The Internal Revenue Service Should Take Additional Actions to Protect Taxpayer Remittances

September 2000

Reference Number: 2000-30-153

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

INSPECTOR GENERAL
for TAX
ADMINISTRATION

September 25, 2000

MEMORANDUM FOR COMMISSIONER ROSSOTTI

Pamela J. Gardiner

FROM: Pamela J. Gardiner
Deputy Inspector General for Audit

SUBJECT: Final Audit Report – The Internal Revenue Service Should Take Additional Actions to Protect Taxpayer Remittances

This report presents the results of our review of the security of remittances received at the Internal Revenue Service (IRS) Centers. The audit objective was to determine whether the IRS had taken corrective actions to reduce the risk of theft of taxpayer remittances in these IRS Centers.

In summary, we found that the IRS has significantly improved physical security and internal controls over taxpayer remittances and has improved the screening processes for job applicants. Despite these actions taken by the IRS, further improvements in the areas of physical security, certain control procedures, and the hiring process are necessary to safeguard taxpayer remittances.

We recommended that the IRS enhance physical security over remittance processing areas, ensure that controls designed to protect taxpayer remittances are functioning, and develop a process to help screen out questionable juvenile applicants for remittance processing jobs. Absent this, taxpayers and the federal government remain vulnerable to financial losses from theft.

Management's response was due on September 20, 2000. As of September 21, 2000, management had not responded to the draft report.

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

or your staff may call Gordon C. Milbourn III, Associate Inspector General for Audit (Small Business and Corporate Programs), at (202) 622-3837.

Table of Contents

Executive Summary

The Internal Revenue Service (IRS) processes over $100 billion per year through its IRS Centers. Without improvements to physical security and other controls at these Centers, taxpayer remittances are vulnerable to theft. Although current data on actual and alleged embezzlements by IRS employees were not available, an earlier IRS internal review[1] reported that, between January 1995 and July 1997, thefts of taxpayer remittances totaling over $5.3 million were investigated.

Recent audit reports issued by the IRS' Internal Audit function (now the Treasury Inspector General for Tax Administration [TIGTA]) and the General Accounting Office (GAO)[2] disclosed a variety of control weaknesses regarding the security of remittances in the IRS Centers. The objective of this audit was to determine whether the IRS had taken corrective actions to reduce the risk of theft of taxpayer remittances in these IRS Centers.

Results

The IRS has significantly improved physical security and internal controls over taxpayer remittances and has improved the screening processes for job applicants. Specific actions taken by the IRS include the following:

- Lockers have been installed at most IRS Centers, and restrictions have been placed on personal items taken into Remittance Processing functions.
- Security is discussed with Remittance Processing personnel on an ongoing basis.
- Areas receiving unopened mail directly from outside sources have been limited.
- Unauthorized IRS Center personnel have been restricted from accepting remittances from taxpayers.

---

[1] *Review of Remittance Processing Activities* (Reference Number 082503, dated March 1998), prepared by the IRS' Internal Security and Internal Audit (now TIGTA).

[2] These audit reports included the following:

- *Review of Remittance Processing Activities* (Reference Number 082503, dated March 1998).
- *Safeguarding Remittances at the Philadelphia Service Center* (Reference Number 681901, dated May 1998).
- *Immediate and Long-term Actions Needed to Improve Financial Management* (Reference Number GAO/AIMD-99-16, dated October 1998).
- *Physical Security Over Taxpayer Receipts and Data Needs Improvement* (Reference Number GAO/AIMD-99-15, dated November 1998).

- Security of remittances in transit from IRS Centers to banks has been improved, and courier contracts have been modified to limit the Government's exposure in the event of lost, stolen, or damaged deposits in transit.
- Policies have been issued restricting the hiring of new employees until fingerprint pre-screening checks have been completed.

Despite these actions taken by the IRS, further improvements in the areas of physical security, certain control procedures, and the hiring process are necessary to safeguard taxpayer remittances.

Physical Security Over the Internal Revenue Service's Remittance Processing Areas Still Needs Improvement

The IRS' physical facilities we reviewed did not meet IRS security standards. The IRS' procedures require that taxpayer remittances be maintained in areas which have been designed to limit access to authorized personnel during duty hours and to prevent undetected entry by unauthorized persons during non-duty hours. However, both of the IRS Centers included in our review had taxpayer remittances in non-secured areas.

The IRS chose not to install surveillance cameras to monitor employees as they are opening, extracting, and sorting mail and processing remittances. Although the IRS requires outside business entities that process remittances for the IRS to have functioning surveillance cameras, IRS officials determined that surveillance cameras in its Remittance Processing functions would not be effective deterrents to theft. The IRS' decision not to use surveillance cameras was based on limited and sometimes inaccurate information.

Some Control Procedures Designed to Protect Taxpayer Remittances Were Not Functioning as Intended

The IRS did not always ensure only authorized employees entered areas with remittances. The Executive Officer for Service Center Operations (EOSCO) issued guidelines to improve the security over remittances. However, only one of the seven Remittance Processing areas we reviewed had copies of the current EOSCO guidelines.

