not fully aware of all the intricacies of disclosure rules (including the Privacy Act), and related procedures.

Improvements Are Needed to Prevent the Potential Disclosure of Confidential Taxpayer Information

4

Corrective Action

We agree with this recommendation and plan to work with the Office of Procurement to revise internal safeguard and contract procedures to ensure they comply with the appropriate laws concerning private contractors.

We have identified business needs that we can integrate into the recent webRTS systemic applications and procedures used by the IRS in our contracting functions. The Office of Governmental Liaison and Disclosure will focus on enhancements and improvements to revise and upgrade internal safeguard and contract provisions for the AWSS Office of Procurement contractors.

Implementation Date

Proposed Date: June 30, 2003

Responsible Official

Deputy Director, Governmental Liaison and Disclosure

Corrective Monitoring Plan

GLD will develop an action plan and monitor it monthly.

Recommendation 6

Provide clear guidance to private contractors on the safeguard requirements and their responsibilities under those requirements.

Assessment of Cause

The portfolio of information IRS provides to contractors is sometimes confusing.

Corrective Action

We will review all of the applicable contractual clauses and our educational portfolio to ensure they are clear, concise, and consistent. Currently we have the following contractual provisions and educational tools to assist contractors in understanding their responsibilities to safeguard FTI:

- 1) IRS Acquisition Procedure (IRSAP), which are agency acquisition regulations that implement and supplement the Federal Acquisition Regulation (FAR) and as the Treasury Acquisition/Procurement Regulation (TAPR);
- 2) Safeguarding IRS Confidential Information: A Guide for Contractors (This is a 14 minute video which discusses the safeguarding requirements to contractors.);

Improvements Are Needed to Prevent the Potential Disclosure of Confidential Taxpayer Information

5

- 3) IRS Disclosure Awareness Pocket Guide for Contractors, Document 9946, (Rev. 2-98), which is a paper leaflet the IRS is required to issue to all contractors to whom we will disclose Sensitive But Unclassified (SBU) data, for use with the video (The contractor will provide a pocket guide to each officer and employee who will have access to SBU data.);
- 4) IRM 1.23.2.2, Contractor Investigations, which includes the TD P 71-10 Non-Disclosure Agreement, contractors must sign when we give them conditional access to SBU information.

Implementation Date

Proposed Date: June 30, 2003

Responsible Official

Acting Deputy Director, Governmental Liaison & Disclosure

Corrective Monitoring Plan

GLD will develop an action plan and monitor it monthly.

Again, we appreciate the recommendations provided by the TIGTA team. If you have any questions, please contact Tom Marusin, Deputy Director of Government Liaison and Disclosure, at (202) 622-3633.