



*The Physical Security Risk Assessment  
Program Needs Improvement*

**September 16, 2013**

**Reference Number: 2013-10-101**

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

---

Phone Number | 202-622-6500

E-mail Address | [TIGTACommunications@tigta.treas.gov](mailto:TIGTACommunications@tigta.treas.gov)

Website | <http://www.treasury.gov/tigta>



## HIGHLIGHTS

### THE PHYSICAL SECURITY RISK ASSESSMENT PROGRAM NEEDS IMPROVEMENT

## Highlights

**Final Report issued on  
September 16, 2013**

Highlights of Reference Number: 2013-10-101 to the Internal Revenue Service Chief, Agency-Wide Shared Services.

### IMPACT ON TAXPAYERS

The IRS's Physical Security and Emergency Preparedness office is responsible for conducting risk assessments to ensure that IRS facilities are secure and employees and taxpayers are safe. TIGTA's review identified deficiencies in the Physical Security Risk Assessment Program and found that all facilities did not receive risk assessments as required. As a result, the IRS may have security vulnerabilities that are not identified and addressed in a timely manner, thereby placing IRS employees and taxpayers at risk.

### WHY TIGTA DID THE AUDIT

This audit was initiated because of the numerous threats made against IRS facilities and employees. To proactively mitigate these threats, the IRS is required to conduct comprehensive and timely risk assessments to identify and address vulnerabilities in physical security. The overall objective of this review was to determine whether physical security risk assessments were conducted as required at all IRS facilities.

### WHAT TIGTA FOUND

The IRS completed 630 risk assessments at IRS facilities and met its requirement to provide a report summarizing the findings to the IRS Commissioner in January 2011. However, the IRS did not complete risk assessments at 14 facilities. Additionally, the IRS could not provide evidence that risk assessments were performed for 49 facilities that are the responsibility of the Federal Protective Service.

These 49 facilities included childcare centers, parking lots and garages, and storage units that, although not occupied by IRS employees, are within or adjacent to facilities housing IRS employees.

Completed risk assessments prepared by the IRS identified numerous additional security countermeasure needs at IRS facilities. However, TIGTA found that some countermeasures were not acted upon. The IRS cited resource constraints as a reason that countermeasures were not implemented. For example, the IRS did not implement blast mitigation countermeasures at approximately 191 facilities and has not added additional guards or other countermeasures at certain Taxpayer Assistance Centers. During site visits to IRS facilities, TIGTA also found that risk assessments did not identify additional vulnerabilities. For example, a childcare center allows direct access to one IRS facility without the required screening. At another facility, a local IRS manager chose not to implement countermeasure improvements paid for and provided to the facility.

### WHAT TIGTA RECOMMENDED

TIGTA made seven recommendations to the Director, Physical Security and Emergency Preparedness, to address identified weaknesses. For example, TIGTA recommended that the IRS include the development of a process to ensure that inventory records contain all relevant information including the dates when risk assessments should be performed. TIGTA also recommended that the IRS implement appropriate security protocols at the facility with the childcare center to screen all visitors entering the grounds and the building according to requirements.

In their response, IRS management agreed with the recommendations and plans to implement corrective actions to address them. For example, the IRS plans to ensure that inventory records include all relevant information and develop a process to ensure that required countermeasures are in place and functioning at all Taxpayer Assistance Centers.



TREASURY INSPECTOR GENERAL  
FOR TAX ADMINISTRATION

DEPARTMENT OF THE TREASURY  
WASHINGTON, D.C. 20220

September 16, 2013

**MEMORANDUM FOR CHIEF, AGENCY-WIDE SHARED SERVICES**

**FROM:** Michael E. McKenney  
Acting Deputy Inspector General for Audit

**SUBJECT:** Final Audit Report – The Physical Security Risk Assessment Program  
Needs Improvement (Audit # 201210007)

This report presents the results of our review to determine whether physical security risk assessments were conducted as required at all Internal Revenue Service (IRS) facilities. Our review focused on the risk assessments conducted by the Physical Security and Emergency Preparedness office in Calendar Year 2010 to address the IRS Commissioner's requirement to conduct risk assessments at all IRS-occupied facilities to identify measures needed to improve employee safety. This review is included in our Fiscal Year 2013 Annual Audit Plan and addresses the major management challenge of Security for Taxpayer Data and Employees.

Management's complete response to the draft report is included as Appendix IX.

Copies of this report are also being sent to the IRS managers affected by the report recommendations. If you have any questions, please contact me or Gregory D. Kutz, Assistant Inspector General for Audit (Management Services and Exempt Organizations).



---

*The Physical Security Risk Assessment  
Program Needs Improvement*

---

*Table of Contents*

**Background** ..... Page 1

**Results of Review** ..... Page 4

    The Physical Security and Emergency Preparedness Office  
    Completed 630 Risk Assessments, but Did Not Perform Risk  
    Assessments on Additional Internal Revenue Service Facilities ..... Page 4

Recommendations 1 through 3: ..... Page 6

    Risk Assessment Findings Were Not Consistently Acted Upon, and  
    Additional Vulnerabilities Were Identified During Site Visits ..... Page 7

Recommendation 4: ..... Page 10

Recommendations 5 through 7: ..... Page 11

**Appendices**

    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 – Outcome Measure ..... Page 16

    Appendix V – Facility Security Level Determination Matrix ..... Page 17

    Appendix VI – Fourteen Internal Revenue Service Buildings That Did  
    Not Receive a Risk Assessment in Calendar Year 2010 ..... Page 18

    Appendix VII – Status of 14 Internal Revenue Service Buildings  
    That Did Not Receive Timely Risk Assessments ..... Page 19

    Appendix VIII – Fourteen Physical Security and Emergency  
    Preparedness Office Territories ..... Page 20

    Appendix IX – Management’s Response to the Draft Report ..... Page 22



*The Physical Security Risk Assessment  
Program Needs Improvement*

---

*Abbreviations*

CY	Calendar Year
FPS	Federal Protective Service
FSL	Facility Security Level
GDI	Graphic Database Interface
IRS	Internal Revenue Service
ISC	Interagency Security Committee
PSEP	Physical Security and Emergency Preparedness
TAC	Taxpayer Assistance Center



## *The Physical Security Risk Assessment Program Needs Improvement*

---

### *Background*

Due to the nature of the Internal Revenue Service's (IRS) mission, the organization remains a target for those who are angry at the tax system or the Government. Threats of violence directed at the IRS's 100,000 employees at more than 600 facilities throughout the country have increased during a time of continued financial hardship.<sup>1</sup> In the one-year period between October 2010 and September 2011, there were more than 1,400 reported threat incidents directed towards IRS employees and infrastructure.

