TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION

To Avoid Duplication, the Internal Revenue Service Should Make Use of Federal Protective Service Risk Assessments

September 15, 2015

Reference Number: 2015-10-077

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.

Redaction Legend:
2 = Information That, If Disclosed, Could Reasonably Be Expected to Endanger the Safety or Life of Any Individual

Phone Number / 202-622-6500
E-mail Address / TIGTACommunications@tigta.treas.gov
Website / http://www.treasury.gov/tigta

TO AVOID DUPLICATION, THE INTERNAL REVENUE SERVICE SHOULD MAKE USE OF FEDERAL PROTECTIVE SERVICE RISK ASSESSMENTS

Highlights

Final Report issued on September 15, 2015

Highlights of Reference Number: 2015-10-077 to the Internal Revenue Service Chief, Agency-Wide Shared Services.

IMPACT ON TAXPAYERS

Due to the nature of the IRS's mission, the organization remains at risk for violence directed at IRS employees and facilities. Effective security measures are key to ensure that IRS employees and facilities are protected from potential threats. At the same time, the IRS has limited resources available and thus must protect employees, property, and taxpayers who visit IRS facilities in the most efficient way possible.

WHY TIGTA DID THE AUDIT

This audit was initiated because there appeared to be duplication between the IRS risk assessment program and the Federal Protective Service's (FPS) mandate. The FPS has the responsibility to conduct risk assessments at the more than 600 IRS facilities throughout the country. The overall objectives of this review were to determine what services the IRS receives for security fees paid to the FPS for risk assessments and to determine whether there is duplication in risk assessment services performed by IRS personnel.

WHAT TIGTA FOUND

While the IRS is required to pay the FPS for risk assessments, it does not fully benefit from the information provided in FPS risk assessments. Specifically, the IRS does not use FPS risk assessments or evaluate recommendations that FPS inspectors made to improve the security at IRS facilities. As a result, IRS risk assessments sometimes do not address security concerns identified by the FPS. The IRS also does not use FPS risk assessments as part of a recently instituted revalidation process. This new process, which is limited to revalidating the security of a facility based on prior IRS risk assessments, did not take into account findings included in the most recent FPS risk assessments. By using FPS assessments, the IRS could reduce duplication and improve security for IRS employees, facilities, and visiting taxpayers.

In addition, the IRS does not consider when a facility last received a risk assessment from the FPS when scheduling its own risk assessments. As a result, the IRS conducted 57 risk assessments at facilities that had already received an FPS risk assessment within the last two years.

Finally, the IRS paid almost $100 million in basic security fees to the FPS for Fiscal Years 2010 through 2014, which included charges for FPS-prepared risk assessments; however, the IRS has also incurred additional costs to perform its own risk assessments of the same facilities. Further, IRS management does not track the cost of its program.

WHAT TIGTA RECOMMENDED

TIGTA made three recommendations to the Director, Facilities Management and Security Services, to address identified weaknesses. For example, TIGTA recommended that the IRS develop a process to retain and review FPS risk assessments and evaluate whether the IRS can rely on FPS risk assessments of some IRS facilities and eliminate the duplicate IRS risk assessment for those facilities.

In their response, IRS management agreed with TIGTA's recommendations. The IRS plans to engage with the FPS to implement a process to obtain Facility Security Assessments for IRS facilities; evaluate whether the IRS can rely on FPS risk assessments at some IRS facilities and eliminate duplicate IRS risk assessments as appropriate; and correct the errors and revise the risk assessment process to include the periodic review of information in the risk assessment repository and Security Information Management System.

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

DEPARTMENT OF THE TREASURY

WASHINGTON, D.C. 20220

September 15, 2015

MEMORANDUM FOR CHIEF, AGENCY-WIDE SHARED SERVICES

FROM: Michael E. McKenney
Deputy Inspector General for Audit

SUBJECT: Final Audit Report – To Avoid Duplication, the Internal Revenue Service Should Make Use of Federal Protective Service Risk Assessments (Audit # 201510001)

This report presents the results of our review to determine what services the Internal Revenue Service (IRS) receives for security fees paid to the Federal Protective Service for risk assessments and to determine whether there is duplication in risk assessment services performed by IRS personnel. This audit is included in our Fiscal Year 2015 Annual Audit Plan and addresses the major management challenge of Achieving Program Efficiencies and Cost Savings.

