

**Physical Security Can Be Improved to  
Maximize Protection Against Unauthorized  
Access and Questionable Mail**

**October 2002**

**Reference Number: 2003-20-004**



DEPARTMENT OF THE TREASURY

WASHINGTON, D.C. 20220

INSPECTOR GENERAL  
for TAX  
ADMINISTRATION

October 8, 2002

MEMORANDUM FOR CHIEF, AGENCY-WIDE SHARED SERVICES

*Pamela J. Gardiner*

FROM: Pamela J. Gardiner  
Acting Inspector General

SUBJECT: Final Audit Report – Physical Security Can Be Improved to  
Maximize Protection Against Unauthorized Access and  
Questionable Mail (Audit # 200220042)

This report presents the results of our review to evaluate the effectiveness of physical security measures implemented at Internal Revenue Service (IRS) facilities. We conducted this audit to address Congressional concerns over security in the IRS in the wake of the terrorist attacks of September 11, 2001, and subsequent Anthrax mailings.

A determined and experienced intruder can breach most lines of defense. Agencies like the IRS, which must offer public access to provide customer service, are particularly difficult to defend. With this in mind, the IRS has established adequate policies and procedures to protect its employees and to minimize the possibility of physical breaches. In addition, the IRS has implemented several physical security enhancements, such as canine units at all campuses for explosive detection and intruder deterrence, increased guard service, and redesigned mail handling to isolate questionable mail. However, security measures have not been consistently applied and IRS facilities were unnecessarily vulnerable to intruders and questionable mail.

In summary, we identified several security weaknesses at the offices we visited that could allow an intruder access to IRS facilities. We attributed the weaknesses to a lack of awareness and non-compliance with policies and procedures by employees and managers. Our results indicate that the heightened security awareness that occurred after September 11<sup>th</sup> may be waning.

We recommended that the Chief, Agency-Wide Shared Services (AWSS), issue guidance to re-emphasize security policies and procedures to address the security

weaknesses in this report. We also recommended that the IRS consider installing or repairing security devices (i.e., alarms, cameras, x-ray machines, metal detectors) and protective items (i.e., blast-resistant film for glass, high quality air filters) to strengthen physical security at IRS sites.

Management's Response: The Deputy Chief, AWSS, agreed with our recommendations. AWSS management will issue memoranda to emphasize security policies and procedures, continue to use the risk assessment process to determine the appropriate level of security for all facilities and to develop budget requirements for upgrade projects, and emphasize mail-handling procedures as part of the Campus Readiness process for the upcoming filing season.

Management's complete response to the draft report is included in Appendix V.

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

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

**Physical Security Can Be Improved to Maximize Protection  
Against Unauthorized Access and Questionable Mail**

---

**Table of Contents**

Background.....	Page 1
The Internal Revenue Service Has Taken Steps to Reduce the Risk of Security Threats.....	Page 2
Physical Measures Can Be Improved to Minimize Unauthorized Access to Internal Revenue Service Offices and External Attacks to Its Buildings.....	Page 3
<u>Recommendations 1 through 3:</u> .....	Page 6
Mail Handling Can Be Improved to Reduce the Risk of Employee Exposure to Potentially Dangerous Substances.....	Page 7
<u>Recommendation 4:</u> .....	Page 8
Incident Handling and Reporting Can Be Improved .....	Page 8
<u>Recommendations 5 and 6:</u> .....	Page 10
Appendix I – Detailed Objective, Scope, and Methodology.....	Page 12
Appendix II – Major Contributors to This Report .....	Page 14
Appendix III – Report Distribution List.....	Page 15
Appendix IV – Matrix of Findings by Location .....	Page 16
Appendix V – Management’s Response to the Draft Report.....	Page 17

## Physical Security Can Be Improved to Maximize Protection Against Unauthorized Access and Questionable Mail

### Background

Physical security has always been an important matter for the Internal Revenue Service (IRS), whether it is safeguarding taxpayer data or protecting its employees and facilities. While the terrorist attacks of September 11, 2001, have increased security awareness and put the entire nation on alert, they have also brought a dramatic shift in assessing risk vulnerabilities, in that what was once considered unthinkable is now very real and likely to occur. In addition, the subsequent anthrax mailings and mail bomb incidents have increased the risks associated with processing mail.

The IRS has always been in the position of balancing the needs of the taxpaying public and its responsibility to protect its employees and assets. Being more accessible to the public means being more vulnerable to attack. The IRS is widely dispersed with over 750 facilities throughout the nation. These facilities can range from one-person offices to large tax return processing campuses with thousands of employees. There are also different tenant sharing arrangements at these facilities, from being housed as an IRS-only office to sharing building space with other Federal agencies and other private companies.