In an effort to address the continued threat to IRS employees and facilities, in March 2010, the IRS Commissioner initiated a Security Readiness Project which established a task force with a mission to determine how to improve the IRS's security posture and assure employees that they are safe in the workplace. One important component of the project included conducting in-depth security reviews (risk assessments) of all IRS facilities by December 31, 2010.

The Agency-Wide Shared Services's Physical Security and Emergency Preparedness (PSEP) office is responsible for program management and operations support to ensure that all IRS physical security and emergency preparedness programs are operating in an integrated manner to protect IRS employees, facilities, critical business operations, and assets.

The PSEP office's primary responsibilities are to:

- Ensure the protection of employees, visitors, and property at IRS facilities.
- Ensure the security of IRS physical infrastructure and classified information.
- Ensure that readiness and preparedness activities enhance the IRS's ability to continue ongoing services to taxpayers.
- Coordinate and execute emergency preparedness and crisis response activities IRS-wide and in conjunction with other Federal, State, local, and relief agencies.
- Develop and maintain an effective working relationship with the Department of Homeland Security, the Department of Defense, and other Federal agencies involved in national security and emergency response issues.

To fulfill one of its primary responsibilities, the PSEP office has implemented a risk assessment program based on the Department of Homeland Security's Interagency

---

<sup>1</sup> The 600-plus facilities include IRS employee-occupied facilities and other non-IRS occupied facilities such as privately run childcare centers or credit unions sites, which typically house non-IRS personnel.



---

## *The Physical Security Risk Assessment Program Needs Improvement*

---

Security Committee (ISC) standards.<sup>2</sup> Risk assessments evaluate both internal and external security risks and are conducted on a pre-established schedule depending on the assigned Facility Security Level (FSL) of the facility.<sup>3</sup>

According to the guidance in the ISC standards, the first step in the risk assessment process entails determining the FSL of the facility. The PSEP office used the criteria in the ISC standards for establishing the FSL, which involves analyzing various factors that make the facility a target for adversarial acts as well as those that characterize the value or criticality of the facility. These factors are input into a matrix of criteria and given a point value, and the total point value determines the FSL of the facility.

The FSL of a facility ranges from one to five, with five being the highest level for security risk and one being the lowest level. For example, a facility designated as FSL V would require the most security. Some of the factors considered in determining the FSL assessment include the number of employees occupying the facility and the square footages. Other factors which could raise the FSL could include intangible items such as symbolic significance or historical importance of a facility.

As such, the PSEP office was tasked with identifying the total number of IRS-occupied buildings and conducting in-depth risk assessments at those facilities.<sup>4</sup> A prior Treasury Inspector General for Tax Administration review<sup>5</sup> evaluated the contract between the IRS and the contractor to ensure that the IRS received the deliverables from the contractor in accordance with the terms of the contract.<sup>6</sup> Based on the concerns raised during that review of the contract, we initiated this review to assess the adequacy of the physical security assessments conducted at IRS facilities.

For this review, we judgmentally<sup>7</sup> selected for review 10 IRS facilities from the 630 risk assessments conducted by the PSEP office. Our review included facilities with FSL II through FSL V levels and represented four of the 14 PSEP office Territories nationwide.<sup>8</sup> Our analysis included site visitations to interview PSEP office staff (including the security specialist and the respective Territory manager) and walkthroughs of each of the 10 facilities. The physical observations during the walkthroughs and interviews with on-site PSEP office staff to discuss the

---

<sup>2</sup> The ISC established standards for security in and protection of Federal facilities. The ISC issued interim standards, *Physical Security Criteria for Federal Facilities – An Interagency Security Committee Standard* (April 12, 2010), that established a baseline set of physical security measures to be applied to all Federal facilities based on their designated Facility Security Level.

<sup>3</sup> See Appendix V for the FSL Determination Matrix used by the PSEP office.

<sup>4</sup> PSEP office management determined they would perform risk assessments only at IRS facilities with employees. The PSEP office excluded some facilities such as parking lots, storage facilities, childcare centers, and credit unions.

<sup>5</sup> Treasury Inspector General for Tax Administration, Ref. No. 2012-10-075, *An Independent Risk Assessment of Facility Physical Security Was Not Performed in Compliance With Contract Requirements* (Jul. 2012).

<sup>6</sup> Physical Security Emergency Preparedness Risk Assessment contract (TIRNO-10-C-00041).

<sup>7</sup> A judgmental sample is a nonstatistical sample, the results of which cannot be used to project to the population.

<sup>8</sup> See Appendix VIII for a list of the 14 PSEP office Territories.



*The Physical Security Risk Assessment  
Program Needs Improvement*

---

risk assessments they conducted in Calendar Year (CY)<sup>9</sup> 2010 provided us with a better understanding of the risk assessment process and helped to determine the status of the CY 2010 findings and recommendations. Our physical observations were not intended to replicate risk assessments performed during CY 2010.

This review was performed at the IRS National Headquarters in the Agency-Wide Shared Services function in Washington, D.C., during the period June 2012 through July 2013. Site visits were also made to two offices in Denver, Colorado; one office in Golden, Colorado; three offices in Atlanta, Georgia; two offices in Memphis, Tennessee; one office in Falls Church, Virginia; and the IRS National Headquarters in Washington, D.C. We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective. Detailed information on our audit objective, scope, and methodology is presented in Appendix I. Major contributors to the report are listed in Appendix II.

---

<sup>9</sup> The 12-consecutive-month period ending on December 31.