In both of the IRS Centers included in our review, cleaning personnel's access to Remittance Processing areas had not been limited as it should have been. Managers at the two IRS Centers we reviewed were unaware of this problem.

Certain remittances that are particularly vulnerable to theft (e.g., returned refund checks) and remittances discovered outside Remittance Processing areas were not properly controlled. Although the IRS had agreed to correct control weaknesses over these remittances, the two IRS Centers included in our review had not implemented the agreed upon corrective actions.

The Internal Revenue Service's Hiring Processes for Employees Handling Taxpayer Remittances Need Further Improvement

The IRS employs juveniles (high school students) to process taxpayer remittances without a process to ensure that they meet minimum suitability requirements. During Fiscal Year 2000, the 2 IRS Centers included in our review had hired 192 juveniles to work in their Remittance Processing areas as of April 2000. All of these juveniles had fingerprint pre-screening checks completed. However, Title 18 of the Federal Criminal Code states that information about a juvenile's record may not be released when the request for information is related to an application for employment. Therefore, the case results from any arrest of these juveniles were unavailable to the IRS.

IRS employees in Remittance Processing functions handle thousands of taxpayer receipts and sensitive taxpayer information, which requires a high degree of public confidence and trust. Because of this, the IRS has specific needs in screening potential job applicants. These needs may not be met by the Office of Personnel Management's guidelines. However, the IRS has not issued guidelines to address these needs.

Summary of Recommendations

The Chief Operations Officer should ensure that physical security over remittances at all IRS Centers meets applicable requirements. The EOSCO and the Assistant Commissioner (Forms and Submission Processing) should implement control procedures designed to protect taxpayer remittances (including those addressed in previous IRS Internal Audit [now TIGTA] and GAO recommendations). Also, the Director, Personnel Services, should provide sufficient guidance to ensure that all job applicants for Remittance Processing functions (including juveniles) meet minimum suitability requirements unique to the IRS.

Management's Response: Management's response was due on September 20, 2000. As of September 21, 2000, management had not responded to the draft report.

Objective and Scope

The objective of this audit was to determine whether the IRS had taken corrective actions to reduce the risk of theft of taxpayer remittances in the IRS Centers.

The objective of this audit was to determine whether the Internal Revenue Service (IRS) had taken corrective actions to reduce the risk of theft of taxpayer remittances in the IRS Centers.

To accomplish our objective, we conducted walk-throughs, performed security reviews, interviewed IRS personnel, and reviewed documentation provided by IRS management including the National Director, Submission Processing, and the Executive Officer for Service Center Operations (EOSCO). We reviewed corrective actions taken by the IRS for the security of remittances received at all 10 IRS Centers and reviewed corrective actions implemented locally at 2 IRS Centers.

We conducted this audit from September 1999 to May 2000. The audit was conducted in accordance with *Government Auditing Standards*.

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

Background

The IRS processes millions of remittances totaling billions of dollars each year through its IRS Centers.

The IRS processes millions of remittances totaling billions of dollars each year through its IRS Centers. In Fiscal Year (FY) 1999 alone, the IRS processed remittances totaling over $100 billion.

Although current data on actual and alleged embezzlements by IRS employees were not available, an earlier IRS internal review[1] reported that, between

[1] *Review of Remittance Processing Activities* (Reference Number 082503, dated March 1998), prepared by the IRS' Internal Security and Internal Audit (now the Treasury Inspector General for Tax Administration [TIGTA]).

January 1995 and July 1997, thefts of taxpayers remittances totaling over $5.3 million were investigated.

Recent audit reports issued by the IRS' Internal Audit function (now TIGTA) and the General Accounting Office (GAO) disclosed a variety of control weaknesses regarding the security of remittances at IRS Centers.[2] Among these control weaknesses were inadequate physical security in Remittance Processing areas and inadequate screening of employees hired to handle taxpayer remittances.

The IRS Commissioner created a task team to review the problem of employee theft and embezzlement. In May 1998, the IRS issued an action plan which listed proposed actions to address the physical security weaknesses reported. In June 1998, the IRS issued another action plan proposing a series of specific actions to address control deficiencies related to the screening of employees hired to process remittances.

Results

While the IRS has made significant improvements, more are needed.

While the IRS has significantly improved physical security and internal controls over taxpayer remittances and has improved the screening processes for job applicants, more improvements need to be made.

[2] These audit reports included the following:

- *Review of Remittance Processing Activities* (Reference Number 082503, dated March 1998).
- *Safeguarding Remittances at the Philadelphia Service Center* (Reference Number 681901, dated May 1998).
- *Immediate and Long-term Actions Needed to Improve Financial Management* (Reference Number GAO/AIMD-99-16, dated October 1998).
- *Physical Security Over Taxpayer Receipts and Data Needs Improvement* (Reference Number GAO/AIMD-99-15, dated November 1998).

