
November 1998

INTERNAL REVENUE SERVICE

Physical Security Over Taxpayer Receipts and Data Needs Improvement





United States
General Accounting Office
Washington, D.C. 20548

Accounting and Information
Management Division

B-280960

November 30, 1998

The Honorable Charles O. Rossotti
Commissioner of Internal Revenue

Dear Mr. Rossotti,

This letter presents the results of our review of the Internal Revenue Service's (IRS) physical controls over receipts and taxpayer data. As reported in our audit of IRS' fiscal year 1997 custodial financial statements¹ and in subsequent congressional hearings on IRS financial management issues,² IRS' internal controls at service centers were not adequate to sufficiently ensure that cash and checks received from taxpayers were properly credited to taxpayers' accounts and deposited to the Department of the Treasury general fund. We further reported that these control weaknesses and inherent vulnerabilities expose IRS and taxpayers to losses.

To follow up on these weaknesses and to assess physical security conditions at IRS during the peak filing season, we observed physical controls over receipts and taxpayer data at service centers and district offices in April 1998 as part of our ongoing audit of IRS' fiscal year 1998 financial statements. This report discusses additional internal control weaknesses over the safeguarding of receipts and taxpayer data that we identified in April 1998 and provides our recommendations for improvement.

Results in Brief

IRS' controls over receipts and taxpayer data do not adequately reduce the vulnerability of the federal government and taxpayers to loss from theft. For example, employees were hired and worked in positions requiring the handling of cash, checks, or sensitive taxpayer information before IRS received the results of these employees' required background and/or fingerprint checks. This condition existed because of the length of time required to conduct background investigations, delays in receiving results of fingerprint checks, and processing demands which required the hiring of thousands of employees during the peak filing season. Placing new hires in sensitive positions prior to, at a minimum, receiving the results of

¹Financial Audit: Examination of IRS' Fiscal Year 1997 Custodial Financial Statements (GAO/AIMD-98-77, February 26, 1998).

²Internal Revenue Service: Remaining Challenges to Achieve Lasting Financial Management Improvements (GAO/T-AIMD/GGD-98-139, April 15, 1998).

fingerprint checks increases the vulnerability of receipts and taxpayer data to theft. In fact, of the 80 thefts IRS investigated at service centers from January 1995 to July 1997, 12 (15 percent) were committed by individuals who had previous arrest records or convictions that were not identified prior to their employment and thus may have influenced IRS' decision on whether to hire these individuals.

We also noted weaknesses in the physical controls over service center and district office receipts. While service center receipts are required to be processed only by authorized individuals in the Receipt and Control Branch, which is a restricted access area, numerous receipts were found in unrestricted areas accessible to other IRS employees and to non-employees not authorized to handle receipts. For example, at one service center receipts and returns were stored in an uncontrolled hallway that individuals can enter unchallenged from an adjoining fitness center and other areas of the service center. Receipts particularly vulnerable to theft, such as returned refund checks, also were not adequately secured.

While it is important to adequately protect cash and checks received at IRS facilities, it is similarly essential to ensure that these receipts are properly protected during transport to depository institutions. We found that single, unarmed couriers in ordinary civilian vehicles were used to transport IRS deposits totaling hundreds of millions of dollars to the depository institutions during the peak filing season. In fact, one courier left a deposit totaling over \$200 million unattended in an open vehicle while he returned to the service center. At one district office, IRS relied upon a bicycle messenger to deliver daily deposits ranging from over \$1 million during the nonpeak season to more than \$100 million during the peak season. Because of the magnitude of IRS' deposits and the sensitivity of taxpayer information contained on the checks, IRS' current courier practice may be inadequate. The theft of one peak season deposit could place a significant administrative burden on IRS to contact taxpayers and initiate stop payment orders on tens of thousands of checks. In addition, many taxpayers could suffer from (1) damages if their stolen checks were used for check cloning operations or (2) identity fraud since checks processed by IRS contain not only bank account numbers, names, addresses, and taxpayer signatures, but also encoded social security numbers.

Although receipts and taxpayer information will always be vulnerable to theft, IRS has a responsibility to protect the government and taxpayers from such losses. Many of the actions we are recommending to minimize these vulnerabilities and thus better protect taxpayer receipts and data

would not result in significant costs, and several other actions we are recommending are already required by IRS policy or are currently under consideration by IRS management. In fact, IRS has prepared two corrective action plans to reduce its vulnerability to theft or loss of receipts and taxpayer data. IRS' Summary Action Plan: Protection of Monetary Instruments, dated May 20, 1998, lists IRS' proposed actions for correcting internal control weaknesses recently identified by internal auditors and by IRS' Office of Systems Standards and Evaluation. This document lists physical security weaknesses identified by IRS and IRS' plans to address these problems. On June 4, 1998, IRS also issued a plan proposing a series of specific actions to address control deficiencies related to recruitment, background, and security investigations. While these two plans begin to address some of the weaknesses we identified, they do not address several issues identified in this report. For example, the action plans do not address internal control weaknesses at district offices or courier-related issues.

Background

In fiscal year 1997, IRS collected more than \$1.6 trillion in tax revenue. Most of this revenue was collected by intermediaries, such as financial depository institutions, and transferred directly to the Treasury general fund. However, the remainder—estimated at over \$100 billion in fiscal year 1997—was collected directly by IRS through its many service centers and district offices. Receipts IRS collected directly consist primarily of cash and checks mailed to IRS service centers with accompanying tax returns or payment vouchers and payments made in person at one of the service centers or district offices.

While adequate physical safeguards over receipts should exist throughout the year, it is especially important during the peak filing season. Each year, during the weeks before and immediately after April 15, an IRS service center may receive and process daily over 100,000 pieces of mail containing returns, receipts, or both. The dollar value of receipts each service center processes increases to hundreds of millions of dollars a day during this time period. In addition, the number of staff increases significantly to handle and process the additional volume. For example, IRS hired over 20,000 seasonal employees nationwide for the 1998 filing season. The increased number of seasonal staff IRS employs to handle and process this large volume of receipts and returns increases IRS' vulnerability to theft.

In addition to adequately safeguarding taxpayer receipts, it is equally important for IRS to protect sensitive taxpayer data. Tax returns, schedules, and supporting documentation contain sensitive identifying information such as name, address, social security number, and details on the taxpayer's financial holdings. Although none of the financial crimes and identity fraud incidents we noted in our previous report on identity fraud³ were reported as being linked to data stolen from IRS, sensitive information similar to that processed by IRS has been used to commit such crimes nationwide. Commonly reported financial crimes and identity fraud include using someone's personal information to fraudulently establish credit, run up debt, or take over and deplete existing financial accounts. According to a Secret Service official, identified losses to victimized individuals and institutions due to financial crimes involving identity fraud increased from \$442 million in fiscal year 1995 to \$745 million in fiscal year 1997.