Of particular difficulty are those buildings with joint occupancy of others. There are certain security measures over which the IRS has little or no control. For example, guard service at buildings with multiple Federal agencies is provided by the General Services Administration's (GSA) Federal Protective Service (FPS). Also, buildings where the IRS is not the lead agency or tenant (i.e., the largest organization in the building) means that the IRS must propose changes to the building security committee, who approves or disapproves security requests.

We conducted this audit to address Congressional concerns over security in the IRS in the wake of the terrorist attacks of September 11, 2001. We performed this audit from March to June 2002 at the National Headquarters office of the Agency-Wide Shared Services (AWSS) and the IRS offices at the following eight locations: (b)(7)(F)

Physical Security Can Be Improved to Maximize Protection  
Against Unauthorized Access and Questionable Mail

---

(b)(7)(F)

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

---

**The Internal Revenue Service  
Has Taken Steps to Reduce the  
Risk of Security Threats**

---

The IRS has adequate physical security policies and procedures for the level of security required at each facility and has taken an active role in strengthening security measures. The following are examples of improvements and security assessments that have been made at campuses and field offices.

- Preliminary assessment surveys, compliance reviews, or vulnerability assessments were completed at IRS facilities.
- Canine units were provided to each campus for explosive detection and intruder deterrence purposes.
- Redesigned workspace was completed to isolate the heating and air conditioning ventilation of the mail receipt area from the rest of the campus.
- Gloves and masks were made available to all employees who process mail.
- Motorized vehicle entrance was controlled by an enclosed guardhouse, and a lift and motorized gate leading to parking areas on a campus.
- Plans were proposed to remove garbage receptacles around a building.
- Cement barriers, security bollards, and planters were placed around a building to guard against explosive attack.
- Public building and street parking were eliminated around a building, and loading dock access was restricted.

## Physical Security Can Be Improved to Maximize Protection Against Unauthorized Access and Questionable Mail

---

- Increased building security guard staff was provided for more deterrence and detection abilities.
- Armed guards were placed in customer service walk-in offices to deter and quickly respond to potential threats.

However, security measures have not been consistently applied and IRS facilities remain vulnerable to intruders and explosive attacks. We identified several security weaknesses at the offices we visited that could allow an intruder access to IRS facilities. Our results indicate that the heightened security awareness that occurred after September 11<sup>th</sup> may be waning. The following findings present these weaknesses and specific examples of these conditions by site are presented in Appendix IV.

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

### **Building perimeters were not adequately secured**

The Department of the Treasury and IRS security standards require that all perimeter doors be locked and alarmed when not guarded. Management must conduct regular reviews of these controls to ensure they are functioning properly and must also train employees to be alert to security vulnerabilities. Weaknesses could allow intruders, visitors, or employees to surreptitiously enter the buildings and threaten the safety of employees and do harm to the building. We identified the following instances.

- In two sites, exterior surroundings such as trees and a removable coil covering a gap in a fence could easily provide an intruder access to IRS grounds and the building. In the case of the trees, the IRS does not have jurisdiction and could have difficulty in removing them because the trees are planted on local city or private property.

---

### **Physical Measures Can Be Improved to Minimize Unauthorized Access to Internal Revenue Service Offices and External Attacks to Its Buildings**

---

## Physical Security Can Be Improved to Maximize Protection Against Unauthorized Access and Questionable Mail

---

- In one site, non-IRS personnel were allowed access to IRS grounds and space for the purpose of visiting a credit union and a childcare facility. The IRS has had similar arrangements in other IRS offices, but has managed to maintain perimeter separation between IRS space and non-IRS space. Local management was unwilling to make any changes because they have had these arrangements with the credit union for a long time and state legislation mandated the availability of the childcare facility. There are IRS entrances from each of these facilities that are controlled by proxy cards. However, tellers at the credit union can allow individuals through that entrance by electronically unlocking the entrance doors (i.e., “buzzing in”) without the need of a proxy card, thus by-passing this control.
- In three sites, delivery trucks were not monitored or inspected. IRS policy requires that all delivery trucks be screened prior to entry into IRS property.
- In three sites, perimeter doors were unlocked, not properly closed, or left unattended for extended periods.
- In one site, the IRS did not have blast resistant film on ground-level windows.
- In five sites, the IRS had alarms that were not installed, operational, or working as intended.
- In five sites, the IRS had cameras that were either not installed, not working as intended, or slated for removal due to mechanical problems, placement, or lighting. In addition, exterior cameras at 2 sites were not monitored 24 hours a day, 7 days a week. The IRS did not have jurisdiction over the monitoring of the cameras.
- In three sites, the IRS did not have x-ray machines or metal detectors in the lobby. At one site, FPS employees did not properly identify the object that set off an alarm. These security measures were



## Physical Security Can Be Improved to Maximize Protection Against Unauthorized Access and Questionable Mail

---

generally out of the control of the IRS. If properly used and uniformly applied, this equipment could be an excellent deterrence and detection device.