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

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).

Table of Contents

Abbreviations

CY	Calendar Year
FMSS	Facilities Management and Security Services
FPS	Federal Protective Service
IRS	Internal Revenue Service
ISC	Interagency Security Committee

Background

Federal facilities continue to be targets for potential terrorist attacks and other acts of violence, as evidenced by the 2010 attack on the Internal Revenue Service (IRS) building in Austin, Texas. Due to the nature of the IRS mission, the organization remains a focus for some taxpayers' frustration and threats of violence directed at IRS employees continue to be a serious concern.

The Department of Homeland Security's Federal Protective Service (FPS) is the primary Federal agency responsible for providing physical security and law enforcement services for the nearly 9,600 Federal facilities that are under the control and custody of the General Services Administration. As the security police division of the Department of Homeland Security, the FPS is responsible for policing, securing, and ensuring a safe environment in which Federal agencies can conduct their business.

The FPS also has the responsibility to conduct risk assessments for all the facilities under its purview including the more than 600 IRS facilities throughout the country. Risk assessments help decisionmakers identify and evaluate security risk and implement protective measures to mitigate risk. Further, risk assessments play a critical role in helping agencies tailor protective measures to reflect their facilities' unique circumstances and enable them to allocate security resources more effectively. Risk assessment standards are established by the Department of Homeland Security's Interagency Security Committee (ISC).[1]

The FPS is a fully fee-funded organization, and security fees are comprised of basic and building/agency specific charges. A basic security fee is assessed for all General Services Administration-controlled space and includes the cost of performing facility risk assessments.[2] The fee rate is set annually on a per-square-foot basis and is currently $.74 per square foot. Applicable agencies are billed on a monthly basis and pay the fee through an Intra-Governmental Payment and Collection[3] agreement.

To help ensure that IRS facilities are safe, the IRS Office of Facilities Management and Security Services (FMSS) implemented an internal risk assessment program. The IRS and FPS risk assessments follow the same ISC standards and are conducted at the same IRS facilities, although under current guidelines, the Office of FMSS does not perform risk assessments at peripheral facilities such as childcare centers, parking garages/lots, and storage facilities. The

[1] The ISC was created after the Oklahoma City bombing of the Alfred Murrah Federal Building in April 1995. ISC standards consist of a baseline set of physical security measures to be applied to all Federal facilities.
[2] See Appendix V for a list of the services provided by the FPS that are included in the basic fee.
[3] The Intra-Governmental Payment and Collection system allows Federal program agencies to transfer funds from one agency to another.

Government Accountability Office[4] previously reported that multiple Federal agencies, including the IRS, are incurring additional costs by completing their own assessments while paying the FPS to complete risk assessments for the same facilities.

This review was performed at the IRS Headquarters in the Agency-Wide Shared Services function in Washington, D.C., during the period October 2014 through June 2015. 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 objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. Detailed information on our audit objectives, scope, and methodology is presented in Appendix I. Major contributors to the report are listed in Appendix II.

[4] Government Accountability Office, GAO-12-342SP, *2012 Annual Report: Opportunities to Reduce Duplication, Overlap and Fragmentation, Achieve Savings, and Enhance Revenue* (Feb. 2012).

Results of Review

The Internal Revenue Service Should Use Federal Protective Service Risk Assessments to Reduce Duplication

During a previous audit,[5] we found the IRS did not obtain some FPS risk assessments and was not tracking recommended security improvements identified by the FPS. At the conclusion of that audit, we recommended that the IRS work with the FPS to ensure that it 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. The IRS agreed with this recommendation and now receives an annual list of FPS-planned risk assessments. However, during interviews with IRS management, they informed us that because they perform their own internal risk assessments, they do not keep track of when FPS risk assessments are performed or the findings and recommendations made by the FPS.