IRS has also suffered losses due to various financial crime schemes. Between October 1995 and September 1997, IRS closed investigations on 22 cases involving theft of receipts at its district offices.⁴ In addition, between January 1995 and July 1997, IRS investigated 80 thefts of receipts totaling \$5.3 million that occurred at its service centers. Of this amount, \$4.6 million was attributable to one individual who stole not only checks but also original tax returns. This individual sent the checks to members of an organized crime ring in New York, who then altered or in some cases, "cloned"⁵ the checks for subsequent negotiation. For example, one taxpayer's check was cloned by the perpetrators into multiple smaller checks and negotiated in England and Germany. The cloning scheme was discovered when the taxpayer's accountants noticed that the check written to IRS was never cashed and that there were multiple additional checks cashed for amounts for which they had no supporting documentation.

Financial crimes and identity fraud committed through the theft of receipts and tax return data can cause damage to many parties. Banks suffer financial loss when held accountable for damages resulting from

³Identity Fraud: Information on Prevalence, Cost, and Internet Impact is Limited (GAO/GGD-98-100BR, May 1, 1998).

⁴These thefts occurred in district offices and other post of duty sites which fall under the responsibility of district directors.

⁵Once a perpetrator obtains information, such as the bank and account number, from a valid check, that information can be used to "clone" or duplicate the original check into multiple fraudulent blank checks. These blank checks can then be made out to different payees, the signature forged, and the checks deposited in the perpetrators' accounts.

cloned checks. The federal government may suffer losses in cases involving IRS' failure to safeguard receipts and taxpayer data. Taxpayers can suffer injury to their reputations when credit is fraudulently established and debts incurred in their names. Bad credit could in turn lead to difficulties in obtaining loans or jobs and require a lengthy and expensive process to clear one's personal records.

While IRS inspectors have identified thefts of receipts and taxpayer data, the true magnitude of such crimes that have occurred within IRS will likely never be known. An IRS inspector stated that the \$5.3 million of investigated thefts at service centers is understated for several reasons. For example, during investigations, prosecuted individuals confessed that they had stole other checks but could not remember the full amount. With the weaknesses and vulnerabilities identified, there are likely many thefts that have gone undetected. Furthermore, although IRS has identified instances of original tax returns stolen from service centers, the extent to which criminals have taken advantage of stolen taxpayer information is less measurable and thus largely unknown. However, the potential for using such data to commit identity fraud is great.

Instances of financial crimes committed at IRS and their possible consequences demonstrate the importance of establishing and maintaining adequate physical controls over receipts and taxpayer data. We recognize that due to the high volume and sensitive nature of IRS' activities, particularly during the peak filing season, no system of internal control can eliminate the vulnerability of receipts and sensitive taxpayer information to theft. However, a sound system of internal control should minimize the extent of this vulnerability to ensure that the government and taxpayers are not unduly exposed to loss of funds and misuse of taxpayer data, both of which could undermine the public's trust in IRS' ability to safeguard taxpayer funds and personal information.

Objectives, Scope, and Methodology

The objectives of our review were to (1) follow-up on cash receipt weaknesses identified in our audit of IRS' fiscal year 1997 Custodial financial statements, and (2) observe operations during the peak filing season as part of our fiscal year 1998 financial statement audit. We conducted our visits from April 20 through April 23, 1998, at the Atlanta, Georgia, Austin, Texas, Ogden, Utah, and Philadelphia, Pennsylvania, service centers. These service centers were selected based on the dollar amount of receipts processed during fiscal year 1997 and on the dollar

amount of reported thefts that occurred between January 1995 and July 1997.

We also conducted observation work at the Los Angeles, Northern California, and North Texas district offices. Two of these three district offices were selected because they had teller units responsible for making deposits of walk-in payments to the banks via courier. We also selected one district office that did not have a teller unit and therefore sent all receipts, along with tax returns, to a service center to be processed.

We conducted observations of the activities and the physical controls over the processing of receipts and tax returns at these service centers and district offices, and had limited discussions with IRS personnel at these sites. As agreed with IRS' Chief Financial Officer, we limited our inquiry of IRS employees during these visits so we would not hinder operations during the peak filing season. However, we subsequently followed-up with IRS service center and national office personnel to obtain clarification and further explanation of IRS procedures. We reviewed internal audit reports and interviewed IRS internal auditors and inspectors at the Philadelphia and Ogden service centers to supplement our understanding and to obtain additional information and insight. We interviewed the Regional Inspector for the Northeast Region to obtain details on incidents of thefts at IRS service centers. We also reviewed IRS' Summary Action Plan: Protection of Monetary Instruments, dated May 20, 1998, to consider IRS' proposed actions on previously identified control weaknesses over monetary instruments, as well as IRS' action plan dated June 4, 1998, to address control deficiencies over recruitment, background, and security investigations. We have not performed subsequent site visits to verify completed corrective actions reported by IRS. However, we intend to follow up on the status of these corrective actions as part of our fiscal year 1998 financial statement audit.

We performed our work from April 1998 through August 1998 in accordance with generally accepted government auditing standards. We requested written comments on a draft of this report from the Commissioner of Internal Revenue or his designee. The Commissioner provided us with written comments, which are discussed in the "Agency Comments and Our Evaluation" section and are reprinted in appendix I.

Delays in Obtaining Background Information Compromise the Security of Taxpayer Data and Receipts at Service Centers

Despite the sensitivity of taxpayer data, we recognize that fully limiting access to such data is not feasible given the nature of IRS' operations. Because the primary nature of IRS operations is to process tax returns, most of the units within the service center work with tax returns or other forms of tax data. Therefore, sensitive taxpayer information is accessible all over the service center. As a result, the vulnerability of this data to theft or misuse is heightened. This vulnerability thus underscores the need for effective deterrent controls to aid in reducing the exposure of tax data to such theft or misuse.

To reduce the inherent risk in this exposure, IRS' policy is to screen out job applicants that may pose a potential threat to IRS operations. IRS requires a fingerprint check on all permanent, seasonal, and temporary employees hired to identify any prior arrests and convictions. In addition, IRS requires a background investigation on all employees with a 90-day appointment or longer. However, IRS internal auditors reported that, in at least some instances, and for numerous reasons which we discuss later in this report, the results of these checks were not completed before the individuals were placed in positions responsible for handling cash receipts and taxpayer data.⁶

The Comptroller General's Standards for Internal Controls in the Federal Government⁷ calls for employees to have personal and professional integrity and to maintain a level of competence that allows them to accomplish their assigned duties. Because IRS employees are entrusted with handling sensitive taxpayer information of a financial and personal nature, as well as billions of dollars in receipts, ensuring worker integrity through a carefully managed recruiting and hiring process is an area demanding special attention from IRS management.

One way to assist in determining worker integrity is to ensure that background investigations of an appropriate level are performed on IRS employees. A background investigation may involve contacting prior employers, schools, and law enforcement agencies to inquire about the applicant's qualifications, character, and other pertinent factors. The extent of the investigation depends on the employing agency's risk

⁶See Review of Remittance Processing Activities (Internal Revenue Service, Office of the Chief Inspector, Reference No. 082503, March 24, 1998). The Office of the Chief Inspector includes Internal Audit, Internal Security, and Regional Inspections.