- In one site, the Director's staff was allowed to clear themselves if badges or proxy cards were forgotten.
- In two sites, interior doors were either left unlocked, did not properly close, or left wide open. Both sites were either Federal buildings or commercial buildings. Non-employees who had access to the building could enter IRS space with relative ease.

These conditions occurred because employees and FPS were not alert to security vulnerabilities and the AWSS staff did not adequately review and test security controls to ensure that locks, alarms, and cameras were functioning properly. In some instances, State regulations and property jurisdiction superseded security concerns. Management also cited a lack of funding as a cause of cameras not functioning and the absences of metal detectors and x-ray machines placed in the lobby of the building.

### **Buildings were vulnerable to explosive attacks**

The Consolidated Physical Security Standards for IRS Facilities (CPSS) provides a set of minimum physical security standards. The CPSS states that receptacles that could conceal explosives should be kept away from buildings. Passive vehicle barriers, such as security bollards, should be provided at all IRS facilities.

Four sites we visited had ill-placed trash receptacles and/or newspaper stands located close or next to the building. Both could be used to conceal explosive devices. Also, buildings at two sites were not separated from parking spaces by security bollards.

Management was aware of many of these conditions but had not taken action either because of cost considerations, lack of awareness of the potential security risks, or lack of jurisdiction.

## Physical Security Can Be Improved to Maximize Protection Against Unauthorized Access and Questionable Mail

---

### Recommendations

We recommend that the Chief, AWSS:

1. Issue an all employee memorandum to reinforce security policies and procedures over building perimeter and interior security, and disallow the practice of electronically overriding proxy card entrances. Employees who do not have proxy cards should be subject to visitor entrance security procedures.

Management's Response: AWSS management will issue a memorandum instructing Facilities Management Officers (FMO) to emphasize the issue of perimeter and interior access control in their local security awareness briefings of all employees. The FMOs will also direct that all employees use their proxy cards every time they enter doors equipped with card readers and require employees without an authorized proxy card to follow the entry procedures for visitors.

2. Consider installing or repairing alarms, cameras, x-ray machines, metal detectors, and blast resistant film on ground-level windows when allocating new funds.

Management's Response: AWSS management will continue to use the risk assessment process to determine the appropriate use and placement of security devices, which will include considerations for all recommended items in this report. In addition, the Real Estate and Facilities Management (REFM) Division has scheduled a November 2002 meeting with the Chief, Field Operations, to develop an implementation strategy to acquire maintenance contracts for security equipment and systems.

3. Issue guidance requiring all individuals (visitors and employees without identification and proxy card access) entering IRS grounds or space to be subject to metal detectors, and their personal items subject to x-ray machines.

Management's Response: The IRS has delegated authority for physical security in only 14 of the approximately 785 facilities. In these 14 facilities, the IRS screens all visitors.

## Physical Security Can Be Improved to Maximize Protection Against Unauthorized Access and Questionable Mail

---

Also, the IRS either screens employees without identification or requires a manager to verify that the individual is still an IRS employee. In all other multi-tenant federal and commercial locations, a Building Security Committee (BSC) established by GSA determines the required level of screening. When the IRS assesses security needs for IRS space in these locations, the upgrades recommended take into consideration the level of security provided, through the BSC, for the entire facility.

Office of Audit Comment: We encourage re-emphasis of this issue as part of the Campus Readiness process for the upcoming filing season.

---

### **Mail Handling Can Be Improved to Reduce the Risk of Employee Exposure to Potentially Dangerous Substances**

---

The IRS Deputy Commissioner issued memoranda requiring all mail and packages received in each field office to be extracted only in a central mailroom or mail-sorting area, wherever possible. Large packages received from unknown sources must be x-rayed or subject to other appropriate screening. The only exception to this requirement is mail or packages that were never outside IRS control or from known vendors or contractors. Following these procedures will restrict the impact of any potential biological incident to areas where special precautions have been taken to minimize risk to employees. We identified the following instances.

- In five sites, employees voluntarily opened mail at their desks or cubicles and not in the central mailroom. Managers did not ensure that employees complied with existing procedures.
- In three sites, employees opened taxpayer correspondence in the walk-in area. Opening mail in a public area could increase the exposure to tainted letters by employees and taxpayers. National guidelines did not specifically include non-mail correspondences, such as hand delivered taxpayer letters and Collection sealed bids, under its mail handling and opening procedures.
- In three sites, mail handlers did not x-ray all incoming mail from other IRS offices, post office

## Physical Security Can Be Improved to Maximize Protection Against Unauthorized Access and Questionable Mail

---

boxes, and third party delivered mail (e.g., Federal Express, United Parcel Service), all of which should have been x-rayed. Again, managers did not ensure employees complied with existing procedures.