We asked the IRS why it did not use any of the 108 risk assessments performed by the FPS in Calendar Year (CY) 2013 or the 169 risk assessments performed in CY 2014. IRS management stated that the reason they have not stressed using FPS risk assessments is that they believe the IRS performs a more detailed review than the FPS. They explained that IRS physical security specialists conduct risk assessments of IRS facilities in accordance with ISC guidance and IRS standards. In addition, the IRS indicated that the FPS has not always shared its risk assessments with the IRS. However, when we interviewed FPS officials, they stated that it is their policy to share their risk assessments with Federal tenants. Additionally, their risk assessments are prepared by highly trained inspectors and are reviewed by the area regional commanders. We were also advised that both the IRS and the FPS conduct risk assessments using the ISC standards which encompass all aspects of a facility's security.

To determine whether the IRS had received and acknowledged any of the 169 CY 2014 FPS risk assessments, we selected a judgmental sample[6] of 22 recent FPS risk assessments and confirmed that the FPS's findings and recommendations had been provided to IRS representatives. In at least 15 of the 22 instances, the IRS acknowledged that its representative had received a copy of the results of the FPS risk assessment. For the remaining seven risk assessments, another Federal agency was the point of contact for the FPS, and thus it was not clear whether the IRS had requested and received a copy of the risk assessment. Further, we found that IRS employees

[5] Treasury Inspector General for Tax Administration, Ref. No. 2013-10-101, *The Physical Security Risk Assessment Program Needs Improvement* (Sept. 2013).
[6] A judgmental sample is a nonprobability sample, the results of which cannot be used to project to the population.

had been interviewed as part of the FPS risk assessment, and they were aware the review was in process.

In addition, the IRS could benefit from using the FPS risk assessments because they highlight security vulnerabilities that the IRS may be unaware of. For example, in a risk assessment performed by the FPS in March 2013, the inspector found that this facility did not meet the minimum requirements for the ISC standards related to biological filtration and recommended that all heating, ventilation, and air conditioning filters be replaced. The IRS risk assessment issued in August 2013 made no mention of this vulnerability or whether it had been mitigated. At a minimum, the IRS should obtain and review FPS risk assessments to ensure that IRS facilities, employees, and taxpayers are protected.

Finally, we also found that in some instances, IRS risk assessments were completed by security specialists who were not physically present at the IRS location for the risk assessment. This brings into question the quality of the risk assessment performed by the IRS as compared to the on-site FPS risk assessment. IRS standard operating procedures state that physical security specialists must perform an on-site review to gather data, interview local law enforcement and occupants, and take photographs if needed. However, for at least nine risk assessments, an IRS security specialist was not physically present at the facility to perform the risk assessment. In some instances, the information needed to prepare risk assessments was gathered months earlier or was obtained by other IRS personnel. For example, we determined that for two Level IV facilities, the physical security specialist relied on data collected previously and FPS risk assessments rather than visiting the facilities. If the IRS continues to conduct risk assessments remotely, in conflict with its own operating procedures, it should always use FPS risk assessments performed by inspectors who are on-site to ensure the safety of IRS personnel and facilities.

The revalidation process could reduce duplication, but the IRS should use FPS risk assessments during its review process

In March 2014, the IRS instituted a new process for some Level I and Level II facilities,[7] which are required to have risk assessments performed every five years according to ISC standards. The IRS has begun the process of "revalidating" prior risk assessments. In order to determine if a risk assessment is eligible for a revalidation, a physical security specialist must complete a one-page form[8] with eight questions. If there have been no significant changes at the facility and all previously identified vulnerabilities have been addressed, the Office of FMSS will forego an on-site risk assessment.

[7] The Facility Security Level of an IRS facility ranges from one (Level I) to five (Level V), with Level V being the highest level for security risk. ISC standards require a risk assessment every three years for Level III to Level V facilities and every five years for Level I and II facilities.
[8] See Appendix VII for a copy of the revalidation form.

Between March 2014 and March 2015, the Office of FMSS revalidated risk assessments for 49 facilities which accounted for 12 percent of its 405 Level I and II facilities during this time period. Office of FMSS management advised us that they established this process to reduce costs such as travel expenses. While we did not evaluate the effectiveness of the revalidation process for this audit, we did find that limited, if any, documentation was retained to support answers provided on the revalidation document.

We also found that the revalidation document did not require the physical security specialist to review the most recent FPS risk assessment or take into account any risks associated with Taxpayer Assistance Centers[9] located at the facilities. The revalidation process appears to be a risk-based decision made by the IRS to conserve resources, but the new process should use recent FPS risk assessments in order to ensure that identified risks are considered by the IRS.