Actions taken by the IRS to address these issues include the following:

- Lockers have been installed at most IRS Centers, and restrictions have been placed on personal items taken into Remittance Processing functions.
- Security is discussed with Remittance Processing personnel on an ongoing basis.
- Areas receiving unopened mail directly from outside sources have been limited.
- Unauthorized IRS Center personnel have been restricted from accepting remittances from taxpayers.
- Security of remittances in transit from IRS Centers to banks has been improved, and courier contracts have been modified to limit the Government's exposure in the event of lost, stolen, or damaged deposits in transit.
- Policies have been issued restricting the hiring of new employees until fingerprint pre-screening checks have been completed.

Despite these actions taken by the IRS, further improvements are necessary to safeguard taxpayer remittances.

Physical Security Over the Internal Revenue Service's Remittance Processing Areas Still Needs Improvement

Because of the vulnerability of taxpayer remittances to theft, areas that handle remittances within the IRS Centers are kept separated from other areas within the IRS Centers. The IRS' procedures require increased security for these areas. Further, *Standards for Internal Control in the Federal Government* require that access to resources be limited to authorized individuals.

Recommendations made in recent years by the GAO and IRS Internal Audit (now TIGTA) addressed inadequate

As a result of some IRS inaction, taxpayer remittances continued to be vulnerable to theft, particularly during non-duty hours.

physical security over taxpayer remittances. While the IRS has taken action on some of these recommendations, many have not been completed. In some instances, the National Headquarters issued guidelines that were not implemented by the IRS Centers and in other instances, the IRS chose not to take corrective actions. As a result, taxpayer remittances continued to be vulnerable to theft, particularly during non-duty hours.

The IRS' physical facilities did not meet security standards for "secured areas"

IRS procedures require that taxpayer remittances be maintained in areas that have been designed to limit access to authorized personnel during duty hours and to prevent undetected entry by unauthorized persons during non-duty hours. At a minimum, these "secured areas" must meet the following criteria:

- The area must be enclosed by slab-to-slab walls[3] supplemented by periodic inspection, or the area may have partition-type walls supplemented by electronic intrusion devices.
- The number of entrances must be kept to a minimum, and all doors entering the space must be locked with appropriate locking devices.

Both of the IRS Centers included in our review had taxpayer remittances in non-secured areas.

Both of the IRS Centers included in our review had taxpayer remittances in non-secured areas. In one center, an area used to process taxpayer remittances was constructed of partitions on one side and was not supplemented by electronic intrusion detecting devices. Four other areas in this same center had the proper physical barriers to protect taxpayer remittances, but the barriers were not used properly. For example, doors to one of these areas were left open after hours, and door locks in two other areas did not meet minimum security requirements. Also, on two separate occasions after normal working hours, an auditor was able to enter areas

[3] Slab-to-slab walls must run from ground level to roof level, with no crawl spaces above or below through which intruders could enter.

containing taxpayer remittances at this center without being detected. Security guards stated they did not respond to motion sensor alarms because they assumed they were set off by janitors.

At the other IRS Center included in our review, taxpayer remittances were kept in areas with walls and locking doors. However, the walls were not slab-to-slab as required, and most of the areas were not supplemented by electronic intrusion devises.

Local IRS officials expressed willingness to comply with requirements to secure taxpayer remittances. However, they must secure or free up necessary funds and must rely on Agency-Wide Shared Services to get the upgrades completed.

Responsibility for security of remittances at the IRS Centers was divided among several IRS executives. Policy was set by the National Director, Submission Processing. Implementation of policy was the responsibility of the EOSCO. Finally, security reviews and oversight were the responsibility of the Director, Security, Evaluation, and Oversight.

The IRS chose not to install surveillance cameras to monitor employees as they are opening, extracting, and sorting mail and processing remittances

The GAO recommended that the IRS consider installing surveillance cameras to reduce vulnerabilities in its Remittance Processing areas. The IRS requires outside business entities that process remittances for the IRS to have functioning surveillance cameras.

Although they place this requirement on outside business entities, IRS officials determined that surveillance cameras would not be effective deterrents to theft.

Although they place this requirement on outside business entities, IRS officials determined that surveillance cameras would not be effective deterrents to theft. They based this decision, at least in part, on their belief that other security enhancements were in place and functioning, including slab-to-slab walls around Remittance Processing areas, motion sensors under raised floors and above ceilings where slab-to-slab walls could not be constructed, intrusion detection and alarm devices, and repairs to doors and locks. However, as

discussed earlier, these enhancements were not in place and functioning in the IRS Centers we visited. In addition, personnel in the office of the EOSCO informed us that when making their decision not to install surveillance cameras, they relied on the expertise of the Security Standards and Evaluation function (SSE). They said the SSE had contacted private banking and gaming firms and found that cameras were expensive and ineffective. Neither the EOSCO nor the SSE could provide documentation of any analysis performed of the cost or benefits of surveillance cameras.