- In three sites, x-ray machines did not receive regular maintenance or calibration. Mail handlers only requested service for the x-ray machines if a problem was noted. National guidance did not address this issue.

### Recommendation

We recommend that the Chief, AWSS:

4. Issue an all employee memorandum to clarify mail handling procedures to include taxpayer correspondence from the walk-in area, Collection sealed bids, and letters or packages received that were outside IRS control be x-rayed or subject to other appropriate screening and opened in a designated centralized mailroom. This memorandum can also include requirements to periodically perform maintenance and calibration on all x-ray machines.

Management's Response: Because the IRS Deputy Commissioner has already issued memoranda for both campuses and field locations that provide specific mail-handling guidance, AWSS management will not issue any more memoranda on the subject. They will emphasize mail-handling procedures as part of the Campus Readiness process for the upcoming filing season. The maintenance and calibration of x-ray machines and security equipment was addressed in the corrective actions for recommendation 2.

The IRS Deputy Commissioner issued a memorandum, dated November 2, 2001, requiring facilities management officers to update the Occupant Emergency Plan (OEP) for each location no later than November 6, 2001. The FPS is responsible for conducting annual reviews to ensure the OEPs are current and adequate. In subsequent memoranda, the Deputy Commissioner required all employees who

---

### Incident Handling and Reporting Can Be Improved

---

## Physical Security Can Be Improved to Maximize Protection Against Unauthorized Access and Questionable Mail

---

extract mail to receive hazardous material awareness information and training. Also, the IRS requires all potential and significant incidents, and unusual situations that may affect the operations of the IRS, to be reported as quickly as possible. We identified the following instances.

- In six sites, the OEPs were not updated and/or did not have current contact points and telephone numbers. IRS procedures require that OEP contact points be updated at least once a year, or when personnel changes, or a significant change in tenant occupancy occurs. Managers were not aware of, or did not comply with, the requirements for updating the OEP.
- In one site, incident reporting points of contact and numbers were posted in the mailroom, but there was no telephone in the mailroom to make a call if an incident should occur. In another site, emergency contacts were not posted in the mailroom.
- In three sites, employees did not always have immediate access to the ventilation system cut-off switch, high quality filters were not always installed in the vacuum system to better capture potentially dangerous powdery substances, and alternate managers were not listed to contact in case of an emergency. These weaknesses existed because management did not account for all reasonable scenarios and procedures.
- In four sites, employees and/or managers were not aware of the escalation procedures. For example, an employee identified and marked a letter as suspicious, but the letter was left in the mailroom and no action was taken until several days later. In another site, an employee identified suspicious letters on 2 continuous days that had similar characteristics. On the second day, a manager decided the letter did not pose any threat because the letter received the prior day was found to be okay. The manager instructed an employee to hand-carry the opened letter in a sealed plastic bag through IRS

## Physical Security Can Be Improved to Maximize Protection Against Unauthorized Access and Questionable Mail

---

space to the Treasury Inspector General for Tax Administration, Office of Investigations, instead of calling local hazard material authorities, as required by procedures.

- In three sites, incidents were not reported on the Situation Awareness Management Center report, which should contain details on all IRS incidents. Incidents not reported include anthrax scares in the designated mailroom and walk-in area. Management was either not aware of the reporting requirements or believed the incidents were not significant enough to report.

In the event of an emergency, properly developed and current OEPs can reduce the threat to personnel, property, and other assets, while minimizing work disruption. Prompt reporting of incidents is essential to advise all levels of management of conditions that affect the operations of the IRS, as well as allow analysis of the information for trends.

### Recommendations

We recommend that the Chief, AWSS:

5. Issue an all employee memorandum to re-emphasize that OEPs should be updated at least once a year, or when personnel changes, or a significant change in tenant occupancy occurs, and to clarify and reinforce escalation procedures.

Management's Response: AWSS management agreed that they must re-emphasize annually the need to update OEPs. However, an all-employee memorandum is not the appropriate vehicle in this situation since the IRS only controls the OEPs for the 14 delegated sites. They will emphasize OEP review, including escalation procedures, as part of the annual Campus Readiness process at these delegated sites.

6. When allocating new funds, consider installing permanent telephones in all mailrooms to allow for the immediate reporting of incidents, ventilation cut-off

## Physical Security Can Be Improved to Maximize Protection Against Unauthorized Access and Questionable Mail

---

switches accessible to IRS employees, and high quality filters in the vacuum system to better capture potentially dangerous substances.