The IRS could reduce duplication by coordinating with the FPS

During CY 2013 and CY 2014, both the FPS and the IRS performed risk assessments at 165 of the same IRS facilities. Further, we identified 57 of the 165 facilities in which the IRS had performed risk assessments after the FPS. This is a concern given the IRS's limited resources and Congress' focus on reducing duplication in Federal programs. Figure 1 shows the time frames when the FPS completed its risk assessments for those 57 facilities.

Figure 1: IRS Risk Assessments Completed After FPS Risk Assessments for CYs 2013 Through 2014

Time Between IRS and FPS Risk Assessments	Number of Facilities
90 calendar days or less after FPS assessment	19
91 to 180 calendar days after FPS assessment	23
181 calendar days to one year after FPS assessment	10
One-to-two years after FPS assessment	5
Total FPS Risk Assessments	**57**

Source: Treasury Inspector General for Tax Administration review of IRS and FPS risk assessments.

The Office of FMSS indicated that there have been recent improvements in communication and coordination efforts between the Office of FMSS and the FPS. The Office of FMSS stated that it

[9] A Taxpayer Assistance Center is an IRS office with employees who answer questions, provide assistance, and resolve account-related issues for taxpayers face to face.

had held quarterly meetings with FPS Headquarters leadership as a part of an FPS Customer Outreach Program. While we were only able to confirm one meeting was held, we believe these meetings are a step in the right direction and should be conducted consistently.

*********;[10] **********2**********2**********2**********. However, during our current review, we identified three risk assessments with incorrect dates, and in each instance, these dates were off by more than one year. Given that these dates may be used to determine when to schedule the next risk assessment, it is imperative that the dates are entered accurately.

Without proper coordination, the IRS will continue to expend resources by performing risk assessments shortly after the FPS has conducted an assessment at the same facility. The IRS should consider relying on FPS risk assessments rather than performing a separate risk assessment on the same facility, especially if the physical security specialist cannot be on-site. This could save resources and reduce duplication.

The IRS is paying the FPS for risk assessments while also conducting its own risk assessments

The IRS paid more than $96 million (an average of more than $19 million annually) in mandated basic security fees to the FPS for Fiscal Years 2010 through 2014. The IRS is required to pay these fees to the FPS as part of the cost associated with space leased through the General Services Administration. Only a portion of the basic security fee is related to facility risk assessments, but the FPS cannot break out the cost of risk assessments versus costs associated with other services covered under the basic security fee.[11] Figure 2 shows the basic security fees paid by fiscal year.

[10] **********2**********2**********

[11] See Appendix V for the services provided by the FPS.

Figure 2: Basic Fees Paid During Fiscal Years 2010 Through 2014

Fiscal Year	Annual Rate Per Square Foot	Basic Fees Paid
2010	.66	$18,171,945
2011	.66	$18,429,309
2012	.74	$20,050,287
2013	.74	$19,970,881
2014	.74	$19,890,379
Total	**----**	**$96,512,801**

Source: IRS Office of FMSS.

While we were able to determine that the IRS has adequate systems in place to ensure the accuracy of fees paid to the FPS based upon its monthly billings, we found the IRS does not track the costs of its own risk assessment program. For example, the Office of FMSS does not maintain a separate budget for the risk assessment program or keep records for all program-specific costs such as travel. We were able to determine that during CY 2014, the IRS spent at least $479,000 on its internal risk assessment program. Those costs include the labor costs associated with physical security specialists who performed the risk assessments and identifiable travel costs associated with the risk assessment program. In addition to labor and travel costs, the IRS spent more than $1.2 million since July 2007 on software development costs associated with the IRS's risk assessment tool.

IRS management indicated they were aware of the duplicate efforts, but they prefer to perform their own risk assessments because their risk assessments are tailored to IRS space and the FPS primarily ensures that the perimeter of a facility is secure. However, we found that both IRS and FPS risk assessments use the same ISC standards[12] and assess the same exterior and interior security risks.[13]

[12] See Appendix VI for a comparison of the two programs.
[13] Per the ISC standards, risk is a measure of potential harm from an undesirable event that encompasses threat, vulnerability, and consequence.