---

*The Physical Security Risk Assessment  
Program Needs Improvement*

---

*Results of Review*

***The Physical Security and Emergency Preparedness Office  
Completed 630 Risk Assessments, but Did Not Perform Risk  
Assessments on Additional Internal Revenue Service Facilities***

By December 31, 2010, the PSEP office completed 630 risk assessments and met its requirement to provide a report summarizing the findings to the IRS Commissioner in January 2011. Although our review did not evaluate the accuracy or completeness of all 630 risk assessments, we did find that the PSEP office completed all 630 risk assessments in the necessary six-month period. However, risk assessments were not completed at 14 facilities occupied by IRS employees in CY 2010.<sup>10</sup> In addition, the PSEP office did not complete risk assessments at 49 other facilities that were not specifically occupied by IRS employees but were located in or adjacent to the facilities.

***Risk assessments were not performed at 14 facilities during CY 2010***

The PSEP office did not conduct risk assessments on 14 facilities occupied by IRS employees. While PSEP office management did not explain why risk assessments were not performed at the 14 facilities we identified, the PSEP office's method of tracking its inventory of facilities may have contributed to the omission. The PSEP office compiles its inventory list by maintaining an Excel spreadsheet based on real estate data contained in the IRS's Graphic Database Interface (GDI).<sup>11</sup> Because the Excel spreadsheet is a standalone document and not linked to the GDI, any changes in a facility's status must be noted by the PSEP office employee and transferred to the spreadsheet manually. Therefore, if the PSEP office employee does not reconcile the changes between the GDI and the Excel spreadsheet, there may be errors and omissions in the inventory list maintained by the PSEP office.

After we informed it of the omission, the PSEP office performed risk assessments on five of the 14 facilities that did not receive a risk assessment in CY 2010. Two of these five facilities were designated as FSL IV, and the remaining three facilities were designated as FSL II. For the

---

<sup>10</sup> See Appendix VI for a list of the 14 facilities, which consisted of four buildings associated with one campus and 10 IRS office buildings. A campus is the data processing arm of the IRS. The campuses process paper and electronic submissions, correct errors, and forward data to the Computing Centers for analysis and posting to taxpayer accounts. Of these 14 facilities, nine have closed and five remain open. See Appendix VII for more information.

<sup>11</sup> The GDI is an automatic system that tracks the IRS real property portfolio including buildings, space, and services. The GDI report is provided to the PSEP office by the Real Estate Facility Management group. PSEP office management used the June 6, 2010, GDI report to estimate the number of buildings in inventory.



---

## *The Physical Security Risk Assessment Program Needs Improvement*

---

remaining nine facilities, PSEP office management stated that although these facilities were open during CY 2010 and should have had risk assessments performed, they are now closed.<sup>12</sup>

Maintaining an accurate inventory of IRS-occupied facilities is imperative for the PSEP office to accomplish its mission. If risk assessments are not done timely or if facilities are missed, security vulnerabilities may not get addressed and IRS employees and Government assets could be subject to increased risk.<sup>13</sup> Approximately 4,408 IRS employees were located at the 14 facilities we identified.<sup>14</sup>

### **Risk assessments were not performed at 49 facilities, including credit unions, childcare centers, storage facilities, and parking lots**

In addition to the 14 facilities previously discussed, we identified 49 facilities that did not receive a risk assessment in CY 2010. These 49 facilities, which included childcare centers, parking lots and garages, storage units, and a credit union, are not specifically occupied by IRS employees. These facilities are used by IRS employees and are typically located either within or next to facilities housing IRS employees. PSEP office management stated that the 49 facilities were excluded because the Federal Protective Service (FPS)<sup>15</sup> is responsible for the security at these facilities. However, the PSEP office did not provide evidence that the 49 facilities received a risk assessment from either the IRS or the FPS.

The PSEP office's Internal Revenue Manual<sup>16</sup> does not address which types of facilities should receive a risk assessment. However, during our audit, PSEP office management issued a Standard Operating Procedure dated August 7, 2012, which provides general information about the types of facilities the PSEP office should review. The document states, "risk assessments are performed at all IRS facilities, occupied by Federal employees and contractors and Day Care centers." Although the PSEP office recently issued procedures, there is limited information about which types of facilities require a PSEP risk assessment. For example, we received conflicting information about childcare centers and storage facilities during interviews with PSEP office management. One PSEP manager stated that if a childcare center is located in a single-tenant building, the IRS (the PSEP office) would perform the risk assessment; however, if the childcare center is located in a multitenant building, the FPS would perform the risk assessment. In another instance, a Territory manager stated that the PSEP office would perform a risk assessment on an unoccupied storage facility if it contained grand jury records.

---

<sup>12</sup> See Appendix VII for more information.

<sup>13</sup> The ISC requires that buildings designated as FSLs III, IV, and V be evaluated on a three-year cycle, and buildings designated as FSLs I and II be completed every five years. The FSL is developed based upon mission criticality, symbolism, population, facility size, and threat to tenant agencies.

<sup>14</sup> See Appendices VI and VII for more information about these facilities.

<sup>15</sup> The FPS is an organization within the Department of Homeland Security.

<sup>16</sup> IRM 10.2.11 (Sep. 28, 2009).



---

## *The Physical Security Risk Assessment Program Needs Improvement*

---

PSEP office management stated that they do not have a documented policy or agreement with the FPS regarding the risk assessment process. They also indicated that the FPS has responsibility for the 49 facilities because they are leased by the General Services Administration. However, PSEP office management also advised us that the General Services Administration leases all IRS buildings because the IRS owns none of its facilities. PSEP office management stated they have an excellent relationship with the FPS, but communications between the two organizations is a challenge.

PSEP office management could not confirm whether the FPS conducted risk assessments at the 49 facilities we identified. As a result, the safety of IRS employees and facilities could be affected because many of these 49 facilities are located adjacent to or in close proximity to IRS facilities. In addition, the Standard Operating Procedure does not provide a clear explanation of the types of facilities that require a risk assessment, so there is a risk that some facilities may be omitted from future risk assessments.

### ***Recommendations***

The Director, PSEP, should:

**Recommendation 1:** Develop a process to ensure that inventory records include all relevant information, such as the date facilities are open and closed as well as the dates risk assessments should be performed.