Management's Response: The REFM Division will contact the Digital Communications Office in the Modernization & Information Technology Services organization to pursue implementation of telephone service in all mailrooms. In addition, AWSS management has isolated the Receipt and Control ventilation systems for the 14 delegated sites, and has ordered high quality filters for the mail opening and sorting equipment used at the campuses and the IRS main headquarters building. These filters will be delivered in October 2002, and the manufacturer will do the initial installation and train IRS equipment operators on proper installation, removal, and disposal procedures.

## Physical Security Can Be Improved to Maximize Protection Against Unauthorized Access and Questionable Mail

### Appendix I

#### Detailed Objective, Scope, and Methodology

The overall objective of this review was to evaluate the effectiveness of physical security measures implemented at Internal Revenue Service (IRS) facilities. To accomplish our objective, we conducted the following audit steps at the Agency-Wide Shared Services Headquarter office, <sup>(b)(7)(F)</sup>

- I. Identified what the IRS had done in the area of physical security and employee safety as a result of September 11, 2001. Specifically, we reviewed prior physical security reviews and the statuses of their implementation, the Threat Assessments and Security Reviews required by the Deputy Commissioner for a judgmental sample of 48 of 752 sites (selected using interval sampling on sites sorted by square footage), physical security incident reports, the Consolidated Physical Security Standards for IRS facilities, physical security requirements and standards, and contacted the Treasury Inspector General for Tax Administration, Office of Investigations, to identify any potential threats and/or current investigations at sites selected for review.
- II. Determined how well IRS buildings are protected against unauthorized entry for the eight sites selected for our review. Specifically, we conducted after hours checks on the strength of security at the entry points and conducted a walk-through of the buildings, evaluated local procedures and security measures on permitting individuals into the buildings, and interviewed security guards to identify their roles, responsibilities, and enforcement capabilities.
- III. Determined how well the perimeters of IRS buildings are protected against explosive threats for the eight sites selected for our review. Specifically, we conducted after hours checks on security measures implemented around the building perimeter and a walk-through of the buildings, evaluated local procedures on protecting and monitoring the building perimeters, and interviewed security guards to identify the capabilities and limitations of the security cameras, and what security measures had been considered and taken to protect the buildings from car attacks.
- IV. Determined how well the IRS is protected against biological threats received via mail for the eight sites selected for our review. Specifically, we evaluated local procedures on mail handling to ensure all mail is subjected to the same requirements and opened in a designated area equipped with the necessary security precautions, and interviewed employees who handle mail to determine if they had received training and are aware of the procedures for processing mail.



**Physical Security Can Be Improved to Maximize Protection  
Against Unauthorized Access and Questionable Mail**

---

- V. Determined if the incident response handling procedures are adequate and effective at minimizing the risks of external threats, unauthorized access, and bio-chemical attacks for the eight sites selected for our review. Specifically, we reviewed the Occupant Emergency Plans to ensure information is current, and roles and responsibilities are clear and defined, interviewed employees and managers to verify everyone is aware of the procedures, and contacted the local fire departments to discuss concerns and/or issues they identified.

**Physical Security Can Be Improved to Maximize Protection  
Against Unauthorized Access and Questionable Mail**

---

**Appendix II**

**Major Contributors to This Report**

Scott E. Wilson, Assistant Inspector General for Audit (Information Systems Programs)  
Steve Mullins, Director  
Kent Sagara, Audit Manager  
Harry Dougherty, Senior Auditor  
Jody Kitazono, Senior Auditor  
Louis Lee, Senior Auditor  
Larry Reimer, Senior Auditor  
Dave Hodge, Auditor  
Joan Raniolo, Auditor  
William Simmons, Auditor