Recommendations

1. The Chief Operations Officer should ensure that physical security over remittances at all IRS Centers meets applicable requirements. He should work with Agency-Wide Shared Services to ensure that high priority is given to providing slab-to-slab walls or intrusion detection devices in all Remittance Processing areas and that doors entering the spaces are locked with appropriate locking devices.
2. The Chief, Agency-Wide Shared Services, should issue and enforce guidelines requiring security guards to respond to all intrusion alarms in secured areas.
3. Because the decision not to use surveillance cameras was based on limited and sometimes inaccurate information, the EOSCO should re-evaluate the option of installing surveillance cameras to monitor staff when they are opening, extracting, and sorting mail and processing remittances.

Management's Response: Management's response was due on September 20, 2000. As of September 21, 2000, management had not responded to the draft report.

Some Control Procedures Designed to Protect Taxpayer Remittances Were Not Functioning as Intended

To reduce the vulnerability of taxpayer remittances to theft, the IRS requires that areas handling remittances be "restricted areas." Specific procedures are to be followed in these areas to ensure that only authorized personnel enter the area. For example:

- Entrances must be controlled during duty hours by employees specifically assigned to monitor doors to ensure that only authorized persons enter the areas.
- Employees assigned to the areas must wear authorized IRS restricted area identification cards.
- Visitors must sign-in and be approved prior to entering the areas.

Because control procedures designed to protect taxpayer remittances were not functioning as intended, taxpayer remittances were unnecessarily put at risk for theft.

Recommendations made by the GAO and IRS Internal Audit (now TIGTA) addressed control procedures over taxpayer remittances. The IRS has taken action on some of these recommendations, but control procedures need improvement to adequately protect taxpayer remittances. Because control procedures designed to protect taxpayer remittances were not functioning as intended, taxpayer remittances were unnecessarily put at risk of theft.

The IRS did not always ensure only authorized employees entered areas with remittances

On two separate occasions during duty hours, an auditor was able to enter one remittance processing area unnoticed by employees or supervisors in the area.

On two separate occasions during duty hours, an auditor was able to enter one Remittance Processing area unnoticed by employees or supervisors in the area. No door monitor was present on either of these occasions. In Remittance Processing areas at both IRS Centers included in our review, visitors were regularly allowed in the areas by door monitors without approval by a supervisor.

The EOSCO issued guidelines for door monitors to improve the security over remittances. However, only one of the seven Remittance Processing areas we reviewed had copies of the current EOSCO guidelines.

Remittance Processing areas were accessible to cleaning personnel during non-business hours

In one of the IRS Centers included in our review, security guards did not respond to motion sensor alarms set off by an auditor before regular duty hours. The security guards stated they assumed that the alarms were set off by the janitor who was generally in the Remittance Processing area at that time of the morning. In the other IRS Center included in our review, nine janitors had restricted area identification badges and key cards that allowed them 24-hour access to the Remittance Processing areas. After the last shift of the day, IRS supervisors locked the doors accessed by these key cards. However, if left unlocked, janitors could use key cards to gain access to Remittance Processing areas. In a review performed by the SSE in 1997, reviewers found a janitor in one of the Remittance Processing areas after hours with no IRS employees present.

Cleaning personnel should only be given access to Remittance Processing areas when authorized personnel are present to supervise. In both of the IRS Centers included in our review, management was unaware that janitors had access to Remittance Processing areas before or after regular duty hours.

Unmatched checks and returned refund checks were not properly secured

Certain remittances processed by the IRS, such as unmatched checks and returned refund checks, are particularly vulnerable to theft.

Certain remittances processed by the IRS, such as unmatched checks and returned refund checks, are particularly vulnerable to theft.

- Unmatched checks are those checks that are inadvertently separated from their accompanying vouchers or tax returns or are mailed to an IRS Center without any instructions from the taxpayers as to how the payments should be applied. Without these instructions, such checks must be set aside until they can be researched to determine which taxpayers' accounts should be credited.
- Returned refund checks are checks from the United States (U.S.) Treasury that are sent to taxpayers and

subsequently returned uncashed to the IRS. Sometimes these checks are endorsed by taxpayers, making them highly negotiable.

Unmatched Checks

In both of the IRS Centers included in our review, unmatched checks were stored in open containers within the remittance processing areas until they could be researched and processed for deposit.

In both of the IRS Centers included in our review, unmatched checks were stored in open containers within the Remittance Processing areas until they could be researched and processed for deposit. This condition was previously reported to the IRS by the GAO.

In response to a GAO recommendation to store unmatched checks in locked security containers, the IRS stated that necessary containers would be purchased and the process for storing unmatched checks in the containers would be in place by August 1999. However, in a memorandum dated April 5, 1999, the National Director, Submission Processing, instructed the IRS Center Directors that if their Receipt and Control areas met secured area requirements, they did not need to provide the additional security for unmatched checks. Although neither of the Receipt and Control areas in the IRS Centers included in our review met secured area requirements, they did not provide the additional security over unmatched checks as recommended by the GAO.