⁷The Comptroller General's Standards for Internal Controls in the Federal Government, issued in 1983, contains the internal control standards to be followed by executive agencies in establishing and maintaining systems of internal control as required by the Federal Managers' Financial Integrity Act of 1982, as amended.

assessment of the sensitivity of the position to be occupied based on guidelines defined by the Office of Personnel Management (OPM). Currently, IRS classifies some Receipt and Control Branch employees as occupying “low risk” positions. These “low risk” employees handle thousands of taxpayer receipts and sensitive taxpayer information which require a high degree of public confidence and trust. Because “low risk” positions require the least comprehensive type of investigation, background investigations for such employees may fail to uncover all pertinent information regarding the suitability of an individual to process taxpayer data and receipts.

However, background investigations are lengthy. According to OPM, even limited investigations take an average of 75 calendar days to complete. Because of the length of time it takes, IRS only requires a background investigation for employees hired for periods of 90 days or more. To help screen individuals, such as seasonal and temporary employees who are hired for less than 90 days, and to more quickly identify potential problems with long-term employees before their background investigations are completed, IRS initiates fingerprint checks of all newly hired staff prior to employment. IRS submits candidates’ fingerprints and preliminary background information on each individual to OPM. OPM then inputs the demographic information into its database and transmits the information with the fingerprints to the Federal Bureau of Investigations (FBI) to check against national records. According to IRS, OPM indicated that results of fingerprint checks can be provided within 21 workdays. However, extensive delays in receiving fingerprint check results prevented IRS from obtaining such pertinent information promptly. The IRS internal audit review mentioned previously reported that the turnaround time for fingerprint checks averaged 68 days, with some fingerprint checks taking as long as 141 days, instead of the 21 days indicated by OPM.

The internal audit review also found that some service centers did not take fingerprints of applicants or did not submit fingerprints in a timely manner. Furthermore, the review found that one service center did not prescreen any 30-day temporary employees, while another service center did not follow procedures requiring that service centers prescreen employees prior to sending background investigation packages for processing. The review also found that IRS personnel offices were reluctant to use the fingerprint prescreening process because the results were not received before employees reported to work.

In February 1998, IRS convened a task team to study the service center prescreening process. The task team found that the delays with fingerprint checks are due to a number of causes that are partially attributable to IRS and partly to the FBI. According to the task team, not all service centers were fingerprinting applicants at the earliest possible point. Additionally, in some instances, fingerprints had to be retaken because of their poor quality and thus could not be processed by the FBI. The task team also found that the FBI's manual processing of fingerprints is labor intensive, particularly for those prints that result in a possible match to the FBI's database of arrest records. The task team found that the FBI had a backlog of 600,000 cases to process as of the date of their study and that the FBI places a higher priority on processing law enforcement requests for fingerprint checks than on requests related to personnel investigations.

The delays in fingerprint checks are particularly serious when they are applied to seasonal and temporary employees. According to IRS data, a total of more than 20,000 seasonal employees were employed in 1998, of which more than 5,000 were new seasonal employees. These seasonal and temporary employees work an average of 8 to 10 weeks during the peak filing season, and may have already finished their term of employment before IRS receives the results of these fingerprint checks. In fact, the internal audit review discussed above found that in four service centers where information was available, as many as 5 percent of the 3,059 temporary and seasonal employees hired and placed in the Receipt and Control Branch during fiscal years 1996 and 1997 had backgrounds that contained arrests or convictions. If the results of fingerprint checks are not received promptly by IRS, these individuals can be placed in positions to steal receipts and taxpayer data.

The failure to ensure that background investigations and fingerprint checks are completed before employment in sensitive areas increases the vulnerability of billions of dollars of cash and checks, as well as taxpayer data, to theft and fraud. According to the internal audit review, of the 80 thefts of receipts at service centers reported between January 1995 and July 1997, 12 were committed by employees with previous arrest records for theft, assault, or drug charges that were not identified prior to employment. The fingerprint prescreening results were not received before six of these employees reported for work and fingerprint prescreenings were not performed for the other six employees.

To help address the slow turnaround time in receiving the results of fingerprint checks, the Philadelphia Service Center (PSC) has negotiated

with local law enforcement to provide police checks on prospective IRS employees. Due to technical problems, PSC missed its August 1998 target date to establish a working, on-line connection between its fingerprinting machine and the local law enforcement's fingerprint database. However, once these problems are resolved, the connection should enable PSC to transmit electronic fingerprint images so that the local law enforcement's database can be checked and PSC alerted of arrest records on IRS applicants within 24 hours. While this should result in a marked improvement, the database can only identify crimes committed locally.

On a nationwide basis, IRS has begun to address the fingerprint check problem. In response to a long-term solution recommended by the IRS task team, IRS is in the process of procuring equipment that will be compatible with the FBI's Integrated Automated Fingerprint Identification System. This system will allow for an automated fingerprint classification. According to IRS, the electronic fingerprints, demographic information, and results from the FBI's search will be channeled through OPM so that OPM can upload the information into its database. The FBI's goal with this system is to process civil fingerprint checks within 24 hours. IRS expects to receive the results of the fingerprint check within 5 days. IRS' target date for implementation of this system is August 1999.

In the meantime, IRS is exploring short-term solutions recommended by the IRS task team to address problems with delayed fingerprint results. According to IRS' action plan, it has retrained employees to take better quality fingerprints. Other planned short-term actions include 1) developing a policy to take fingerprints of filing season applicants upon their first contact with IRS, 2) issuing guidelines for service centers to contact local police agencies to determine if they will provide police checks on prospective employees, 3) determining the feasibility of moving employees from other units so that only employees with completed fingerprint checks are assigned to process receipts, and 4) bringing all service center personnel offices on-line with OPM so that the offices can receive background checks from OPM as soon as the results from FBI are uploaded to OPM's database. These additional actions, however, have not yet been implemented.

Recommendations

To ensure that employees assigned to process receipts and sensitive taxpayer data are subjected to the appropriate level of background check, we recommend that the Commissioner reevaluate the risk classification of

all positions in IRS' Receipt and Control Branch and reclassify such positions where appropriate.

To reduce the incidence of applicants not subjected to fingerprint checks, we recommend that the Commissioner (1) establish procedures to review the applications and associated documents for all applicants given job offers to ensure that fingerprint checks are initiated on these individuals and (2) implement procedures to provide supervisory feedback on these reviews as necessary to ensure that personnel staff are aware of and follow IRS' policy requiring fingerprint checks.

To assist in the prompt receipt of fingerprint results of applicants, we recommend that the Commissioner continue with the agency's plans to develop and implement a policy to fingerprint filing season applicants at the earliest possible time in the job application process.

We also recommend that until the problems with delays in fingerprint checks are resolved, the Commissioner develop and implement a policy prohibiting new employees from being assigned to process receipts until results of fingerprint checks are received and reviewed by management.

To obtain background information on a more timely basis, we recommend that the Commissioner continue the agency's efforts to explore the feasibility of obtaining local police checks on IRS applicants and evaluate the efficiency and effectiveness of PSC's electronic fingerprinting system in order to supplement FBI fingerprint checks.

In the long term, to decrease the turnaround time for FBI fingerprint check results, we recommend that the Commissioner continue the agency's efforts to negotiate with OPM and the FBI and procure the necessary equipment so that it can participate in the FBI's Integrated Automated Fingerprint Identification System program by August 1999.