**Physical Security Can Be Improved to Maximize Protection  
Against Unauthorized Access and Questionable Mail**

---

Appendix III

**Report Distribution List**

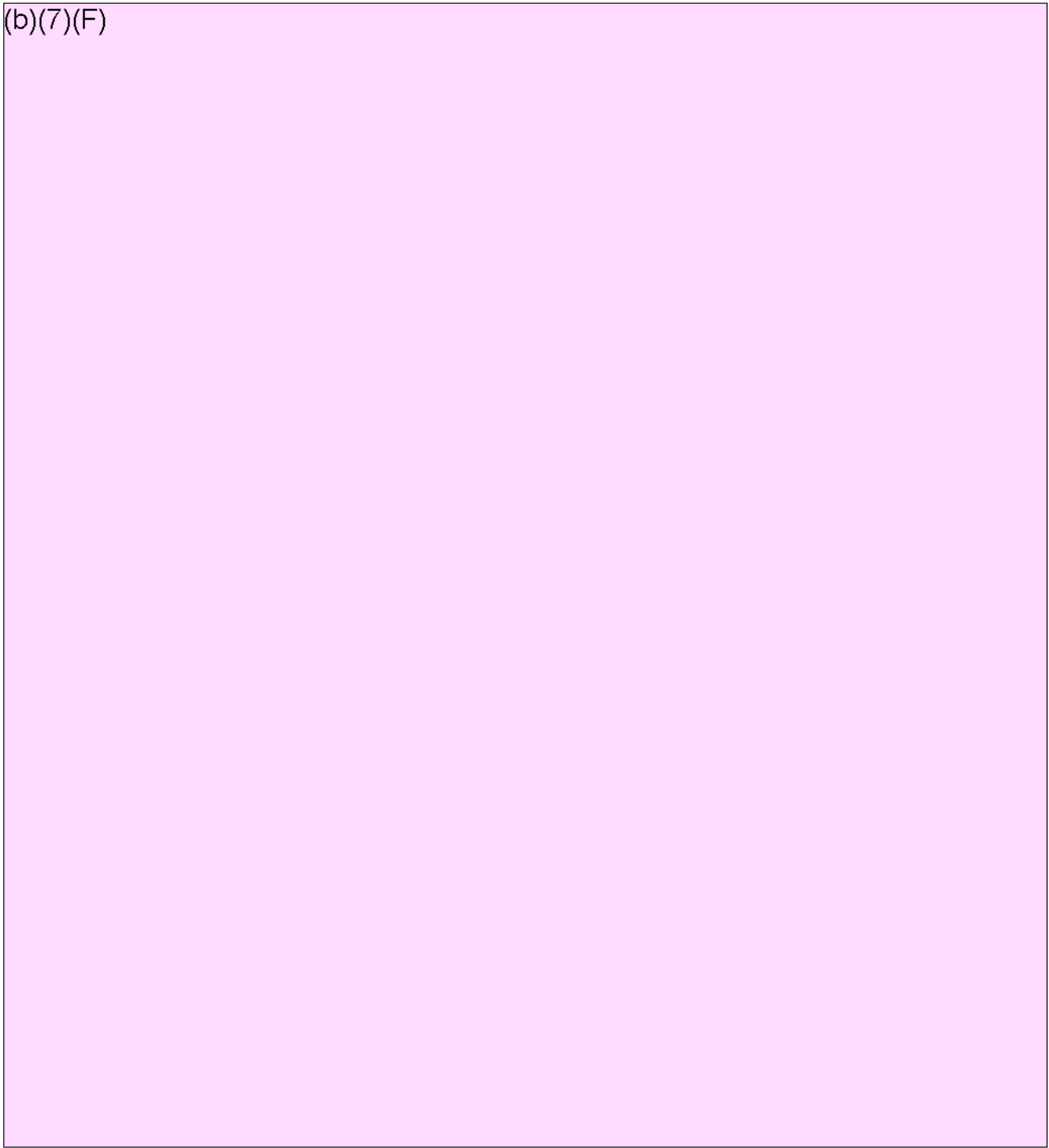
Commissioner N:C  
Deputy Commissioner N:DC  
Deputy Commissioner for Modernization & Chief Information Officer M  
Deputy Chief, Agency-Wide Shared Services A  
Chief, Security Services M:S  
Director, Real Estate and Facilities Management A:RE  
Director, Facilities Operations A:RE:O  
Director, Safety and Security A:RE:S  
Director, Mission Assurance M:S:A  
Director, Security Policy Support and Oversight M:S:S  
Management Control Coordinator A  
Deputy Chief Financial Officer, Department of the Treasury

**Physical Security Can Be Improved to Maximize Protection  
Against Unauthorized Access and Questionable Mail**

---

**Appendix IV**

(b)(7)(F)



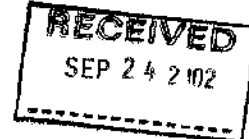
**Physical Security Can Be Improved to Maximize Protection  
Against Unauthorized Access and Questionable Mail**

Appendix V

**Management's Response to the Draft Report**



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



September 24, 2002

MEMORANDUM FOR PAMELA J. GARDINER  
DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: Gregory D. Rothwell *Gregory D. Rothwell*  
Deputy Chief, Agency-Wide Share Services

SUBJECT: Draft TIGTA Audit Report #200220042, Physical Security Can Be  
Improved to Maximize Protection Against Unauthorized Access  
and Questionable Mail, dated August 22, 2002

I have reviewed the above audit report and agree with your recommendations. Historically, providing a safe and secure workplace for our employees and taxpayers has been a primary concern of IRS. Following the events of September 11, we have focused on providing adequate protection for employees and assets. The IRS actually began to redefine and improve its physical security program after the attack on the Oklahoma City Federal Office Building in April 1995. We developed and implemented a risk assessment and facility enhancement program to identify threats, determine vulnerabilities, and recommend appropriate protective measures. We implemented the program on a priority basis, determined by the mission critical functions performed at a site. Therefore, our initial efforts addressed security needs at our campuses, computing centers, and large area (former district) offices.