Returned Refund Checks

Current IRS procedures require refund checks returned to the IRS by taxpayers to be stamped "non-negotiable." Until November 1998, the procedures did not specifically state when this should be done. However, in response to recommendations by the GAO, the IRS issued instructions to all of its centers stating that all returned refund checks should be overstamped "non-negotiable" as soon as they are removed from their envelopes. The Internal Revenue Manual was also revised to reflect these instructions.

Neither of the two IRS Centers included in our review was stamping returned refund checks "non-negotiable" immediately after the checks were removed from their envelopes.

Neither of the two IRS Centers included in our review was stamping returned refund checks "non-negotiable" immediately after the checks were removed from their envelopes. Management at the two IRS Centers expressed concerns that employees opening mail did not have the expertise to identify checks to be stamped "non-negotiable." They stated that returned refund checks look similar to other checks drawn on the U.S. Treasury. Many of these other checks are meant to be negotiated, such as checks from other government agencies for payment of withholding taxes or levied wages. Once these checks have been stamped "non-negotiable," they require special procedures to be made negotiable again.

Remittances discovered outside of Remittance Processing areas were not adequately accounted for and secured

Because of the high volume of mail processed at the IRS Centers, cash and/or checks are sometimes erroneously overlooked in the mail Extracting function. As tax returns are processed in other areas of the IRS Centers, these overlooked remittances are subsequently discovered. In addition, a few functions in the IRS Centers receive their mail directly, without it being opened in the Extracting function. Occasionally, this mail will contain taxpayer remittances.

To reduce the risk of theft of remittances discovered outside of the Remittance Processing areas, the IRS requires these remittances to be immediately documented on a Record of Discovered Remittances (Form 4287) and to either be delivered immediately to the Deposit function or secured in a locked container. The key to the locked container should be maintained by a designated Deposit function employee.

At the IRS Centers included in our review, adequate control and/or accountability was not maintained over discovered remittances.

At the IRS Centers included in our review, adequate control and/or accountability was not maintained over discovered remittances. In one center, most remittances discovered outside the Remittance Processing areas were placed in an open box in an unsecured area and never documented on Form 4287. Several times

throughout the day, the contents of the box were delivered to the Remittance Processing function. In the other IRS Center, all discovered remittances were properly documented. However, not all functions that might discover remittances had locking containers. Those areas that did have locking containers took the remittances out of the containers and placed them in an unsecure envelope prior to delivering them to the Remittance Processing function.

In response to prior findings regarding the security of discovered remittances, the IRS issued a memorandum to all IRS Centers reinforcing the need to follow established procedures when remittances were discovered outside of Remittance Processing areas. Local management at both of the IRS Centers included in our review chose not to follow the memorandum.

Recommendations

4. The EOSCO should ensure that all Remittance Processing functions receive and implement guidelines for door monitors.
5. The EOSCO should ensure that cleaning personnel have access to Remittance Processing areas only when IRS personnel are present.
6. As previously agreed to, the Assistant Commissioner (Forms and Submission Processing) should ensure that unmatched checks are stored in locked containers until they can be researched and processed for deposit.
7. The Assistant Commissioner (Forms and Submission Processing) should either train Remittance Processing personnel to properly stamp all returned refund checks “non-negotiable” as soon as they are removed from envelopes or develop an alternate method to reduce the vulnerability of returned refund checks to theft.
8. As previously agreed to, the Assistant Commissioner (Forms and Submission Processing) should ensure

that taxpayer remittances discovered outside Remittance Processing areas are immediately documented on Form 4287 and maintained in secured containers until they are delivered to the Deposit function.

The Internal Revenue Service's Hiring Processes for Employees Handling Taxpayer Remittances Need Further Improvement

Because IRS employees are entrusted with handling billions of dollars in taxpayer remittances each year, the IRS must take special precautions to ensure the integrity of its employees.

Because IRS employees are entrusted with handling billions of dollars in taxpayer remittances each year, the IRS must take special precautions to ensure the integrity of its employees. In recent years, the IRS has significantly improved the screening process of job applicants who will handle taxpayer remittances. The two IRS Centers included in our review had implemented a policy to fingerprint applicants at the earliest possible time in the job application process. They both participated in the Federal Bureau of Investigation's (FBI) Integrated Automated Fingerprint Identification System. In a memorandum issued to all Submission Processing Center Directors, the IRS' Deputy Commissioner Operations stated:

> *The IRS will not employ applicants in any of our offices unless the fingerprint checks and case dispositions have been completed. In the event that staff shortages occur, managers should take steps to move staff from work in less sensitive areas to cover needs. No applicants for employment who have not had their case dispositions completed may be hired and placed in any of our offices.*

Despite these actions, the IRS still needs to improve hiring practices.

The IRS employs high school students to process taxpayer remittances without a process to ensure that they meet minimum suitability requirements

Because of the cyclical nature of processing income taxes, the IRS has to use temporary employees who are hired for less than 90 days. The two IRS Centers included in our review often use high school students to fill these short-term positions. Many of these high school students are juveniles.