Recommendations

The Director, FMSS, should:

Recommendation 1: Develop a process to retain and review FPS risk assessments and ensure that they are readily available to security personnel. In addition, require an assessment of the FPS's most recent findings as part of any current risk assessment and revalidation processes performed by the IRS.

> ***Management's Response:*** The IRS agreed with this recommendation. The Chief, Agency-Wide Shared Services, will engage with the FPS to develop and implement a process to obtain current and future FPS Facility Security Assessments for IRS facilities upon completion. The IRS will also revise its current risk assessment process to integrate FPS Facility Security Assessment findings in risk assessments and revalidation processes performed by the IRS.

Recommendation 2: Use the *Listing of FPS Planned Risk Assessments* and evaluate whether the IRS can rely on FPS risk assessments of some IRS facilities and eliminate the duplicate IRS risk assessment for those facilities.

> ***Management's Response:*** The IRS agreed with this recommendation. The Chief, Agency-Wide Shared Services, is currently evaluating whether the IRS can rely on FPS risk assessments at some IRS facilities and eliminate the duplicate FMSS risk assessment for those facilities as appropriate.

Recommendation 3: Correct the errors noted in the risk assessment repository and Security Information Management System and ensure that information maintained in those systems is checked regularly for accuracy.

> ***Management's Response:*** The IRS agreed with this recommendation. The Chief, Agency-Wide Shared Services, recognizes that the errors noted within the report were administrative in nature. Regardless, they will correct the errors and revise the current risk assessment process to include the periodic review of information contained in the risk assessment repository and Security Information Management System.

Appendix I

Detailed Objectives, Scope, and Methodology

The overall objectives were to determine what services the IRS receives for security fees paid to the FPS for risk assessments and to determine whether there is duplication in risk assessment services performed by IRS personnel. To accomplish our objectives, we:

I Reviewed IRS policies to gain an understanding of why the IRS performs risk assessments internally while paying FPS fees for the same service.

- A. Determined if there are any policies and procedures related to services provided by the FPS and for-fee arrangements with the General Services Administration and the FPS.
- B. Documented current IRS procedures for performing risk assessments and whether the FPS plays a role.

II. Determined how much the IRS pays the FPS to conduct risk assessments at IRS facilities and the services the FPS provides.

- A. Interviewed IRS management to gain an understanding of the FPS's fee structure, services provided, and how the fees are charged to the IRS.
- B. Determined how much the IRS paid the FPS in basic security fees and whether the IRS pays security fees on all IRS facilities.
- C. Obtained a list of IRS facilities and schedules to determine whether the FPS performed risk assessments during CY 2013 and CY 2014.
- D. Determined whether the IRS monitors FPS risk assessment activities and payments made by the IRS for FPS risk assessments included in the basic security fee.

III. Requested documentation to show the costs of the IRS risk assessment program.

- A. Obtained documentation to establish which facilities received IRS risk assessments in CY 2013 and CY 2014.

IV. Determined the extent of any duplication between FPS and IRS risk assessments.

A. Selected a judgmental sample of 22 of the 169 CY 2014 FPS risk assessments to determine if the findings and recommendations had been provided to IRS representatives.[1]

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 that the following internal controls were relevant to our audit objectives: the policies and procedures guiding the payment of the security fees and the risk assessment process. We evaluated these controls by interviewing IRS management, reviewing the monthly billing and payment process, and reviewing applicable documentation, including the pertinent ISC standards.

[1] We used a judgmental sample because we were not projecting the results to the population of CY 2014 risk assessments.