Our building inventory includes approximately 785 locations. Of these, the GSA has delegated physical security authority to the IRS in 14 locations. These locations include the ten submission processing campuses, the two computing centers, the Main Headquarters Building, and the New Carrollton Federal Building. We have the responsibility for all aspects of security in these locations and, since 1996, have implemented upgrades totaling over \$30 million. Upgrades typical to all 14 sites include the constructing of fences with vehicular and pedestrian gates; segregating visitor parking; improving security lighting; using surveillance cameras; installing electronic entry control and intrusion detection systems; and enhancing the security console rooms to better monitor activities. In addition, We employ guards to control entrances, patrol the perimeter, and respond to incidents. This past February, we added canine explosive detecting teams to each campus to screen incoming vehicles and mail.

The remaining 771 IRS offices are located in commercial or federal facilities. In a few of these buildings the IRS is the sole occupant. The vast majority are multi-tenant facilities with a mix of federal and private occupants. In these facilities, we only control physical security in the space we occupy. We have no authority or control over perimeter

## Physical Security Can Be Improved to Maximize Protection Against Unauthorized Access and Questionable Mail

---

2

security or security in common or shared areas of the buildings. That authority and control resides in the Building Security Committees (BSC), established in all multi-tenant facilities housing federal employees following the Oklahoma City attack. The Federal Protective Service chairs the BSCs and operates on the principle of one agency, one vote. Recommendations approved by the BSCs determine the level of perimeter security and protection in lobby and other shared areas. When we assess security needs for IRS space in these offices, the upgrades recommended take into consideration the level of security provided, through the BSC, for the entire facility. We have implemented over \$25 million in upgrades in these facilities.

Typical improvements for the non-delegated sites include: electronic entry control and intrusion detection systems, duress alarms, and surveillance cameras. To date, we have completed risk assessments for 185 offices. The 185 offices represent only 24 percent of the total building inventory but account for 65 percent of the square footage occupied. We will complete risk assessments for the remaining sites are scheduled for completion by December 31, 2003.

As your report noted, we must ensure procedures for handling mail and Occupant Emergency Plans are current. Please see the attached responses for actions planned to address these issues.

If you have additional questions, please contact me at (202) 622-7500 or Ron Stephen, Director, Real Estate and Facilities Management at (202) 283-9400. For matters addressing audit follow-up and liaison, please contact Greg Rehak at (202) 622-3702

Attachment

## Physical Security Can Be Improved to Maximize Protection Against Unauthorized Access and Questionable Mail

---

3

### Attachment

**RECOMMENDATION 1:** Issue an all employee memorandum to reinforce security policies and procedures over building perimeter and interior security, and disallow the practice of electronically overriding proxy cards. Employees who do not have proxy cards should be subject to visitor entrance security procedures.

**CORRECTIVE ACTION 1:** AWSS will issue a memorandum instructing Facilities Management Officers (FMO) to emphasize the issue of perimeter and interior access control in their local security awareness briefings for all employees. Security awareness briefings have proven to be an effective means of communicating and emphasizing the important role employees have in security. Before the filing season, FMOs will conduct briefings in all buildings where the IRS has employees.

**PROPOSED COMPLETION DATE:** December 31, 2002

**CORRECTIVE ACTION 2:** AWSS will issue a memorandum to the FMOs directing that all employees use their card keys every time they enter doors equipped with readers. We will require employees without an authorized card key to follow the entry procedures for visitors.

**PROPOSED COMPLETION DATE:** December 31, 2002

**RESPONSIBLE OFFICIAL:** Director, Real Estate and Facilities Management, AWSS

**Physical Security Can Be Improved to Maximize Protection  
Against Unauthorized Access and Questionable Mail**

---

4

**RECOMMENDATION 2:** Consider installing or repairing alarms, cameras, x-ray machines, metal detectors, and blast resistant film on ground-level windows when allocating new funds.

**CORRECTIVE ACTION 1:** AWSS uses the risk assessment process to determine the appropriate use and placement of security devices. This risk assessment process includes consideration of all recommended items. We will continue to use the risk assessment process to determine the appropriate level of security for all facilities and to develop budget requirements for upgrade projects.

**COMPLETION DATE:** September 3, 2002

**CORRECTIVE ACTION 2:** The Real Estate and Facilities Management (REFM) Division held preliminary discussions with the Chief, Field Operations, Procurement Division on the issue of maintenance contracts. REFM has scheduled a follow-on meeting for November 13, 2002, with the Chief, Field Operations to develop an implementation strategy to acquire maintenance contracts for security equipment and systems.