Physical Safeguards Are Inadequate to Protect Cash Receipts

The Comptroller General's Standards for Internal Controls in the Federal Government requires that access to resources and records, such as IRS receipts and taxpayer data, be limited to authorized individuals in order to reduce the risk of unauthorized use or loss to the government. However, at the service centers and district offices we visited, we identified internal control weaknesses that allowed unauthorized access to such resources and records. Specifically, we found that IRS service centers did not (1) have adequate controls to limit unauthorized access to receipts and

accompanying tax returns and (2) implement adequate safeguards over returned refund and unmatched checks. At district offices, we found that IRS did not (1) adequately secure receipts as required by the Internal Revenue Manual (IRM)⁸ and (2) perform necessary reconciliations to ensure accountability for district office receipts. Because IRS service centers and district offices directly collected over \$100 billion in fiscal year 1997 and are responsible for processing all taxpayer data submitted by taxpayers, such weaknesses increase the vulnerability of receipts and taxpayer data to theft or misuse.

Service Centers Lacked Adequate Deterrent Controls to Limit Unauthorized Access to Receipts

During the peak filing season, the processing of receipts and returns occurs 24 hours a day. IRS handles and processes taxpayer receipts and returns in several stages. The Receipt and Control Branch at each IRS service center is responsible for the receipt and initial processing of mail containing receipts and returns delivered to the service centers. The branch is to be located in a restricted access area limited to authorized personnel. Staff extract the contents of envelopes mailed by taxpayers, post the payment data to credit taxpayers' accounts for the amounts received, and then endorse and prepare the checks for deposit.⁹ After the payments are processed, units outside the Receipt and Control Branch review the tax returns and post the tax return data to taxpayers' accounts. The units that post the tax return data are not located in restricted areas and are thus accessible to all employees and nonemployees who have access to an IRS service center.

IRM 1(16)41 Physical Security Handbook, section 257.4, requires that the mail extraction operation—the first stage of processing—take place in a secured and restricted access area. However, at the four service centers we visited, mail that contained tax returns and receipts was left in carts in open, unrestricted corridors or rooms. Because of limited space at the service centers, these areas served as overflow storage when the units responsible for extracting mail could not accommodate all the mail received during the peak filing season. At two of the service centers, both unopened mail and opened mail that had been separated and clearly

⁸The IRM prescribes the procedures that IRS employees must follow when processing IRS documents and data.

⁹The unit responsible for posting payments to taxpayer accounts is sometimes organizationally part of the Receipt and Control Branch and sometimes part of the Data Conversion Branch, depending on the service center. However, at the service centers we visited, this unit was always physically located in the Receipt and Control Branch's restricted access area.

labeled as either “with remittances” or “without remittances”¹⁰ were stored in these areas. These overflow areas were not located in restricted access areas and, thus, were easily accessible to anyone in the service center, such as employees not authorized to process receipts or visitors who had no need to access receipts or taxpayer data. In fact, at one service center, the corridor used as an overflow area was a heavily travelled corridor used by employees carrying gym bags to access a fitness center. During our observations, no guards patrolled these areas in three of the four service centers visited. Although one service center used surveillance cameras to monitor activities in the corridor, the cameras’ views of activities were obstructed by 7-foot-high carts used to store unsorted and sorted mail.

At the end of the extraction process, IRS staff illuminate, or “candle,” all envelopes which have already gone through the extraction process to ensure that all contents are actually removed prior to the envelopes’ destruction. The final candling activity at one service center was located in an unsecured room off an unrestricted corridor. Since the final candling activity is an extension of the extraction of receipts and taxpayer data, this operation should be located in a secured and restricted access area, as required by IRM 1(16)41 Physical Security Handbook section 257.4. Because many checks are found during the candling process, the lack of security over the candling area increases IRS’ vulnerability to theft or loss of checks.

We also found that receipts discovered outside the Receipt and Control Branch were not adequately accounted for and secured. IRM 38(43)3.2, section (10), Service Center Deposit Activity, requires that “discovered remittances” not delivered immediately to the units responsible for depositing these receipts are to be held in locked containers. “Discovered remittances” are cash and/or checks that were either erroneously overlooked during the extraction process or that bypassed extraction because the receipts were sent unopened to other units, such as the Offer-in-Compromise Unit. The IRM further requires that as each such receipt is discovered, it is to be recorded by a supervisor on a control log. At two service centers, we observed numerous checks left on desks, shelves, or file folders in unsecured areas, such as the Code and Edit Unit and the Offer-in-Compromise Unit.

At one of the service centers where we performed additional work, we found that these checks were not recorded on control logs until they were

¹⁰IRS uses the terms “remittances” and “receipts” interchangeably to refer to taxpayers’ payments against their tax liabilities. To the taxpayer, such amounts are remittances (payments), but to IRS they are receipts.

ready to be taken for receipt processing and deposit. We were informed that during the peak filing season, these checks were recorded on control logs and submitted to the appropriate unit for receipt processing on an hourly basis. However, prior to doing so, unsecured and unattended checks outside restricted areas were susceptible to theft by any individual who had access to the service center.

Prior IRS internal audits and other internal reviews have identified other weaknesses in controls over the safeguarding of receipts. In response to these findings, each service center provided IRS management with its respective corrective action plan, which was then incorporated into IRS' Summary Action Plan: Protection of Monetary Instruments, dated May 20, 1998. The plan reported corrective actions pending and some completed for weaknesses noted at specific service centers. However, the plan did not specifically address the use of overflow areas for storing receipts, nor did it address the weaknesses over "discovered remittances". Additionally, the plan addressed the candling issue only at sites other than the one where we noted the weakness.

Service Centers Lacked Additional Safeguards Over Unmatched and Returned Refund Checks

Certain receipts that are particularly vulnerable to theft, such as "unmatched" and returned refund checks, were not properly secured. Unmatched checks are those checks that were inadvertently separated from their accompanying vouchers or tax returns or were mailed to the service center without any instructions from the taxpayers as to how the payments should be applied. Without such instructions, such checks must be set aside until they can be researched to determine which taxpayers' accounts should be credited. At all service centers, unmatched checks are not subject to additional security but are stored in open baskets accessible to all who have access to the Receipt and Control Branch. As a result, these unmatched checks are particularly vulnerable to theft because they are not immediately processed and are stored in open baskets for long periods of time.

Returned refund checks are Treasury refund checks that are sent to taxpayers and subsequently returned uncashed to IRS as payment against other tax liabilities. IRM 3.8.43, Service Center Direct Receipts - Service Center Deposit Activity, section 43.4.2.47, requires refund checks returned to IRS by taxpayers to be stamped "non-negotiable." Although the IRM does not state when the returned refund checks should be voided, some of these checks were already endorsed by the taxpayers, making them highly negotiable. Consequently, they should be voided as soon as they are

extracted. However, at two service centers, returned refund checks discovered by the Extraction Unit were handled by several employees before they were voided. These returned refund checks were left in unsecured bins or file folders on desks prior to being stamped “non-negotiable,” significantly increasing the risk of theft. According to internal auditors at one service center, seven returned refund checks totalling \$300,000 were stolen from that service center. This demonstrates the susceptibility of these refund checks to theft.