**Management's Response:** The IRS agreed with this recommendation. The Director, PSEP, Agency-Wide Shared Services, implemented a process to ensure that PSEP inventory records include all relevant information, such as the date facilities are opened and closed as well as the dates risk assessments should be performed. The PSEP staff uses monthly reports from the GDI Building Directory and the Joint Information Management Site Consolidated Report to maintain an accurate building inventory and to calculate the due dates for risk assessments.

**Recommendation 2:** Work with the FPS to ensure that the IRS receives copies of FPS risk assessments performed at IRS facilities and a schedule of when the FPS plans to perform future risk assessments of IRS facilities.

**Management's Response:** The IRS agreed with this recommendation. The Director, PSEP, will request from the FPS National Director, copies of all FPS risk assessments of space in IRS inventory and a schedule of when the FPS plans to perform future risk assessments.

**Recommendation 3:** Update the policies for the risk assessment program to distinguish which facilities, such as childcare centers, parking lots, and storage facilities, require an FPS risk assessment and which ones, such as IRS employee-occupied facilities, require a PSEP office risk assessment.



---

*The Physical Security Risk Assessment  
Program Needs Improvement*

---

**Management's Response:** The IRS agreed with this recommendation. The Director, PSEP, will update Physical Security Internal Revenue Manual 10.2.11, *Basic Security Concepts*, and Standard Operating Procedures 021 (a), *Risk Assessments*, to distinguish which risk assessments are the responsibility of the FPS and which risk assessments are the responsibility of the PSEP office.

***Risk Assessment Findings Were Not Consistently Acted Upon, and Additional Vulnerabilities Were Identified During Site Visits***

The risk assessment project completed in CY 2010 included numerous findings related to additional security countermeasures needed at IRS facilities. However, some findings were not acted upon. Specifically, we found that the process to implement the security countermeasures did not consistently follow the established prioritization schedule, and some countermeasures were not implemented, which the IRS attributed in part to resource constraints. In addition, during our site visits, we identified security weaknesses that were not addressed through the risk assessment process and that records on prior risk assessments were not always retained.

**The PSEP office did not consistently follow up on risk assessment findings**

Although PSEP office management developed a prioritization schedule to roll out the security countermeasures, we found they sometimes implemented lower priority countermeasures before other higher priority actions. The prioritization schedule was intended to phase in the large volume of countermeasures based on criticality, over a period of time, as funding became available. PSEP office management made a decision to address "low-hanging fruit" if a lower priority countermeasure, such as posting signs advising of video surveillance, was low cost and could be easily implemented. However, by diverting attention from higher priority countermeasures to lower, less critical countermeasures, critical vulnerabilities may not have been addressed timely.

We also found that PSEP office management made a decision to not implement blast mitigation at approximately 191 facilities that were identified through the CY 2010 risk assessment project. Blast mitigation countermeasures generally refer to specially designed window systems to mitigate the hazards from glass and flying debris. These countermeasures vary by the FSL of a facility, but are required by ISC standards for FSL II through V facilities. PSEP office management explained that the costs associated with updating numerous IRS facilities with needed blast mitigation measures were prohibitive and impractical; management had decided to accept the risk of not implementing this countermeasure. However, we believe blast mitigation should have been considered on a case-by-case basis because some IRS facilities may be more vulnerable than others. For example, a single-story building where parking is allowed adjacent to the building could be at greater risk than an IRS space that is located on a higher floor of a building and further removed from parked vehicles.



---

## *The Physical Security Risk Assessment Program Needs Improvement*

---

Finally, as of May 2013, some Taxpayer Assistance Centers (TAC)<sup>17</sup> still lacked additional guards and other countermeasures, although these vulnerabilities were identified in the CY 2010 risk assessments. On November 8, 2010, PSEP office management reported that a decision was made to maintain a permanent guard presence at all TACs as a result of the risk assessment project and, according to PSEP records, each TAC has at least one guard present at each location.<sup>18</sup> However, risk assessments performed at TACs across the country identified that some TACs need additional guard presence and other countermeasures such as x-ray machines to comply with the ISC standards. During our audit, we found that at least four TACs do not currently have the additional guard or x-ray machine recommended by the risk assessments. PSEP office management stated that this information is not tracked on a national level and thus could not provide information on how many TACs nationally have increased vulnerability because additional guards and other countermeasures are not in place.

The ISC standards require that certain facilities maintain a guard presence and that the risk assessment determines the need for security guard presence. Despite the apparent critical nature of this countermeasure, PSEP office management categorized guard deployment as the lowest priority level for implementation. PSEP office management also stated that they were unable to place additional guards at all of the offices that need them because of budget constraints.

Because IRS employees at the TACs are engaged in face-to-face contact with taxpayers daily, there is an ongoing risk that they may come into contact with individuals who pose a physical threat to them or the facility. Having all the required countermeasures at these offices is critical to ensuring the safety of IRS employees and members of the public who visit IRS offices.

### **Site visits identified additional unaddressed security vulnerabilities**

During our site visits to 10 IRS facilities, we identified security vulnerabilities at two locations that PSEP office management was unaware of until the audit team brought it to their attention. At one location, the CY 2010 risk assessment did not disclose a security vulnerability related to a childcare center located within an IRS facility. At another location, local management did not implement the security countermeasures recommended by the PSEP office.

---

<sup>17</sup> A TAC is an IRS office with employees who answer questions, provide assistance, and resolve account issues for taxpayers face to face.

<sup>18</sup> The Agency-Wide Shared Services *Business Performance Review*. The Business Performance Review process is conducted quarterly for each operating division. During these reviews, division commissioners and chiefs discuss their progress on meeting their performance targets or goals and new or emerging issues that may affect major programs and performance.



---

## *The Physical Security Risk Assessment Program Needs Improvement*

---

At one location we visited, the risk assessment failed to disclose that visitors to a childcare center did not receive the appropriate security screening.<sup>19</sup> This specific childcare center is located inside of the IRS building, but visitors enter the childcare center space through a separate reception area where there is no physical security screening. Additionally, childcare center visitors are allowed to enter the overall campus grounds with their vehicle if the childcare center has provided their name to the guard on duty at the entrance.