Federal regulations state that background investigations should be initiated within 14 days of placement into all positions except for certain high-risk positions, which must be completed before employees report to work. Temporary appointments of 90 days or less to low-risk positions, such as clerks in Receipt and Control functions, are the only cases for which an investigation need not be initiated. However, the IRS' policy requires that, at a minimum, all of these appointees must have a fingerprint pre-screening check completed. During this pre-screening check, an applicant's fingerprints are compared with information on the FBI's national database of arrest records. Although fingerprint results can identify if a job applicant was arrested, further review of the disposition of the case is necessary to determine if the applicant was convicted of the crime.

Case results from any arrest of a juvenile cannot be released if the information is related to an application for employment.

As of April 2000, the 2 IRS Centers included in our review had hired 192 juveniles to work in their Remittance Processing areas during FY 2000. All of these juveniles had fingerprint pre-screening checks completed. However, Title 18 of the Federal Criminal Code states that information about a juvenile's record may not be released when the request for information is related to an application for employment. It further states that responses to such inquiries shall not be different from responses made about persons who have never been involved in a delinquency proceeding. Therefore, the case disposition from any arrest of these juveniles could not be released.

The FBI's national database is dependent upon local law enforcement agencies for much of its information.

Because juveniles' records are sealed, it is not certain that local authorities would forward juvenile arrest records to the FBI. Even if a fingerprint screening identified the record of a juvenile's arrest, an investigator would not be able to determine the disposition of the case against the juvenile.

The recruiting specialists in the two IRS Centers included in our review indicated they relied on high school personnel to help screen out questionable applicants, but there were no guidelines issued by the IRS requiring them to contact schools or counselors. The EOSCO just recently issued informal guidelines recommending the IRS Centers require juvenile applicants to sign releases to allow their records to be accessed. However, requiring juvenile job applicants to provide evidence regarding their juvenile records as a condition of their being hired may not be in compliance with the intent of the Federal Criminal Code.

Placing juveniles into sensitive remittance processing jobs without determining their suitability may put taxpayer remittances at risk of theft.

Placing juveniles into sensitive Remittance Processing jobs without ensuring that an effective process exists to screen out questionable applicants may put taxpayer remittances at risk of theft. In fact, TIGTA Special Agents have investigated juveniles for theft of taxpayer remittances.

The IRS should consider issuing specific guidelines for recruiting personnel to help determine applicants' suitability for certain jobs

Recruiting personnel in the two IRS Centers included in our review expressed concern regarding not having specific guidelines to address the IRS' special needs for screening potential job applicants.

Part 5 of the Code of Federal Regulations (CFR) contains guidelines for determining applicants' suitability for U.S. Government jobs in general. The Office of Personnel Management (OPM) offers some supplements to these guidelines. These supplements also contain general guidelines regarding suitability for Government jobs in general.

IRS employees in Remittance Processing functions handle thousands of taxpayer receipts and sensitive taxpayer information each year. Because this requires a high degree of public confidence and trust, the IRS has specific needs in screening potential job applicants beyond those addressed by OPM's guidelines.

Applicants meeting OPM's general guidelines may be found suitable for employment even though they have been convicted of certain crimes within the last 3 years. The IRS Center recruiting personnel can object to hiring these individuals by preparing documentation and forwarding it to the OPM for consideration. If there is a nexus or relationship between the applicant's crime and the position for which he/she is applying, the OPM may sustain the IRS' objection and the individual will not be hired.

Management at the IRS has not issued specific instructions and criteria on when to object to a job applicant.

Management at the IRS has not issued specific instructions and criteria on what constitutes a valid nexus and when to prepare an objection document. As a result, an applicant meeting the general OPM suitability guidelines may be hired at one IRS Center where an applicant with a similar background may not be hired at another IRS Center. For example, an individual with only 1 conviction for theft within the last 3 years would meet the OPM suitability criteria and could be hired. However, if an IRS Center objected to hiring individuals with any history of theft to work in the Remittance Processing areas, it could prepare an objection document based on the type of work/type of conviction nexus and submit it to the OPM. If sustained, the applicant would not be hired even though he or she met the general OPM suitability guidelines. On the other hand, another IRS Center may not have the same strict standard and may hire the individual.

The two IRS Centers we visited were conscientiously preparing and submitting objection documents to the OPM to screen out questionable applicants. However, absent specific guidelines, there is no guarantee that all of the IRS Centers would have the same consistent high standards. This can result in job applicants being treated

The need for consistent suitability guidelines for remittance processing employees becomes more significant during the IRS' peak income tax filing season, when the IRS hires many temporary employees.

inequitably from IRS Center to IRS Center and in applicants being hired who may not instill public confidence in the IRS' ability to accomplish its mission.

This situation becomes more significant during the IRS' peak income tax filing season, when the IRS hires many temporary employees for periods of less than 90 days. The OPM has no adjudicative authority over the hiring of these employees and the need for IRS guidelines becomes even greater.

Recommendation

9. Because fingerprint pre-screening procedures are not effective for juvenile job applicants, the Director, Personnel Services, should develop a process to help screen out questionable juvenile applicants for Remittance Processing jobs.