IRS internal audit similarly identified weaknesses over the handling of returned refund checks and recommended establishing tighter controls over these instruments. According to IRS’ Summary Action Plan: Protection of Monetary Instruments, IRS is pursuing a plan of action to address this weakness. However, no changes have yet been implemented.

District Offices Did Not Adequately Secure Receipts

Although district offices do not receive the same volume of receipts as service centers, it is nonetheless important for such offices to diligently control access to and accountability for their receipts. However, as in the service centers, we found weaknesses in the internal controls over district office receipts that expose them to risk of theft or loss.

Procedures for handling receipts at district offices vary slightly depending on whether the district office has a teller function. In all cases, however, the Customer Service Unit at the district office collects walk-in payments and tax returns from the taxpayers. If the district office has a teller function, walk-in payments are submitted to the Teller Unit, which posts receipt data into the IRS database in the same way the service centers do.¹¹ These district offices use couriers to deliver their checks for deposit to the bank and to deliver any accompanying tax returns to the service centers for processing. If the district office does not have a teller function, the Customer Service Unit collects walk-in payments and returns and transmits all the documents via courier to the service center for processing.

IRM 1(16)(41), Physical Security Handbook, section 500, “Minimum Protection Standards,” establishes a nationwide, uniform method of protecting items which require safeguarding. Specifically, it requires that checks and currency be stored in locked containers and that the keys to

¹¹Due to the presence of different systems, the service centers and the district offices might initially post receipts on different systems. However, after processing, data from the different systems eventually feed into the main IRS database, which contains data on both payments received and taxes owed.

access those containers also be stored in a locked container. At the three district offices visited, we observed receipts stored in unlocked containers during the day and, at two district offices, in containers accessible to numerous employees overnight. Specifically, we found the following:

- At one district office, Customer Service employees left their desks unattended during the day, even though receipts were stored in drawers and the keys were still in the locks. At the end of the day, employees emptied their desk drawers of receipts in order to store them in a file cabinet overnight. If an employee left early, another employee would empty the drawer of receipts for overnight storage. The key to the file cabinet was accessible to all employees assigned to that unit.
- At another district office, Customer Service employees stored receipts in an unlocked cash box. The Customer Service area was accessible to all IRS employees at the district office. The receipts were locked in a file cabinet at the Teller Unit area overnight, and the key to the cabinet was stored in an unlocked desk. Several employees in the unit were aware of where the key was stored.
- In the third district office, receipts were stored in an open bin during the day. These receipts were stored overnight in a locked cabinet. At this district office, access to the cabinet was limited to two people in the unit.

The use of unsecured containers to store receipts, or the failure to limit storage container accessibility to employees designated to open such containers, increases the potential for theft.

District Offices Did Not Perform Necessary Reconciliation to Ensure Accountability

To ensure proper access to and accountability for resources, the Comptroller General's Standards for Internal Controls in the Federal Government specifies that periodic comparisons should be made between resources and records and that the frequency of such comparisons be determined by the vulnerability of the asset. However, at all three district offices we visited, receipts were not recorded in control logs or transmittal sheets until a few hours after receipt or even the following day. Additionally, no one reconciled the receipts against the control logs prior to or after overnight storage and prior to submitting them to the district office teller unit or to the service centers for processing. Given the weaknesses in securing receipts discussed above, the failure to immediately record receipts in control logs and to reconcile these control logs to receipts on hand decreases the likelihood of the timely detection of theft of receipts. Under current practices, incidents of theft may not come to IRS' attention until taxpayers receive erroneous default notices or

identify anomalies in their cancelled checks or bank statements and contact IRS.

Recommendations

To ensure that the mail extraction process takes place in a secure and restricted access area, as required by the IRM, we recommend that the Commissioner improve the physical security controls over receipts and returns stored in unsecured overflow areas. These controls might include limiting unnecessary traffic by temporarily designating these overflow areas as restricted access areas and/or posting additional security guards over such areas during the peak filing season.

To limit exposure to theft and provide adequate monitoring in accordance with IRM requirements, we recommend that the Commissioner ensure that all final candling activities are consistently located in a restricted access area.

To reduce the vulnerability of receipts found outside restricted access areas, we recommend that the Commissioner provide secure containers for service center employees to store “discovered remittances” prior to inventory and submission to the Receipt and Control Branch. Immediately upon discovery, the receipts should be recorded into a control log, the receipts secured in a locked container, and the discovered receipts reconciled to the control log prior to submission for processing.

To reduce the vulnerability of receipts that are especially susceptible to theft and misuse, we recommend that the Commissioner ensure that all unmatched checks are stored in locked containers until they can be researched and processed for deposit.

To reduce the vulnerability of returned refund checks to theft, we recommend that the Commissioner ensure that all returned refund checks are stamped “non-negotiable” as soon as they are extracted.

To better safeguard receipts at district offices, we recommend that the Commissioner require district office employees to store walk-in payments in secure containers in accordance with IRM 1(16)(41), section 500. District office management should ensure that this policy is followed and should limit the number of employees with access to the keys or combination to these containers.

To improve accountability for walk-in payments received, we recommend that the Commissioner ensure that these receipts are recorded in a control log prior to depositing the receipts in the locked container and ensure that the control log information is reconciled to receipts prior to the submission of the receipts to another unit for payment processing. To ensure proper segregation of duties, the reconciliation should be performed by an employee not responsible for logging receipts in the control log.

Courier Security Does Not Adequately Protect Deposits and Sensitive Taxpayer Data From Theft or Loss

Proper safeguarding of assets requires that IRS ensure adequate security over receipts from the time they are received at the service center until the time they are deposited at financial depository institutions. However, at all four service centers we visited, receipts for deposits were picked up from the service centers by a single unarmed, plain-clothes courier for delivery to the depositing bank. During our visits, these couriers were entrusted with transporting peak season deposits ranging from \$100 million to almost \$200 million for each deposit twice a day. At one district office, we observed that the courier was a bicycle messenger entrusted with over \$1 million of receipts during nonpeak season to more than \$100 million per deposit during the peak season.

Deposits were also improperly safeguarded during pickup. At one service center, we observed that the courier left deposits unattended in the car while he returned inside the service center to pick up another batch of deposits. At another service center, we observed that the courier left deposits worth over \$200 million unattended in the vehicle with the window open while he returned a borrowed cart to the interior of the service center. Onlookers at this service center were aware of the nature of the courier's visit.

According to a commercial bank and courier company officials, banking industry practice is generally to use unarmed couriers to transport checks and armored vehicles to transport currency. Therefore, IRS' current practice of transporting checks via unarmed couriers is similar to current banking industry practices.¹² However, because of the magnitude of IRS' deposits, both in dollars and the number of checks, and the sensitivity of

¹²At the sites we visited, IRS converted any currency received into cashiers' checks, usually at a credit union located on IRS premises. Therefore, at these sites, deposits transported by the couriers consisted only of checks.

taxpayer information contained on the checks,¹³ the security provided by the unarmed courier services may be inadequate to meet IRS' responsibility to protect government assets and personal taxpayer information.