For this childcare center, we observed that FPS guards do not screen visitors, and we were informed that PSEP office management are unaware of what screening procedures are used by the childcare center. The IRS facility the childcare center is located in is unique because it houses critical IRS infrastructure and is designated as a combined FSL IV and V. Because of the significance of this facility, ISC standards<sup>20</sup> require that all visitors be screened by an armed FPS guard, be screened via a magnetometer, and be submitted to x-raying of personal items. In contrast, we visited two other FSL IV buildings that house childcare centers and observed that they screened visitors as required by ISC standards.

PSEP office staff explained that the childcare center at this facility is operated by a private company that leases the space directly from the General Services Administration. According to PSEP office management, the General Services Administration made a decision to lease the childcare center space to a private company. In addition, after being advised of the situation on December 3, 2012, PSEP office management stated that they believed appropriate screening measures were in place at this facility but did not provide any documentation to confirm that visitors to the childcare center space are screened by the FPS. We subsequently revisited the childcare center on December 18, 2012, and confirmed that visitors still enter the childcare center without being screened by the FPS. Because the general public is allowed access to the IRS grounds and facility and come in close proximity to IRS operations, appropriate security measures should be in place to ensure the safety of the approximately 2,626 IRS employees as well as visitors at this facility.

At another location we visited, the countermeasures recommended by PSEP office staff were not implemented, although they were funded and provided to the facility. During our site visit to this FSL III facility, we found that the local manager of the TAC had not implemented the countermeasures that the PSEP office security staff recommended after the CY 2010 risk assessment review. The risk assessment recommended that the office space be reconfigured (by moving a wall between the waiting area and the entrance to the office) to allow the armed FPS security guard to see visitors entering the facility and those seated in the waiting room.

---

<sup>19</sup> The ISC standard requires that the screening consists of having the individual go through the magnetometer or be screened with a handheld magnetometer wand as well as screening all bags and packages that the person has in his or her possession. A magnetometer is a form of electronic screening and may be a device persons walk through or a handheld device.

<sup>20</sup> Department of Homeland Security, *FSL Determinations for Federal Facilities, An Interagency Security Committee Standard* (March 2008).



---

## *The Physical Security Risk Assessment Program Needs Improvement*

---

Additionally, a handheld magnetometer wand was recommended so that the guard could screen the visitors as required by the ISC standards for an FSL III facility.

The TAC manager told us that he initially reconfigured the office and removed the wall in accordance with the risk assessment recommendation. However, he did not like the office reconfiguration or having to use the handheld magnetometer wand to screen visitors. Without informing the PSEP office, the TAC manager stopped using the magnetometer wand and reconfigured the office back to the way it was before the risk assessment. The security specialist responsible for this facility stated that she was very familiar with the facility and was surprised that the countermeasures were not implemented by the TAC manager. The security specialist also stated that there is no mechanism in place to follow up on recommended countermeasures resulting from the risk assessments. A follow-up visit to the TAC in April 2013 found that this condition had not been addressed. The ongoing vulnerability continues to expose IRS employees and taxpayers because critical countermeasures are not in place.

### **Risk assessments prior to CY 2010 were not maintained at sites visited**

For eight of the 10 sites we visited, PSEP office management did not provide us with risk assessments that were conducted prior to CY 2010 because records were not retained. PSEP office management also could not provide us with the dates risk assessments were performed at those locations prior to CY 2010. Consequently, we could not determine how long security vulnerabilities identified in CY 2010 had existed for these locations. The ISC standards require that risk assessments be performed every five years for facilities designated as FSL I and FSL II and every three years for facilities designated as FSLs III, IV, and V. However, PSEP office management stated that their policy is to retain risk assessment records for only three years or until discontinuance of the facility (whichever is sooner).<sup>21</sup> Therefore, records from prior risk assessments may not be available for security personnel to review when upcoming risk assessments are scheduled for FSL I and FSL II facilities.

Without access to prior risk assessment documentation, the program lacks transparency and the PSEP office cannot provide assurance that the required risk assessments are performed timely or that security vulnerabilities raised in the past have been mitigated or resolved.

### ***Recommendations***

The Director, PSEP, should:

**Recommendation 4:** Follow the prioritization schedule developed by PSEP office management to implement the recommendations from the CY 2010 risk assessments and ensure that the most critical security vulnerabilities are addressed as funding becomes available.

---

<sup>21</sup> Internal Revenue Manual 1.15.20 (Oct. 19, 2010).



---

*The Physical Security Risk Assessment  
Program Needs Improvement*

---

**Management's Response:** The IRS agreed with this recommendation. The Director, PSEP, will follow the prioritization schedule to implement the recommendations from the CY 2010 risk assessments. As funding becomes available, the most critical security vulnerabilities will be addressed.

**Recommendation 5:** Develop a process to ensure that required countermeasures are in place and functioning as required at all TACs.

**Management's Response:** The IRS agreed with this recommendation. The Director, PSEP, will develop a process to ensure that required countermeasures are in place and functioning as required at all TACs.

**Recommendation 6:** Implement appropriate security protocols at the facility with the childcare center to ensure that all visitors entering the campus grounds and the building are screened according to ISC standards.

**Management's Response:** The IRS agreed with this recommendation. The Director, PSEP, will ensure that language is included in Physical Security Internal Revenue Manual 10.2.11, *Basic Security Concepts*, that clarifies the requirement to ensure that visitors entering the campus grounds and the building are screened according to ISC standards before entering the childcare center.

**Recommendation 7:** Ensure that risk assessment documents are retained long enough so they will be available when future risk assessments are conducted.

**Management's Response:** The IRS agreed with this recommendation. The Director, PSEP, will ensure that the Standard Operating Procedures 021(a), *Risk Assessments*, is updated to include the requirement that risk assessments are to be maintained until a new risk assessment is completed.