Appendix II

Major Contributors to This Report

Gregory D. Kutz, Assistant Inspector General for Audit (Management Services and Exempt Organizations)
Jonathan T. Meyer, Director
Janice M. Pryor, Audit Manager
Mary F. Herberger, Lead Auditor
Yasmin B. Ryan, Senior Auditor
Trisa M. Brewer, Auditor

Appendix III

Report Distribution List

Commissioner C
Office of the Commissioner – Attn: Chief of Staff C
Deputy Commissioner for Operations Support OS
Director, Facilities Management and Security Services OS:A:FMSS
Deputy Director, Facilities Management and Security Services OS:A:FMSS
Chief Counsel CC
National Taxpayer Advocate TA
Director, Office of Program Evaluation and Risk Analysis RAS:O
Director, Office of Audit Coordination OS:PPAC:AC
Office of Internal Control OS:CFO:CPIC:IC
Audit Liaisons:
    Deputy Commissioner for Operations Support OS
    Chief, Agency-Wide Shared Services OS:A

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:

- Reliability of Information – Potential; we identified three risk assessments with incorrect dates in the Security Information Management System, and in each instance, these dates were incorrect between one and four years (see page 3).

Methodology Used to Measure the Reported Benefit:

We identified risk assessments for three facilities that the IRS initially indicated were issued in CY 2014, and we later confirmed that all three risk assessments were issued prior to CY 2014.

Appendix V

Services Provided by the Federal Protective Service

The following services are provided by the FPS in exchange for the basic security fee:

- General law enforcement on Public Building Service-controlled property
- Physical security assessments
- Crime prevention and awareness training
- Advice and assistance to building security committees
- Intelligence-sharing program
- Criminal investigation
- Assistance and coordination in Occupancy Emergency Plan development
- Coordination of mobilization and response to terrorist threat or civil disturbance
- Program administration for security guard contracts
- Megacenter operations for monitoring building perimeter alarms and dispatching appropriate law enforcement response

Source: Title 41 Code of Federal Regulations - Federal Management Regulations Section 102-85.35.

Appendix VI

Comparison of Federal Protective Service and Internal Revenue Service Risk Assessment Programs

Standard	FPS	IRS
Statutorily responsible for protecting IRS buildings, grounds, and property	Yes	No – No statutory responsibility.
Determines the initial Facility Security Level	Yes	No – Although the final Facility Security Level determination rests with the designated official and/or Facility Security Committee who make the decision in consultation with the General Services Administration and the FPS.
When conducting risk assessments, considers all space occupied by Federal tenants	Yes	No – The IRS generally does not have access to other tenant's space.
Performs risk assessments at peripheral IRS facilities such as childcare centers, credit unions, and parking lots	Yes	No – Current procedures only require risk assessments at facilities under the control of IRS personnel.
Conducts risk assessments using ISC standards	Yes	Yes
Uses an ISC-approved tool when conducting risk assessments	No – However, the FPS is working toward developing an ISC-approved tool.	No – The IRS has no plan to obtain ISC certification of its risk assessment tool.
Considers area crime statistics as part of the risk assessment	Yes	Yes
Interviews multiple tenants during risk assessment review	Yes	Yes
Recommends countermeasures to address security vulnerabilities identified during risk assessment	Yes	Yes
Performs risk assessments at certain facilities using a "revalidation" process	No – Inspectors are required to be physically present.	Yes

Source: Treasury Inspector General for Tax Administration analysis of IRS and FPS risk assessment programs.

Appendix VII

Physical Security and Emergency Preparedness Risk Assessment Re-Validation Form

Physical Security & Emergency Preparedness
Risk Assessment Re-validation Form

Facility # _____

Address: _____

_____

Facility Type (choose one):

POD FOB

CC Campus

Security Level: _____

Specialist: _____

Date of Last Assessment: _____

Is the current Risk Assessment on file less than 5 years old?

Yes No

If Yes, go to next question. If No, a new Risk Assessment is required.

Has a Physical Security Specialist met with the Commissioner's representative since the last Risk Assessment?

Yes No

If Yes, go to next question. If No, a new Risk Assessment is required.

Have all identified vulnerabilities been addressed (mitigated or countermeasure funding requested)?

Yes No

If Yes, go to next question. If No, a new Risk Assessment is required.

Are there significant changes in documented crime statistics in the immediate area since the last Risk Assessment? Yes No

If Yes, a new risk assessment is required. If No, go to next question.

Have there been significant changes in employee population and/or business mission since the last Risk Assessment? Yes No

If Yes, a new risk assessment is required. If No, go to next question.

Have there been significant building modifications completed since the last Risk Assessment?

Yes No

If Yes, a new risk assessment is required. If No, go to next question.

Is there already a re-validation completed on the Risk Assessment on file?