**PROPOSED COMPLETION DATE:** March 31, 2003

**RESPONSIBLE OFFICIAL:** Director, Real Estate and Facilities Management, AWSS



**Physical Security Can Be Improved to Maximize Protection  
Against Unauthorized Access and Questionable Mail**

---

5

**RECOMMENDATION 3:** Issue guidance requiring all individuals (visitors and employees without identification and proxy card access) entering IRS grounds or space to be subject to metal detectors, and their personal items subject to x-ray machines.

**CORRECTIVE ACTION:** The IRS has delegated authority for physical security in only 14 of the approximate 785 facilities in our building inventory. In these 14 facilities, we screen all visitors. Also, we either screen employees without identification or require a manager to verify that the individual is still an IRS employee. In all other multi-tenant federal and commercial office locations, a Building Security Committee (BSC) established by GSA, determines the required level of screening.

**COMPLETION DATE:** September 3, 2002

**RESPONSIBLE OFFICIAL:** Director, Real Estate and Facilities Management, AWSS

## Physical Security Can Be Improved to Maximize Protection Against Unauthorized Access and Questionable Mail

---

6

**RECOMMENDATION 4:** Issue an all employee memorandum to clarify mail handling procedures to include taxpayer correspondence from the walk-in area, collection sealed bids, and letters or packages received that were outside IRS control be x-rayed or subject to other appropriate screening and opened in a designated centralized mailroom. This memorandum can also include requirements to periodically perform maintenance and calibration on all x-ray machines.

**CORRECTIVE ACTION:** The Deputy Commissioner issued memorandums, dated December 20, 2001, for campuses and January 23, 2002, for field locations, that provide specific mail-handling guidance. These memorandums are available on our web site at <http://communications.no.irs.gov/CommPlan/campussecurity.htm>. We will emphasize mail-handling procedures as part of the Campus Readiness process for the upcoming filing season. As stated under Recommendation 2, AWSS plans to address maintenance and calibration of x-ray machines and related security equipment.

**PROPOSED COMPLETION DATE:** December 31, 2002

**RESPONSIBLE OFFICIAL:** Director, Real Estate and Facilities Management, AWSS

## Physical Security Can Be Improved to Maximize Protection Against Unauthorized Access and Questionable Mail

---

7

**RECOMMENDATION 5:** Issue an all employee memorandum to re-emphasize that Occupant Emergency Plans (OEPs) should be updated at least once a year, or when personnel changes, or significant change in tenant occupancy occurs, and to clarify and reinforce escalation procedures.

**CORRECTIVE ACTION:** We agree we must re-emphasize annually the need to update OEPs, however, an all employee memorandum is not the appropriate vehicle in this situation. We only control OEPs for the 14-delegated sites. We will emphasize OEP review including escalation procedures as part of the annual Campus Readiness process at these delegated sites.

**COMPLETION DATE:** December 31, 2002

**RESPONSIBLE OFFICIAL:** Director, Real Estate and Facilities Management, AWSS

## Physical Security Can Be Improved to Maximize Protection Against Unauthorized Access and Questionable Mail

---

8

**RECOMMENDATION 6:** When allocating new funds, consider installing permanent telephones in all mailrooms to allow for the immediate reporting of incidents, ventilation cut-off switches accessible to IRS employees, and high quality filters in the vacuum system to better capture potentially dangerous substances.

**CORRECTIVE ACTION 1:** The Digital Communications Office in the MITS organization has primary responsibility for installing and maintaining phone service. The REFM Division will contact this office to pursue implementation of this corrective action. As an alternative to installing permanent phones, REFM will examine the use of cell phones in mailroom operations as well.

**PROPOSED COMPLETION DATE:** December 31, 2002

**CORRECTIVE ACTION 2:** We have evaluated this recommendation and isolated the Receipt and Control HVAC systems in the 14-delegated sites. Most non-delegated sites do not have isolated mailroom HVAC systems. The ventilation systems impact multiple areas of the building, and the lessor or GSA controls them.

**COMPLETION DATE:** September 3, 2002

**CORRECTIVE ACTION 3:** We have ordered high efficiency particulate air (HEPA) filters for the mail opening and sorting equipment used at the campuses and the IRS Main Headquarters Building. The filters are scheduled for delivery in October 2002. The manufacturer will do the initial installation and train IRS equipment operators on proper installation, removal, and disposal procedures.

**PROPOSED COMPLETION DATE:** December 31, 2002

**RESPONSIBLE OFFICIAL:** Director, Real Estate and Facilities Management, AWSS