---

*The Physical Security Risk Assessment  
Program Needs Improvement*

---

## **Appendix I**

### *Detailed Objective, Scope, and Methodology*

The overall objective of this review was to determine whether physical security risk assessments were conducted as required at all IRS facilities. Our review focused on the risk assessments conducted by the PSEP office in CY 2010, which addressed the IRS Commissioner's requirement to conduct risk assessments at all IRS-occupied facilities and identify measures needed to improve employee safety. To accomplish our objective, we:

- I. Determined the process used by the IRS to conduct physical security risk assessments of its facilities in CY 2010.
  - A. Interviewed PSEP office management to gain an understanding of the procedures used to conduct the physical security risk assessments.
  - B. Identified the policy, guidelines, *etc.*, used by the IRS for conducting the physical security risk assessments.
  - C. Requested a list of all IRS facilities as of December 31, 2010, the endpoint of the risk assessment project.
- II. Determined if physical security risk assessments were performed in CY 2010 for all IRS facilities.
  - A. Obtained all physical security risk assessments conducted by the IRS in CY 2010 and confirmed whether a physical security risk assessment was performed for every IRS facility as required.
  - B. Obtained June 2010 reports from the Treasury Integrated Management Information System<sup>1</sup> and the GDI to identify all occupied facilities.
  - C. Compared the list of IRS facilities with the physical security risk assessments conducted in CY 2010.
- III. Assessed the process followed by IRS personnel when performing physical security risk assessments in CY 2010.

---

<sup>1</sup> Treasury Integrated Management Information System supports payroll and personnel processing and reporting requirements for the IRS. The system contains data for IRS employees including job series, grade, and location. This system is currently operated by the U.S. Department of Agriculture at their National Finance Center in New Orleans, Louisiana, which is a third party to the IRS.



---

*The Physical Security Risk Assessment  
Program Needs Improvement*

---

- A. Selected a judgmental sample<sup>2</sup> of 10 facilities to review based on the FSL of the facility, the geographic location, and the type of facility. A judgmental sample of 10 facilities of the more than 600 facilities was selected due to resource constraints associated with physical travel to the various locations.
- B. Performed a site visitation to the 10 facilities selected in our sample.
  1. Determined whether any of the vulnerabilities identified during the physical security risk assessments still exist.
  2. Interviewed IRS personnel who performed the physical security risk assessments to obtain their feedback on the assessment process and whether they are aware of any unreported vulnerabilities that were in existence at the time of the CY 2010 assessments.
- C. Determined how the recommendations and findings in the physical security risk assessments were addressed, implemented, or mitigated.

**Internal controls methodology**

Internal controls relate to management's plans, methods, and procedures used to meet their mission, goals, and objectives. Internal controls include the processes and procedures for planning, organizing, directing, and controlling program operations. They include the systems for measuring, reporting, and monitoring program performance. We determined the following internal controls were relevant to our audit objective: policies and procedures guiding the risk assessment process, PSEP office staff qualifications and training, and management oversight. We evaluated these controls by interviewing IRS management, reviewing a sample of risk assessments performed in CY 2010, and reviewing applicable documentation, including the pertinent ISC standards to support the program.

---

<sup>2</sup> A judgmental sample is a nonstatistical sample, the results of which cannot be used to project to the population.



*The Physical Security Risk Assessment  
Program Needs Improvement*

---

**Appendix II**

*Major Contributors to This Report*

Gregory D. Kutz, Assistant Inspector General for Audit (Management Services and Exempt Organizations)  
Jeffrey M. Jones, Director  
Jonathan T. Meyer, Director  
Janice M. Pryor, Audit Manager  
Yasmin B. Ryan, Lead Auditor  
Allen L. Brooks, Senior Auditor  
Michele N. Strong, Senior Auditor



*The Physical Security Risk Assessment  
Program Needs Improvement*

---

**Appendix III**

*Report Distribution List*

Acting Commissioner  
Office of the Commissioner – Attn: Chief of Staff C  
Deputy Commissioner for Operations Support OS  
Deputy Chief Financial Officer OS:CFO  
Director, Physical Security and Emergency Preparedness OS:A:PSEP  
Director, Risk Management Operations and Policy OS:A:PSEP  
Director, Security Standards and Enhancements OS:A:PSEP  
Chief Counsel CC  
National Taxpayer Advocate TA  
Director, Office of Legislative Affairs CL:LA  
Director, Office of Program Evaluation and Risk Analysis RAS:O  
Office of Internal Control OS:CFO:CPIC:IC  
Audit Liaison: Chief, Agency-Wide Shared Services OS:A



---

*The Physical Security Risk Assessment  
Program Needs Improvement*

---

## **Appendix IV**

### *Outcome Measure*

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

#### **Type and Value of Outcome Measure:**

- Protection of Resources – Potential; five facilities were potentially at risk for having inadequate physical security or security protocols that were not in compliance with ISC standards. Approximately 248 IRS employees were potentially affected in those five facilities (see page 4).

#### **Methodology Used to Measure the Reported Benefit:**

We compared PSEP office inventory lists of IRS-occupied buildings to the June 2010 GDI reports to determine if any facilities were omitted from the CY 2010 risk assessment project. We found that the IRS did not conduct risk assessments at these five buildings, housing 248 IRS employees, which are currently open. We traced the five buildings to the June 2010 GDI report to confirm the number of employees at each location.

To determine if any buildings were omitted, we compared both the June 2010 GDI report and the June 2010 Treasury Integrated Management Information System report against the IRS's list to receive a risk assessment, but risk assessments were not completed.



The Physical Security Risk Assessment  
Program Needs Improvement

**Appendix V**

*Facility Security Level Determination Matrix*

Factor	Points			
	1 point	2 points	3 points	4 points
Mission Criticality	Low	Medium	High	Very High
Symbolism	Low	Medium	High	Very High
Facility Population	<100	101–250	251–750	>750
Facility Size (Square Footage)	<10,000	10,000– 100,000	100,001– 250,000	>250,000
Threat to Tenant Agencies	Low	Medium	High	Very High
Intangible Factors	—	—	—	—
<b>Total Score</b>	—	—	—	—

Source: PSEP office management.

Note: The FSL may be raised or lowered one level at the discretion of the Agency Designated Official based on intangible factors. However, the intangible factor should not be used to raise or lower the FSL in response to a particular threat act.

Scoring	Total Points to Determine the FSL
Level I	5–7 Points
Level II	8–12 Points
Level III	13–17 Points
Level IV	18–20 Points
Level V	The criteria and decisionmaking authority for identifying Level V facilities are within the purview of the individual agency.

Source: PSEP office management.