During the peak filing season, one service center deposit typically has tens of thousands of checks. If a deposit were lost or stolen, IRS would have to expend substantial efforts to initiate actions to recover stolen checks and prevent them from being negotiated. However, even if stolen checks are not cashed, they can be used for check cloning schemes, and sensitive personal information on these checks can be used to perpetrate identity fraud. Such an incident of loss or theft could result in the loss of funds and financial damage and could impose considerable burden on the taxpayers. Any such incident would greatly reduce the taxpayer's confidence in IRS' ability to safeguard tax receipts and the taxpayer's personal data.

Due to differences in courier contracts, IRS is not consistently covered in the event of deposits being lost, stolen, or damaged in transit. In some contracts, the bank provides the courier service and the liability insurance for deposits in transit. In these instances, the bank is liable for the loss, theft, or destruction of any deposit from the time it is picked up from IRS by the bank's courier. If the deposits are stolen, the bank is liable for any loss that IRS cannot recover after IRS has notified the taxpayers, issued stop payment orders, and received replacement checks. However, in other cases where IRS directly contracts with the courier service, the courier service is only liable up to the limit specified in the contract. This limit varies between \$350,000 in a contractual agreement for one service center to \$1 million for another service center, while other contracts did not specifically refer to liability coverage. Because of the high dollar value and the volume of checks involved in one peak season shipment of deposits, the government could be exposed to losses which exceed the courier's contractual liability if all the lost or stolen checks cannot be recovered.

We also observed inconsistencies in the physical access rights to service centers that IRS provided to the couriers. At three of the service centers, IRS employees delivered the daily deposits from the Receipt and Control Branch to the couriers in the lobby or outside the building. However, at one service center, the courier was provided a restricted access area badge after checking in with the guard. This type of badge provided the courier greater access within the service center than most service center employees because it entitled the courier access to both unrestricted and

¹³Most checks received by service centers are processed through the Remittance Processing System, which automatically encodes the back of each check with the taxpayer's social security number.

restricted areas within the service center. This courier then proceeded to walk unescorted through the service center where tax returns were processed and entered the payment processing area through one of the restricted access doors not guarded by a door monitor. Because tax returns were stored unsecured and sometimes unattended throughout the service center and unprocessed receipts were stored in open baskets throughout the payment processing area, taxpayer data and checks were accessible to an individual who did not have a need to access them.

Recommendations

To ensure that IRS meets its responsibility to protect government assets and taxpayer information, we recommend that the Commissioner study the feasibility of improving security for its deposits in transit. In conducting this study, IRS should consider a number of alternatives, including the use of depositories in closer proximity to its various field locations and employing security guards to accompany couriers to the depositories.

To limit exposure to losses of deposits in transit, we recommend that the Commissioner develop a policy to ensure that contracts related to courier services do not unduly expose the government to losses in the event of lost, stolen, or damaged deposits in transit.

To limit courier access to sensitive taxpayer information and unguarded receipts in the Receipt and Control Branch, we recommend that the Commissioner ensure that courier access is limited to service center premises. Deposit unit employees should deliver the deposits to couriers waiting at the guard station instead of providing couriers badges allowing them unnecessary service center access.

Agency Comments and Our Evaluation

In commenting on this report, the Commissioner of Internal Revenue generally agreed with our findings and recommendations and noted that IRS has or would be taking action to address the issues raised in the report. These actions include

- conducting an analysis of risk classifications of positions in the Receipt and Control Branch to ensure background checks are commensurate with the level of risk associated with the position;
- ensuring IRS has the necessary equipment to participate in the FBI's Integrated Automated Fingerprint Identification System program by August 1999;

-
- working with each service center to determine appropriate methods for securing overflow areas and ensuring all final candling areas are located in restricted access areas;
 - exploring various options for security containers for unmatched checks and implementing a process for such storage by August 1999;
 - revising procedures to require stamping all returned refund checks “non-negotiable” as soon as they are extracted from envelopes;
 - revising procedures for safeguarding receipts received in walk-in facilities and for maintaining a control log of receipts received and deposited or transferred to another unit by January 1999; and
 - studying alternative methods for transporting deposits to depositories and service center practices for limiting courier access to service centers.

These actions are generally consistent with the recommendations contained in our report and, if effectively implemented, would assist IRS in reducing the risk of loss or misuse of receipts and taxpayer information. However, there are a number of our recommendations for which IRS’ responses do not appear to adequately address. Specifically, IRS stated it would work with the Office of Personnel Management and IRS’ General Legal Services to determine when job applicants can be fingerprinted and would, to the extent possible, prohibit new employees from processing receipts until the results of fingerprint checks are received and reviewed by management. However, IRS noted that to wait for the results of fingerprint checks before hiring seasonal employees in the service centers would adversely affect IRS’ ability to collect and process tax returns. IRS also stated that it would not always be possible to prohibit new employees from processing receipts during its April peak returns processing period. However, it is particularly during these peak periods when receipts and taxpayer information are most susceptible to theft. Consequently, we believe that to further reduce such risk, IRS should carefully consider the need to have fingerprint checks performed prior to hiring new employees and have the results of all fingerprint checks reviewed prior to allowing personnel to handle taxpayer receipts and data.

With regard to our recommendation that IRS provide secure containers for service center employees to store discovered remittances prior to inventory and submission to the Receipt and Control Branch and to maintain an inventory of these remittances on a control log, IRS noted that it currently has procedures which require service centers to store such remittances in a secure container and to record remittance information. However, we found that these procedures were not uniformly followed by the service centers. Consequently, IRS will need to be proactive in

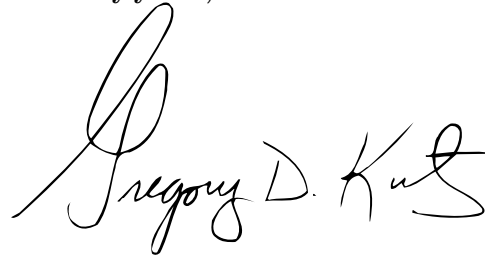
providing secure containers to the service centers and in ensuring records are maintained of discovered remittances.

This report contains recommendations to you. The head of a federal agency is required by 31 U.S.C. 720 to submit a written statement on actions taken on these recommendations. You should send your statements to the Senate Committee on Governmental Affairs and the House Committee on Governmental Reform and Oversight within 60 days after the date of this letter. A written statement also must be sent to the House and Senate Committees on Appropriations with the agency's first request for appropriations made over 60 days after the date of this letter.

We are sending copies of this report to the Secretary of the Treasury and the Director of the Office of Management and Budget. We are also sending it to the Chairmen and Ranking Minority Members of the Senate Committee on Appropriations and its Subcommittee on Treasury and General Government; Senate Committee on Finance and its Subcommittee on Taxation and IRS Oversight; Senate Committee on Governmental Affairs; Senate Committee on the Budget; House Committee on Appropriations and its Subcommittee on Treasury, Postal Service, and General Government; House Committee on Ways and Means; House Committee on Government Reform and Oversight and its Subcommittee on Government Management, Information and Technology; House Committee on the Budget; and other interested congressional committees. Copies will be made available to others upon request.

Please contact me at (202) 512-9505 or Steven J. Sebastian, Assistant Director, at (202) 512-9521 if you or your staff have any questions concerning this report. Major contributors to this report are listed in appendix II.

