INSPECTOR GENERAL
for TAX
ADMINISTRATION

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

November 22, 2000

MEMORANDUM FOR COMMISSIONER ROSSOTTI

Pamela J. Gardiner

FROM: Pamela J. Gardiner
Deputy Inspector General for Audit

SUBJECT: Office of Audit's Comments Concerning Management's Response to the Audit Report, *"The Internal Revenue Service Should Take Additional Actions to Protect Taxpayer Remittances"*

This memorandum presents our concerns with the Internal Revenue Service's (IRS) management response to the audit report, *"The Internal Revenue Service Should Take Additional Actions to Protect Taxpayer Remittances"* (Reference Number 2000-30-153). The response to the report was received after the final report was released. Because of our significant concerns with the IRS' response to many of our recommendations and the repetitive nature of these findings, we intend to elevate this to the Assistant Secretary for Management and Chief Financial Officer of the Treasury for her consideration.

The IRS' response contains some factual errors regarding the number of potential and actual stolen payments and the availability of that data from the Office of Investigations. More importantly, we are concerned that the IRS plans to take no action in response to two of the ten recommendations in our report, and plans inadequate actions in response to four others.

The data from our report, management's response, and the Office of Audit's comments follow.

Executive Summary: The 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

reported that between January 1995 and July 1997, thefts of taxpayer remittances totaling over $5.3 million were investigated.

Management's Response: The report says that current information regarding thefts was not available. However, current information is available from the TIGTA Office of Investigations, which is responsible for investigating embezzlements of tax payments. Their office maintains current information about the number of potential and actual thefts/embezzlement.

In Fiscal Year (FY) 1999, TIGTA conducted an audit entitled "Additional Emphasis Is Needed to Identify and Resolve Thefts of Taxpayer Payments" (Audit No. 199940108). In this audit, they identified that the TIGTA, Office of Investigations, received reports of 54 potential thefts in FY 1999. Only 12 of the 54 potential thefts were determined to be stolen payments from Submission Processing Centers and Lockbox sites.

The TIGTA, Office of Investigations, reports 6 cases of embezzled payments involving $1,603 from the Submission Processing Centers for FYs 1999 and 2000 (to date). This illustrates an actual loss ratio of payments to receipts processed in the Submission Processing Centers of .0000016 percent.

Office of Audit Comment: TIGTA's Office of Investigations does not, in fact, maintain readily available information about the number of potential and actual thefts/ embezzlements. Because Special Agents may classify cases involving stolen payments in a variety of ways, the only way to obtain reliable data regarding the number of thefts is to manually review the narrative portion of each case entry on the Office of Investigations' Management Information System. To obtain this data nationwide requires a significant investment of staff time. The six cases totaling $1,603, referred to in the IRS' response, reflect cases referred to the IRS by the Office of Investigations. The Office of Investigations makes such referrals to request that injured taxpayers' accounts be credited after an embezzlement takes place. However, this figure in no way represents the total number of payments investigated as stolen from the IRS' Service Centers.

In some cases, stolen payments are not cashed and the Office of Investigations would not need to request that a taxpayer's account be credited. For example in one IRS Center in FY 1999, an IRS employee admitted stealing between 40 and 60 checks. None of these checks were cashed and therefore no request was necessary to credit any of the taxpayers' accounts. In the past, IRS employees have stolen checks which were not cashed, but were used to produce clones of the checks made out to different payees.

Also, not all thefts of remittances are identified by the IRS and referred for investigation. The audit report referred to by the IRS specifically states, "During our audit period, 54 instances of potential payment thefts were identified. While this is a relatively small number, the IRS did not have an effective process for identifying and controlling potential payment theft cases it received as direct referrals from taxpayers. The IRS did not

adequately train its employees to identify thefts of payments. As a result, the IRS cannot ensure that all instances of payment thefts have been identified and referred for investigation." Further, the General Accounting Office (GAO) has reported that the true magnitude of thefts of receipts and taxpayer data that have occurred within the IRS will likely never be known. In a 1998 report, GAO quoted an IRS Inspector who stated that during investigations, prosecuted individuals have confessed that they stole other checks but could not remember the details.

Recommendations for Which the IRS Plans No Corrective Actions

Recommendation number 3: Because the decision not to use surveillance cameras was based on limited and sometimes inaccurate information, the Executive Officer for Service Center Operations (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: The IRS determined that surveillance cameras would not effectively deter theft.

The IRS requires outside business entities that process remittances for the IRS (known as lockbox sites) to have functioning surveillance cameras. The lockbox sites do not perform the same functions as the service centers and do not have the same security. Our service centers have layered security – at the fence line, at the doors, and at the restricted area. We also have management controls in place.

Our Security, Evaluation and Oversight Office looked at the security operations of casinos in three cities. They have cameras focused on all tables and slot machines. The cameras only record events. They are not watched unless a casino employee sends a warning to watch a particular area. Their systems include routers, switches, cameras, and monitors.

For surveillance cameras to be effective at the service centers, they need to be focused on each work area. Because the work is spread over a large amount of the space, the number of cameras and monitors required for each service center would be enormous. Staff would be needed to constantly watch the monitors as well. Installation of surveillance cameras would also reduce our flexibility to move space or furniture within space.