10. The Director, Personnel Services, should provide guidelines establishing consistent minimum standards necessary for job applicants to be hired in Remittance Processing functions.

Conclusion

Although the IRS has significantly improved physical security and internal controls over taxpayer remittances received at the IRS Centers and the screening processes for job applicants, further enhancements are necessary. Absent this, taxpayers and the federal government remain vulnerable to financial losses from theft.

Appendix I

Detailed Objective, Scope, and Methodology

The objective of this audit was to determine whether the Internal Revenue Service (IRS) had taken corrective actions to reduce the risk of theft of taxpayer remittances in the IRS Centers.

To accomplish our objective, we conducted walk-throughs, performed security reviews, interviewed IRS personnel, and reviewed documentation provided by IRS management including the National Director, Submission Processing, and the Executive Officer for Service Center Operations. Our audit included a review of corrective actions taken by the National Headquarters for the nationwide security of remittances received at all 10 IRS Centers and a review of how corrective actions were implemented locally at 2 IRS Centers. Specifically, we performed the following audit tests.

I. Management corrective actions in general.

   A. Reviewed proposed management corrective actions from two 1998 IRS Internal Audit (now the Treasury Inspector General for Tax Administration [TIGTA]) and two 1998 General Accounting Office (GAO) audit reports[1] to determine whether these actions would correct the identified findings outlined in the reports.

   B. Reviewed the Treasury Department's Inventory Tracking and Control System, interviewed IRS personnel responsible for the corrective actions, and reviewed appropriate documentation to determine whether corrective actions were taken for each recommendation outlined in the four reports.

II. Management corrective actions regarding the fingerprinting and background checks of new hires at two IRS Centers.

[1] These four audit reports were:
- *Review of Remittance Processing Activities* (Reference Number 082503, dated March 1998).
- *Safeguarding Remittances at the Philadelphia Service Center* (Reference Number 681901, dated May 1998).
- *Immediate and Long-term Actions Needed to Improve Financial Management* (Reference Number GAO/AIMD-99-16, dated October 1998).
- *Physical Security Over Taxpayer Receipts and Data Needs Improvement* (Reference Number GAO/AIMD-99-15, dated November 1998).

A. Reviewed the Internal Revenue Manual (IRM), Background Investigation Processing Guide, and Staffing Handbook to identify the procedures required for processing new hires and the criteria required to determine suitability of an individual for employment.

B. Interviewed the Personnel Branch Chief and reviewed management and personnel records to determine whether the two IRS Centers:

1. Were following the proper procedures for processing new hires and were using the correct criteria to determine suitability of an individual for employment.

2. Had implemented corrective actions for all IRS Internal Audit (now TIGTA) and GAO recommendations identified in our review.

C. Conducted walk-throughs, analyzed procedures to process prospective and new employees, and conducted interviews to determine:

1. Whether the fingerprint screenings for filing season applicants were done at the earliest possible time in the job application process.

2. The amount of time it takes to receive fingerprint results back from the Federal Bureau of Investigation.

3. Whether the fingerprint screenings were done early enough in the job application process to allow managers adequate time to review the applicants' files before report-to-work certificates were issued.

4. Whether additional screening methods (such as vendors and state and local law enforcement checks) were used to obtain background information when fingerprint results could not be received and reviewed prior to employment.

5. Whether employees were prohibited from being assigned to process receipts until results of fingerprint checks were received and reviewed by management.

III. Management corrective actions regarding the physical security of remittances received at two IRS Centers.

A. Reviewed the IRM and identified the standards and requirements for the physical security of remittances.

B. Obtained National Headquarters reports containing data from all 10 IRS Centers to determine the volume and dollar amount of remittances processed in Fiscal Year 1999.

C. Interviewed the Processing Division Chiefs and the Receipt and Control Branch Chiefs and reviewed documentation to determine whether the two IRS Centers:

1. Were following the proper physical security standards and requirements for the security of remittances.

2. Had implemented corrective actions for all IRS Internal Audit (now TIGTA) and GAO recommendations identified in our review.

D. Conducted a physical security review of the Remittance Processing areas of the Receipt and Control Branches at the two IRS Centers to determine whether the requirements of a restricted and a secured area were being met.

1. Were the areas prominently posted as "Restricted" and separated from other areas by physical barriers to control access?

2. Were there a minimum number of entrances and were the entrances adequately controlled during duty hours by a responsible employee (door monitor) to assure that only authorized persons entered the areas?

3. Was access limited to authorized personnel and was admittance permitted only on a need-to-enter basis for all personnel not regularly assigned to work in the area?

4. Were all employees assigned to the areas wearing authorized IRS restricted area identification cards in the prescribed manner?