Yes No

If Yes, a new risk assessment is required. If No, go to next question.

Has there been a significant increase in the number of Incidents reported at this location since the last Risk Assessment? Yes No

If Yes, a new Risk Assessment is required. If No, existing Risk Assessment can be re-validated.

I, _____,

Territory Manager, approve / disapprove this Re-validation.

Concur: _____,

Area Director

Source: IRS Office of FMSS.

Appendix VIII

Management's Response to the Draft Report

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

CHIEF
AGENCY-WIDE
SHARED SERVICES

August 27, 2015

MEMORANDUM FOR MICHAEL E. MCKENNEY
DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: Kevin Q. McIver
Acting Chief, Agency-Wide Shared Services

SUBJECT: Draft Audit Report – To Avoid Duplication, the Internal Revenue Service Should Make Use of Federal Protective Service Risk Asessments (Audit #201510001)

Thank you for the opportunity to respond to the subject draft audit report. We are committed to improving the coordination with the Federal Protective Services and controls over Internal Revenue Service Risk Assessments.

We agree with the three recommendations and will develop and implement the corrective actions detailed in our attached response.

If there are technical questions, a member of your staff may contact Tracey L. Showman, Acting Director, Facilities Management and Security Services, at (703) 414-2151. For matters concerning audit procedural follow-up, please contact Patricia Alvarado, Resource and Operations Management, Agency-Wide Shared Services, at (202) 317-3272 or Steven Scheer, Resource and Operations Management, Agency-Wide Share Services, at (901) 546-4515.

Attachment

Attachment

RECOMMENDATION 1:
Develop a process to retain and review FPS risk assessments and ensure that they are readily available to security personnel. In addition, require an assessment of the FPS's most recent findings as part of any current risk assessment and revalidation processes performed by the IRS.

CORRECTIVE ACTION:
We agree with this recommendation. The Chief, Agency-Wide Shared Services (AWSS) will engage with Federal Protective Service (FPS) to develop and implement a process to obtain current and future FPS Facility Security Assessments (FSA) for Internal Revenue Service (IRS) facilities upon completion. IRS will also revise its current risk assessment process to integrate FPS FSA findings in risk assessments and revalidation processes performed by the IRS.

IMPLEMENTATION DATE:
May 31, 2016

RESPONSIBLE OFFICIAL:
Director, Facilities Management and Security Services (FMSS), Agency-Wide Shared Services

CORRECTIVE ACTION MONITORING PLAN:
FMSS, AWSS, will enter accepted corrective actions into the Joint Audit Management Enterprise System (JAMES). These corrective actions are monitored on a monthly basis until completion.

RECOMMENDATION 2:
Use the *Listing of FPS Planned Risk Assessments* and evaluate whether the IRS can rely on FPS risk assessments of some IRS facilities and eliminate the duplicate IRS risk assessment for those facilities.

CORRECTIVE ACTION:
We agree with this recommendation. The AWSS Chief is currently evaluating whether the IRS can rely on FPS risk assessments at some IRS facilities and eliminate the duplicate FMSS risk assessment for those facilities as appropriate.

IMPLEMENTATION DATE:
May 31, 2016

RESPONSIBLE OFFICIAL:
Director, Facilities Management and Security Services, Agency-Wide Shared Services

CORRECTIVE ACTION MONITORING PLAN:
FMSS, AWSS, will enter accepted corrective actions into JAMES. These corrective actions are monitored on a monthly basis until completion.

RECOMMENDATION 3:
Correct the errors noted in the risk assessment repository and Security Information Management System and ensure that information maintained in those systems is checked regularly for accuracy.

CORRECTIVE ACTION:
We agree with this recommendation. The AWSS Chief recognizes that the errors noted within the report were administrative in nature. Regardless, we will correct the errors and revise the current risk assessment process to include the periodic review of information contained in the risk assessment repository and Security Information Management System (SIMS).

IMPLEMENTATION DATE:
May 31, 2016

RESPONSIBLE OFFICIAL:
Director, Facilities Management and Security Services, Agency-Wide Shared Services

CORRECTIVE ACTION MONITORING PLAN:
FMSS, AWSS, will enter accepted corrective actions into JAMES. These corrective actions are monitored on a monthly basis until completion.