*The Physical Security Risk Assessment  
Program Needs Improvement*

**Appendix VI**

*Fourteen Internal Revenue Service Buildings  
That Did Not Receive a Risk Assessment  
in Calendar Year 2010*

<b>Building Number</b>	<b>FSL</b>	<b>City, State</b>	<b>Type of Property</b>	<b>Number of IRS Employees</b>
AK0029	IV	Fairbanks, Alaska	IRS Office	6
CA6000	II	San Francisco, California	IRS Office	179
CA8072	Unknown	Santa Cruz, California	IRS Office	10
CT0059	IV	Bridgeport, Connecticut	IRS Office	54
DE0017	II	Dover, Delaware	IRS Office	10
FL2046	II	Deerfield Beach, Florida	IRS Office	104
KY3048	II	Florence, Kentucky	IRS Office	19
MI1942	II	Clinton Township, Michigan	IRS Office	50
PA0462	IV	Philadelphia, Pennsylvania	Campus	1,713
PA0719	II	Bethlehem, Pennsylvania	IRS Office	34
PA0727	IV	Philadelphia, Pennsylvania	Campus	479
PA0739	III	Philadelphia, Pennsylvania	Campus	222
PA6520	IV	Philadelphia, Pennsylvania	Campus	1,520
TX2353	II	Bryan, Texas	IRS Office	8
<b>Total IRS Employees Stationed at the 14 Buildings in CY 2010</b>				<b>4,408</b>

*Source: Treasury Inspector General for Tax Administration review of the June 2010 GDI report.*



The Physical Security Risk Assessment  
Program Needs Improvement

Appendix VII

Status of 14 Internal Revenue Service Buildings  
That Did Not Receive Timely Risk Assessments

Building Number	City, State	Was a Risk Assessment Completed in CY 2010	Was a Risk Assessment Completed After CY 2010	Date of Risk Assessment	Date Building Closed
AK0029	Fairbanks, Alaska	No	Yes	10/18/2012	—
CA6000	San Francisco, California	No	No	—	8/31/2011
CA8072	Santa Cruz, California	No	No	—	5/31/2012
CT0059	Bridgeport, Connecticut	No	Yes	11/12/2012	—
DE0017	Dover, Delaware	No	No	—	11/30/2011
FL2046	Deerfield Beach, Florida	No	Yes	9/28/2012	—
KY3048	Florence, Kentucky	No	No	—	11/30/2011
MI1942	Clinton Township, Michigan	No	Yes	3/05/2012	—
PA0462	Philadelphia, Pennsylvania	No	No	—	4/30/2011
PA0719	Bethlehem, Pennsylvania	No	Yes	6/15/2012	—
PA0727	Philadelphia, Pennsylvania	No	No	—	4/30/2011
PA0739	Philadelphia, Pennsylvania	No	No	—	4/30/2011
PA6520	Philadelphia, Pennsylvania	No	No	—	4/30/2011
TX2353	Bryan, Texas	No	No	—	9/30/2011
<b>Buildings That Closed After CY 2010 and Did Not Receive a Risk Assessment</b>					<b>9</b>
<b>Buildings That Received a Risk Assessment After CY 2010</b>					<b>5</b>

Source: Treasury Inspector General for Tax Administration review of the June 2010 GDI report and the June 2010 Treasury Integrated Management Information System report.





*The Physical Security Risk Assessment  
Program Needs Improvement*

**Appendix VIII**

*Fourteen Physical Security and  
Emergency Preparedness Office Territories*

<b>Territory</b>	<b>State/Location</b>
<b>Andover</b>	Connecticut Maine Massachusetts New Hampshire Rhode Island Vermont
<b>Atlanta</b>	Alabama Florida Georgia
<b>Austin</b>	Texas
<b>Brookhaven</b>	New York
<b>Covington</b>	Kentucky Ohio
<b>Detroit</b>	Illinois Indiana Michigan Wisconsin
<b>Fresno</b>	Alaska California (Fresno, Tulare, and Visalia) Idaho Nevada Oregon Washington



*The Physical Security Risk Assessment  
Program Needs Improvement*

Territory	State/Location
<b>Kansas City</b>	Iowa Kansas Minnesota Missouri Nebraska North Dakota Oklahoma South Dakota
<b>Martinsburg</b>	North Carolina Puerto Rico South Carolina United States Virgin Islands Virginia West Virginia
<b>Memphis</b>	Arkansas Louisiana Mississippi Tennessee
<b>National Capital</b>	Delaware Maryland
<b>Oakland</b>	California (Rest of the State) Hawaii
<b>Ogden</b>	Arizona Colorado Montana New Mexico Utah Wyoming
<b>Philadelphia</b>	Pennsylvania New Jersey

Source: PSEP office website, March 2013.



*The Physical Security Risk Assessment  
Program Needs Improvement*

**Appendix IX**

*Management's Response to the Draft Report*

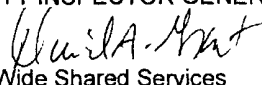


CHIEF  
AGENCY-WIDE  
SHARED SERVICES

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

August 26, 2013

MEMORANDUM FOR MICHAEL E. MCKENNEY  
ACTING DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: David A. Grant   
Chief, Agency-Wide Shared Services

SUBJECT: Draft Audit Report – The Physical Security Risk Assessment  
Program Needs Improvement (Audit #201210007)

Thank you for the opportunity to respond to the subject draft audit report. The audit was conducted to determine whether physical security risk assessments were conducted as required at all Internal Revenue Service (IRS) facilities.

Ensuring the security of IRS employees, facilities and taxpayers is of the utmost importance to us. We agree with the seven recommendations that will strengthen our risk assessment program and will implement the corrective actions detailed in our attached response.

We appreciate the continued support and assistance provided by your office. If you have any questions, please contact me at (202) 622-7500. If there are any technical questions, a member of your staff may contact Kevin McIver, Director, Physical Security and Emergency Preparedness, at (202) 622-0831. For matters concerning audit procedural follow-up, please contact Patricia Alvarado, Resource and Operations Management, Agency-Wide Shared Services, at (202) 622-5542.

Attachment



---

*The Physical Security Risk Assessment  
Program Needs Improvement*

---

Attachment

**RECOMMENDATION 1:**

Develop a process to ensure that inventory records include all relevant information, such as the date facilities are open and closed as well as the dates risk assessments should be performed.