Sincerely yours,

A handwritten signature in black ink that reads "Gregory D. Kutz". The signature is written in a cursive style with a large, stylized initial "G".

Gregory D. Kutz
Associate Director, Governmentwide Accounting
and Financial Management Issues

Comments From the Internal Revenue Service

Note: GAO comments supplementing those in the report text appear at the end of this appendix.



COMMISSIONER

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

October 29, 1998

Mr. Gene L. Dodaro
Assistant Comptroller General
United States General Accounting Office
441 G Street, N.W.
Washington, D.C. 20548

Dear Mr. Dodaro:

Thank you for the opportunity to comment on your draft report, "Internal Revenue Service: Physical Security Over Taxpayer Receipts and Data Needs Improvement." We are generally in agreement with the findings and recommendations contained in the report. The following is our response to each recommendation:

RECOMMENDATION

To ensure that employees assigned to process receipts and sensitive taxpayer data are subjected to the appropriate level of background check, we recommend that the Internal Revenue Service (IRS) reevaluate the risk classification of all positions in IRS' Receipt and Control Branch and reclassify such positions where appropriate and in conformance with Office of Personnel Management (OPM) guidelines.

COMMENTS

We will conduct an analysis of the risk classification of positions in the Receipt and Control Branch and take action as appropriate to ensure that employees are subjected to the appropriate level of background check.

RECOMMENDATION

To reduce the incidence of applicants not subjected to fingerprint checks, we recommend that IRS Personnel management establish procedures to review the applications and associated documents for all applicants given job offers to ensure that fingerprint checks are initiated on these individuals. Personnel management should also provide supervisory feedback on these reviews as necessary to ensure that Personnel staff are aware of and follow IRS' policy requiring fingerprint checks on all applicants prior to their reporting for duty.

COMMENTS

The IRS has in place procedures regarding the fingerprinting of job applicants in the form of a Background Investigation Processing Guide. This guide clearly establishes the requirement that all applicants must be fingerprinted, and the fingerprints must be submitted to OPM (and subsequently forwarded to the Federal Bureau of Investigation (FBI)). These procedures are specific in nature, giving step-by-step directions on fingerprinting applicants. We are also working with OPM and our General Legal Services (GLS) to determine when a job applicant can legally be fingerprinted and, based on this determination, we will require the fingerprinting of applicants at the earliest possible time in the application process. Fingerprints are taken of all job applicants for whom job offers are made. 5 CFR 736.201(c) establishes that investigations must be initiated within 14 days of placement in the position, except for certain positions designated critical-sensitive where the investigation must be completed before placement unless a waiver is approved. There is no internal policy of waiting on fingerprint results prior to hiring individuals (with the above noted exception). To do so would adversely affect our ability to timely hire seasonal employees in the service centers and significantly impact the ability of the agency to collect and process tax returns.

It should be noted that although the turnaround time on fingerprints now exceeds 60 days, we have procured state-of-the-art live scan fingerprint equipment which is compatible with the FBI's Integrated Automated Fingerprint Identification System (IAFIS) scheduled for implementation in July 1999. We have expressed an interest with the FBI to be a pilot in its implementation of IAFIS. This may occur as early as February 1999. Once IAFIS is operational, fingerprint checks are expected to be completed in a 5-day period of time.

RECOMMENDATION

To assist in the timely receipt of fingerprint results of applicants, we recommend that IRS continue with its plans to develop and implement a policy to fingerprint filing season applicants on their first personal contact with the agency.

COMMENTS

We are working with OPM and our General Legal Services (GLS) to determine when a job applicant can legally be fingerprinted and based on this determination, we will require the taking of applicants fingerprints at the earliest possible time in the application process.

See comment 1.

RECOMMENDATION

To reduce the opportunity for employees with unsuitable backgrounds to steal receipts, we recommend that until the problems with delays in fingerprint checks are resolved, IRS develop and implement a policy prohibiting new employees from being assigned to process receipts until results of fingerprint checks are received and reviewed by management.

COMMENTS

We will, to the extent possible, prohibit new employees from being assigned to process receipts until results of fingerprint checks are received and reviewed by management. This may not always be possible, particularly during April peak when a large percentage of returns contain remittances. The centers are required by law to make deposits within a specified time frame of receipt. This problem should be resolved when IAFIS is implemented.

RECOMMENDATION

To provide suitability information on a more timely basis, we recommend that IRS continue its efforts to explore the feasibility of obtaining local police checks on IRS applicants and evaluate the efficiency and effectiveness of the Philadelphia Service Center's electronic fingerprinting system in order to supplement FBI fingerprint checks and to ensure that, at a minimum, local arrest records are brought immediately to IRS' attention.

COMMENTS

We have had some success in implementing procedures for obtaining local police checks on applicants, and we are continuing to pursue this as an option.

RECOMMENDATION

In the long term, to decrease the turnaround time for FBI's fingerprint check results, we recommend that IRS continue with its efforts to negotiate with OPM and the FBI and procure the necessary equipment so that it can participate in FBI's IAFIS program by August 1999.

See comment 1.

COMMENTS

We have already procured the live scan fingerprint equipment which is compatible with IAFIS. It has been delivered to 17 sites across the country (including the 10 service centers) and is awaiting installation. Installation and training of systems administrators and operators are being scheduled and should be completed in the next 2 months. We will be ready to participate in IAFIS when it comes on line and has requested to be a pilot for the program.

RECOMMENDATION

To ensure that the mail extraction process takes place in a secure and restricted access area, as required by the Internal Revenue Manual (IRM), we recommend that IRS improve the physical security controls over receipts and returns stored in unsecured, overflow areas. These controls might include limiting unnecessary traffic by temporarily designating these overflow areas as restricted access areas and/or posting additional security guards over such areas during the peak filing season.

COMMENTS

We agree that all mail extraction processing should take place in a secure and restricted access area, as required by the IRM. We also agree that we must improve the physical security controls over receipts and returns stored in unsecured, overflow areas. However, due to unique service center issues such as available space, return volumes during peak processing, cost of securing overflow areas, etc., we will have to work with each individual service center to determine the best alternatives for securing overflow areas.

RECOMMENDATION

To limit exposure to theft and provide adequate monitoring in accordance with IRM requirements, we recommend that IRS consistently locate all final candling activities in a restricted access area.

COMMENTS

We agree that all final candling activities should be located in a restricted access area. We will work with the service centers to ensure that they comply with this IRM requirement.

RECOMMENDATION

To reduce the vulnerability of receipts found outside restricted access areas, we recommend that IRS provide secure containers for service center employees to store "discovered remittances" prior to inventory and submission to the Receipt and Control Branch. Immediately upon discovery, the receipts should be recorded into a control log, the receipts secured in a locked container, and the discovered receipts reconciled to the control log prior to submission for processing.

COMMENTS

Current instructions require the service centers to store "discovered remittances" in a secure container and record the information on Form 4287, Record of Discovered Remittance. The Deposit Activity Unit is responsible for verifying information contained on Form 4287 is accurate and complete. These instructions are contained in IRM 3.8.43 (Service Center Deposit Activity).