5. Were the following procedures followed to control the access of persons entering the restricted areas who are not assigned to the areas?

   a. Was a Restricted Area Register (Form 5421) maintained at the main entrance to the restricted area and was each person entering the restricted area, who is not assigned to the area, required to sign the Form 5421?

   b. Did the monitor properly complete the register by adding the individual's name, assigned work area, person to be contacted, purpose for entry, identification (ID) card number, and time and date of entry and departure?

   c. Did the monitor identify each visitor by comparing the name and signature entered in the register with the name and signature on the visitor's photo ID card?

d. Was entry approved by the supervisor responsible for the area and were visitors issued an appropriate restricted area non-photo ID card after verification of identity?

e. Was an Authorized Access List maintained to facilitate the entry of employees who have a frequent and continuing need to enter the restricted area, was it prepared monthly, and was it dated and signed by the Branch Chief indicating his/her approval of all names on the list?

6. Was the clean desk policy being observed and was sensitive information (including unopened mail, tax documents, and remittances) stored in a secured area or in locked containers when it was being distributed or processed or when otherwise not in the custody of an authorized IRS employee?

7. Were keys and lock combinations to doors, cash boxes, and security containers controlled and maintained as required?

8. Were cash boxes stored in an appropriate security container at the end of each workday?

9. Was the space enclosed by slab-to-slab walls constructed of approved materials and supplemented by periodic inspection to prevent undetected entry by unauthorized persons during non-duty hours, or was the space enclosed by any lesser type partition supplemented by motion sensors?

10. Were motion sensors or other electronic intrusion detection devices functioning and being monitored, or were all doors entering the space locked in accordance with IRM requirements to prevent undetected entry by unauthorized persons during non-duty hours?

11. Was the space cleaned by maintenance personnel during duty hours or in the presence of a regularly assigned employee during non-duty hours?

E. Conducted a walk-through of the Remittance Processing areas of the Receipt and Control Branches at the two IRS Centers to determine whether:

1. Incoming mail, not being distributed or processed, was stored in a secured area or in locked containers.

2. Mail extraction processes took place in restricted and secured areas.

3. All candling[2] activities were located in restricted and secured areas.

4. Lockers had been provided outside the Remittance Processing areas for storing employees' personal belongings.

5. Personal items that employees can bring into the Remittance Processing areas had been restricted.

6. Staff was properly monitored by management to ensure that the proper procedures were being followed.

F. Conducted an after-hours review of the Remittance Processing areas of the Receipt and Control Branches during non-working hours on 2 separate days at the 2 IRS Centers to determine whether the clean desk policy was being followed (i.e., remittances were properly secured when not under the direct and continuous supervision of authorized personnel) and security containers and doors to offices were being locked.

G. Conducted an after-hours review of the areas outside of the Receipt and Control Branch restricted areas during non-working hours on 2 separate days at the 2 IRS Centers to determine whether "discovered remittances" were stored in a locked container.

H. Selected a judgmental sample of 165 tax documents and correspondence opened in the Extracting function and routed to areas outside the Receipt and Control Branch at the 2 IRS Centers. The sample was selected from the work in process on the day of our visit. We reviewed these documents to determine whether any remittances had been overlooked in the extraction process.

I. Reviewed the procedures for processing unmatched checks at the two IRS Centers to ensure they were stored in locked containers until they were researched and processed for deposit.

J. Reviewed the procedures for processing returned refund checks at the two IRS Centers to ensure they were stamped "non-negotiable" as soon as they were extracted.

K. Observed the courier picking up daily deposits on 2 separate days at the 2 IRS Centers to verify that courier access to IRS Center premises had

[2] Candling is the process that allows IRS employees to recheck envelopes for missed contents. Envelopes are passed over a light which allows employees to see through most envelopes for contents that were missed in the extraction process.

been limited and to determine whether additional security procedures had been implemented to improve the security of deposits in transit.

L. Interviewed the security guards at the two IRS Centers to determine how they handled walk-in taxpayers who wanted to make a tax payment to ensure that unauthorized individuals did not receive taxpayer payments.

Appendix II

Major Contributors to This Report

Gordon C. Milbourn III, Associate Inspector General for Audit (Small Business and Corporate Programs)
Richard J. Dagliolo, Director
Kyle R. Andersen, Audit Manager
Roy E. Thompson, Senior Auditor
Scott Critchlow, Auditor
Annette B. Hodson, Auditor

Appendix III

Report Distribution List

Deputy Commissioner Operations C:DO
Chief Operations Officer OP
Commissioner, Small Business/Self-Employed Division S
Assistant Commissioner (Forms and Submission Processing) OP:FS
Chief, Agency-Wide Shared Services A
Chief, Personnel Security Office A:PS:PSO
Executive Officer for Service Center Operations OP:SC
Office of the Chief Counsel CC
Office of Management Controls CFO:A:M
National Director, Submission Processing OP:FS:S
National Taxpayer Advocate C:TA
Director, Legislative Affairs CL:LA
Director, Office of Program Evaluation and Risk Analysis M:O
Director, Personnel Services A:PS
Audit Liaisons:
- Chief Operations Officer OP
- Assistant Commissioner (Forms and Submission Processing) OP:FS
- Chief, Agency-Wide Shared Services A
- Submission Processing OP:FS:S:X