OMB Circular A-123, Attachment II, Establishing Management Controls, states, "To help ensure that controls are appropriate and cost-effective, agencies should consider the extent and cost of controls relative to the importance and risk associated with a given program." The $1,603 of losses reported in FYs 1999 and 2000 and the 12 cases reported by TIGTA in 1999 do not justify the expense of cameras.

Office of Audit Comment: The layered security measures referred to by the IRS are designed mainly to restrict access to the IRS Centers, or to areas within the centers, not to stop employee embezzlement within the mail receipt and remittance processing functions. Also, as our report pointed out, many of the management controls established by the IRS to protect remittances are not functioning as intended.

In response to a prior GAO report, the IRS agreed to determine the feasibility of using surveillance cameras. To make this determination, IRS officials looked at casinos when they might have been better served to contact businesses that process payments similar to the IRS. For example, Discover Card utilizes surveillance cameras in its payment processing centers. We contacted the manager of one of Discover Card's payment processing centers. He believes the cameras are a very effective deterrent to theft. Information gained from visiting one of these payment processing sites may have provided more relevant data than that gathered from casinos.

Finally, in our opinion, the understated figures referred to in the IRS' response do not provide valid reasons for dismissing the use of surveillance cameras under Office of Management and Budget (OMB) Circular A-123. As discussed earlier, the IRS does not have an effective process for identifying and referring employee theft, and the numbers regarding thefts referred to by the IRS were not complete. More importantly, remittance processing functions have an inherently high risk associated with them. The fact that the IRS processes through its Centers over $100 billion in payments entrusted to them by taxpayers significantly increases the importance associated with this program. In our view, the use of surveillance cameras deserves more serious consideration than the IRS has apparently given it. We believe the risk of loss is real and legitimate, and the single factor of the cost of surveillance cameras alone should not prohibit their consideration.

Recommendation number 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.

Management Response: A January 1, 2000 Internal Revenue Manual (IRM) update directed the service centers to overstamp returned refund checks "non-negotiable" upon extraction. Feedback from the service centers indicated these procedures were resulting in the erroneous overstamping of many negotiable third party checks; therefore, we developed an alternate method. On May 4, 2000, an Information Alert (HQ-IA-210) was issued directing the service centers to place all returned refund checks in a designated bin upon extraction. The Lead/Manager will determine if the check should be overstamped and then stamp accordingly. No corrective action is planned.

Office of Audit Comment: The pertinent issue, discussed in our report and in a prior GAO report, is the amount of time returned refund checks are left vulnerable to theft. Immediately overstamping these checks minimizes this vulnerability. If the IRS opts not to immediately

overstamp the checks, it should develop an alternate method which reduces the vulnerability of the checks to theft. Placing returned refund checks in a designated bin awaiting a determination by the lead or manager leaves these checks vulnerable to theft, and does not comply with the minimum protection standards specified in the IRS' own Physical Security Standards Handbook. Chapter 5 of this handbook specifies that checks drawn on the U.S. Treasury must be stored in a security container, regardless of the area security provided, due to special access control needs.

Recommendations for Which the IRS Plans Inadequate Corrective Actions

Recommendation number 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.

Management's Response: Unmatched checks are researched and processed in the Receipt and Control area of the service center, which is a secured area. Only authorized employees have access. A representative of Forms and Submission Processing performs an annual unannounced security review at all 10 service centers. During the security review, we pay close attention to the correct handling of unmatched checks.

The Directors, Submission Processing of the new Operating Divisions will draft and forward a memorandum to the Submission Processing Service Center Directors reinforcing the importance of storing unmatched checks in a secure area.

Office of Audit Comment: Our report specifically points out that the Receipt and Control areas in the IRS Centers included in our review do not meet secured area requirements. Until the IRS completes its assessment of the physical security status of restricted areas and corrects deficiencies, it should ensure that unmatched checks are stored in locked containers regardless of the area they are processed in.

Recommendations number 4, 5, and 8: These recommendations discussed ineffective management controls. In each case, the IRS corrective action consists of discussing the issues and issuing memorandums or guidelines with no plans for follow-up to ensure the guidelines are followed. All three are repeat findings. In response to prior audit reports, the IRS issued similar guidelines which were not appropriately implemented at the Centers. Without proper follow-up, the IRS' corrective actions may result in the same inaction from its Centers that occurred previously.

We continue to believe the IRS needs to more fully address our recommendations. Therefore, we intend to elevate this to Treasury. You should submit a written reply to the Treasury Assistant Secretary for Management and Chief Financial Officer within 30 calendar days from the date of this memorandum. Your reply should explain the IRS'

reasons for not taking the specific corrective actions recommended in our report. You should also provide us with a copy of your reply.

Financial crimes and identity fraud committed through the theft of payments and associated tax return data can cause damage to many parties, including the federal government, financial institutions, and most importantly, the taxpaying public. Taxpayers expect and deserve to have their tax payments and personal tax information safeguarded in an environment where controls are fully in place to deter and detect criminal acts.

Copies of this memorandum are also being sent to the IRS managers who received a copy of the final report. 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.