RECOMMENDATION

To reduce the vulnerability of receipts which are especially susceptible to theft and misuse, we recommend that IRS store unmatched checks in locked containers until they can be researched and processed for deposit.

COMMENTS

We agree with your recommendation that checks not properly secured are vulnerable to theft and misuse. We will survey the centers to determine if they have suitable containers. If not, we will explore the various types of security containers, i.e., cabinets, safes, etc., to determine the type that would be suitable to unmatched remittances. Once the type of container has been selected, if needed, one will be purchased for each center. The process for storing unmatched checks in locked containers will be in place by August 1999.

RECOMMENDATION

To reduce the vulnerability of returned refund checks to theft, we recommend that IRS stamp all returned refund checks "non-negotiable" as soon as they are extracted.

See comment 1.

COMMENTS

We agree that returned refund checks should be stamped "non-negotiable" as soon as they are extracted. We will issue a Production Evaluation Report effective on receipt and also revise IRM 3.10.72 (Extracting, Sorting and Numbering) to include this procedure for January 1, 1999.

RECOMMENDATION

To better safeguard receipts at district offices, we recommend that IRS require district office employees to store walk-in payments in secure containers in accordance with IRM 1(16)41, Section 500. District office management should ensure that this policy is followed and should limit the number of employees with access to the keys or combinations to these containers.

COMMENTS

By January 1, 1999, guidelines for safeguarding receipts of cash payments received in walk-in facilities will be contained in IRM 21.1.6, Walk-in Procedures, Section 6.6.3.1, Procedures for Accepting Cash Payments. It provides instructions to assistors for maintaining receipts in a locked container in accordance with IRM 1(16)41, Physical Security Handbook.

RECOMMENDATION

To improve accountability for walk-in payments received, we recommend that IRS record these receipts in a control log prior to depositing the receipts in the locked container and ensure that the control log information is reconciled to receipts prior to submission of the receipts to another unit for payment processing. To ensure proper segregation of duties, the reconciliation should be performed by an employee not responsible for logging receipts in the control log.

COMMENTS

By January 1, 1999, guidelines for recording and reconciling receipts will be contained in IRM 21.1.6. Section 6.6.3.2, Preparation of Forms 795, Daily Report of Collection Activity, provides guidance to assistors for completion each workday of forms for accounting for monies collected and receipts issued. Detailed instructions are provided in the completion of Form 795 by the walk-in operator prior to submitting for payment processing by the Teller Unit.

RECOMMENDATION

To ensure that IRS meets its responsibility to protect government assets and taxpayer information, we recommend that IRS study the feasibility of improving security for its deposits in transit. In conducting this study, IRS should consider a number of alternatives, including the use of depositories in closer proximity to its various field locations and employing security guards to accompany couriers to the depositories.

COMMENTS

We agree that enhancements are needed to protect the Government's assets and taxpayer information. We will research the various security methods available for transporting deposits to the depository and determine which one will ensure that the Government's assets are not exposed to losses of deposits while in transit. New procedures will be in place by August 1999.

RECOMMENDATION

To limit exposure to losses of deposits in transit, we recommend that IRS develop a policy and to ensure that contracts related to courier services do not unduly expose the Government to losses in the event of lost, stolen, or damaged deposits in transit.

COMMENTS

We agree that enhancements are needed to protect the Government's assets and taxpayer information. We will research the various security methods available for transporting deposits to the depository and determine which one will ensure that the Government's assets are not exposed to losses of deposits while in transit. New procedures will be in place by August 1999.

RECOMMENDATION

To limit courier access to sensitive taxpayer information and unguarded receipts in the Receipt and Control Branch, we recommend that IRS limit courier access to service center premises. Deposit unit employees should deliver the deposits to couriers waiting at the guard station instead of providing courier badges allowing them unnecessary service center access.

COMMENTS

We agree that IRS should limit courier access to service center premises. We will study how each service center is currently delivering the deposits to couriers and implement procedures that limit courier access to service centers.

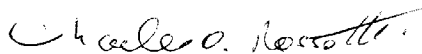
CONCLUSION

We recognize that financial crimes and identity fraud committed through the theft of receipts and tax return data not only harm the government but taxpayers and banks as well. We are committed to mitigating this risk by establishing and maintaining adequate physical controls over receipts and taxpayer data. We appreciate your acknowledgment of the steps already taken to reduce our vulnerability. The Summary Action Plan for the Protection of Monetary Instruments and the action plan developed as a result of the task team on recruitment background and security investigations address specific actions for mitigating risk. Many of the action items are completed or are in process.

Please include our response to the draft report in the appendix of the final report.

If you have any questions, please call John Dalrymple, Chief Operations Officer, or a member of your staff may contact Hugh Barrett at 622-7051.

Sincerely,



Charles O. Rossotti

**Appendix I
Comments From the Internal Revenue
Service**

The following is GAO's comment on the Internal Revenue Service's letter dated October 29, 1998.

GAO Comment

1. Discussed in the "Agency Comments and Our Evaluation" section.

Major Contributors to This Report

**Accounting and
Information
Management Division,
Washington, D.C.**

Steven Sebastian, Assistant Director
Charles Fox, Assignment Manager
Paul Foderaro, Assignment Manager

Atlanta Field Office

Aditi Archer, Senior Auditor
Alva Archie, Auditor
Veronica Mayhand, Auditor
Angel Sharma, Auditor

Dallas Field Office

George Jones, Senior Auditor
Ellen Wolfe, Senior Auditor
Michael Coy, Senior Auditor
Leonard Zapata, Senior Auditor

**San Francisco Field
Office**

Ellen Rominger, Senior Auditor
Laurie King, Auditor

**Los Angeles Field
Office**

Barbara House, Senior Auditor
Stacey Osborn, Auditor

Seattle Field Office

Doreen Eng, Assistant Director
Delores Lee, Auditor-In-Charge
Tuyet-Quan Thai, Auditor-In-Charge
Pat Seaton, Senior Auditor

Ordering Information

The first copy of each GAO report and testimony is free. Additional copies are \$2 each. Orders should be sent to the following address, accompanied by a check or money order made out to the Superintendent of Documents, when necessary. VISA and MasterCard credit cards are accepted, also. Orders for 100 or more copies to be mailed to a single address are discounted 25 percent.

Orders by mail:

U.S. General Accounting Office
P.O. Box 37050
Washington, DC 20013

or visit:

Room 1100
700 4th St. NW (corner of 4th and G Sts. NW)
U.S. General Accounting Office
Washington, DC

Orders may also be placed by calling (202) 512-6000 or by using fax number (202) 512-6061, or TDD (202) 512-2537.

Each day, GAO issues a list of newly available reports and testimony. To receive facsimile copies of the daily list or any list from the past 30 days, please call (202) 512-6000 using a touchtone phone. A recorded menu will provide information on how to obtain these lists.

For information on how to access GAO reports on the INTERNET, send an e-mail message with "info" in the body to:

info@www.gao.gov

or visit GAO's World Wide Web Home Page at:

<http://www.gao.gov>

**United States
General Accounting Office
Washington, D.C. 20548-0001**

**Bulk Rate
Postage & Fees Paid
GAO
Permit No. G100**

**Official Business
Penalty for Private Use \$300**

Address Correction Requested