**CORRECTIVE ACTION:**

We agree with this recommendation. The Director, Physical Security and Emergency Preparedness (PSEP), Agency-Wide Shared Services (AWSS), implemented a process to ensure that PSEP inventory records include all relevant information, such as the date facilities are opened and closed as well as the dates risk assessments should be performed. PSEP pulls the Graphic Database Interface (GDI) Building Directory and the Joint Information Management Site (JIMS) Consolidated Report from the JIMS site once a month. These reports are used by the PSEP staff to maintain an accurate building inventory and to calculate the due dates for risk assessments.

**IMPLEMENTATION DATE:**

February 28, 2013 (Completed)

**RESPONSIBLE OFFICIAL:**

Director, Physical Security and Emergency Preparedness, Agency-Wide Shared Services

**CORRECTIVE ACTION MONITORING PLAN:**

Corrective action will be entered into the Joint Audit Management Enterprise System (JAMES) as completed.

**RECOMMENDATION 2:**

Work with the FPS to ensure that the IRS receives copies of FPS risk assessments performed at IRS facilities and a schedule of when the FPS plans to perform future risk assessments of IRS facilities.

**CORRECTIVE ACTION:**

We agree with this recommendation. The Director, PSEP, will request from the Federal Protective Service (FPS) National Director, copies of all FPS risk assessments of space in IRS inventory, and a schedule of when FPS plans to perform future risk assessments.

**IMPLEMENTATION DATE:**

March 31, 2014



---

*The Physical Security Risk Assessment  
Program Needs Improvement*

---

2

**RESPONSIBLE OFFICIAL:**

Director, Physical Security and Emergency Preparedness, Agency-Wide Shared Services

**CORRECTIVE ACTION MONITORING PLAN:**

Physical Security and Emergency Preparedness will enter accepted corrective actions into JAMES. These corrective actions are monitored on a monthly basis until completion.

**RECOMMENDATION 3:**

Update the policies for the risk assessment program to distinguish which facilities, such as childcare centers, parking lots and storage facilities, require an FPS risk assessment and which ones, such as IRS employee-occupied facilities, require a PSEP office risk assessment.

**CORRECTIVE ACTION:**

We agree with this recommendation. The Director, PSEP, will update Physical Security Internal Revenue Manual (IRM) 10.2.11, *Basic Security Concepts*, and Standard Operating Procedure (SOP) 021(a), *Risk Assessments* to distinguish which risk assessments are the responsibility of FPS and which risk assessments are the responsibility of PSEP.

**IMPLEMENTATION DATE:**

April 30, 2014

**RESPONSIBLE OFFICIAL:**

Director, Physical Security and Emergency Preparedness, Agency-Wide Shared Services

**CORRECTIVE ACTION MONITORING PLAN:**

Physical Security and Emergency Preparedness will enter accepted corrective actions into JAMES. These corrective actions are monitored on a monthly basis until completion.

**RECOMMENDATION 4:**

Follow the prioritization schedule developed by PSEP office management to implement the recommendations from the CY 2010 risk assessments and ensure that the most critical security vulnerabilities are addressed as funding becomes available.



---

*The Physical Security Risk Assessment  
Program Needs Improvement*

---

3

**CORRECTIVE ACTION:**

We agree with this recommendation. The Director, PSEP, will follow the prioritization schedule to implement the recommendations from the CY 2010 risk assessments. As funding becomes available, the most critical security vulnerabilities will be addressed.

**IMPLEMENTATION DATE:**

January 31, 2014

**RESPONSIBLE OFFICIAL:**

Director, Physical Security and Emergency Preparedness, Agency-Wide Shared Services

**CORRECTIVE ACTION MONITORING PLAN:**

Physical Security and Emergency Preparedness will enter accepted corrective actions into JAMES. These corrective actions are monitored on a monthly basis until completion.

**RECOMMENDATION 5:**

Develop a process to ensure that required countermeasures are in place and functioning as required at all TACs.

**CORRECTIVE ACTION:**

We agree with this recommendation. The Director, PSEP, will develop a process to ensure that required countermeasures are in place and functioning as required at all Taxpayer Assistance Centers (TACs).

**IMPLEMENTATION DATE:**

March 31, 2014

**RESPONSIBLE OFFICIAL:**

Director, Physical Security and Emergency Preparedness, Agency-Wide Shared Services

**CORRECTIVE ACTION MONITORING PLAN:**

Physical Security and Emergency Preparedness will enter accepted corrective actions into JAMES. These corrective actions are monitored on a monthly basis until completion.

**RECOMMENDATION 6:**

Implement appropriate security protocols at the facility with the childcare center to ensure that all visitors entering the campus grounds and the building are screened according to the ISC standards.



---

*The Physical Security Risk Assessment  
Program Needs Improvement*

---

4

**CORRECTIVE ACTION:**

We agree with this recommendation. The Director, PSEP, will ensure that language be included in Physical Security IRM 10.2.11, *Basic Security Concepts* that clarifies the requirement to ensure that visitors entering the campus grounds and the building are screened according to the Interagency Security Committee (ISC) standards before entering the childcare center.

**IMPLEMENTATION DATE:**

April 30, 2014

**RESPONSIBLE OFFICIAL:**

Director, Physical Security and Emergency Preparedness, Agency-Wide Shared Services

**CORRECTIVE ACTION MONITORING PLAN:**

Physical Security and Emergency Preparedness will enter accepted corrective actions into JAMES. These corrective actions are monitored on a monthly basis until completion.

**RECOMMENDATION 7:**

Ensure that risk assessment documents are retained long enough so they will be available when future risk assessments are conducted.

**CORRECTIVE ACTION:**

We agree with this recommendation. The Director, PSEP, will ensure the SOP 021(a), *Risk Assessments* is updated to include the requirement that risk assessments are to be maintained until a new risk assessment is completed.

**IMPLEMENTATION DATE:**

March 31, 2014

**RESPONSIBLE OFFICIAL:**

Director, Physical Security and Emergency Preparedness, Agency-Wide Shared Services

**CORRECTIVE ACTION MONITORING PLAN:**

Physical Security and Emergency Preparedness will enter accepted corrective actions into JAMES. These corrective actions are monitored on a monthly basis until completion.