

# TREASURY INSPECTOR GENERAL FOR TAX ADMINISTRATION



## **The Process for Tracking Physical Security Weaknesses Identified in IRS Facilities Does Not Ensure That Vulnerabilities Are Properly Addressed**

September 14, 2022

Report Number: 2022-10-046

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 .

# HIGHLIGHTS: The Process for Tracking Physical Security Weaknesses Identified in IRS Facilities Does Not Ensure That Vulnerabilities Are Properly Addressed

Final Audit Report issued on September 14, 2022

Report Number 2022-10-046

## Why TIGTA Did This Audit

As the Nation's tax collection agency, the IRS is often the target of threats from individuals and organizations looking to do it harm. To safeguard the security and safety of its personnel, facilities, and assets, the IRS develops and implements physical security policies, procedures, and processes to mitigate both current and emerging threats.

This audit was initiated to determine whether the IRS process for implementing countermeasures recommended in facility security risk assessments ensures that 1) identified security vulnerabilities are addressed or 2) risk acceptance is adequately documented when countermeasures are not implemented.

## Impact on Tax Administration

The IRS manages 532 locations throughout the United States. It is important for the IRS to track the status of countermeasures at these locations to ensure that known security vulnerabilities are mitigated. Without effective management and documentation of the countermeasure tracking and approval process for known security vulnerabilities, IRS employees and facilities may be at increased risk if a necessary countermeasure was not implemented.

## What TIGTA Found

The IRS updated security countermeasure procedures in response to a prior TIGTA report; however, the new process did not ensure that minimum physical security countermeasures were tracked and considered. The IRS's process for documenting the tracking and monitoring of recommended countermeasures was not effective because the IRS does not consistently use a centralized system to track physical security countermeasure recommendations, approvals, implementation actions, and associated costs. As a result, TIGTA was unable to determine the status of all current recommended physical security countermeasures in [REDACTED] of the IRS facilities reviewed.



Furthermore, physical security specialists did not consistently and clearly document when a request for risk acceptance was made or have a defined process to reject a recommended countermeasure. Without a process that requires physical security specialists to document their rationale and obtain approval for rejecting a recommended countermeasure, physical security specialists may choose not to implement a countermeasure that is required per Interagency Security Committee standards, thereby increasing risk to IRS personnel and facilities.

## What TIGTA Recommended

TIGTA recommended that the Chief, Facilities Management and Security Services: 1) ensure that countermeasure recommendations, approvals or denials, implementation decisions and actions, risk acceptance decisions, and the associated cost of implementation are adequately tracked and maintained in a central location; 2) update the policies and procedures for any changes related to the tracking of countermeasures identified in a Facility Security Assessment or Facility Security Assessment Addendum and provide formalized training to the physical security specialists; 3) ensure that all recommended countermeasures from the most recent risk assessment are tracked until a new risk assessment is completed using the new countermeasure tracking mechanism; and 4) ensure that the countermeasure tracking mechanism requires physical security specialists to document the reason and obtain approval for rejecting a recommended countermeasure. IRS management agreed with our recommendations and plans to implement a Countermeasure Tool to track and maintain countermeasures in a central location. Management also plans to update policies and procedures and to provide formalized training.



TREASURY INSPECTOR GENERAL  
FOR TAX ADMINISTRATION

## U.S. DEPARTMENT OF THE TREASURY

WASHINGTON, D.C. 20024

September 14, 2022

### MEMORANDUM FOR: COMMISSIONER OF INTERNAL REVENUE

**FROM:**

*Heather Hill*

Heather M. Hill  
Deputy Inspector General for Audit

**SUBJECT:**

Final Audit Report – The Process for Tracking Physical Security  
Weaknesses Identified in IRS Facilities Does Not Ensure That  
Vulnerabilities Are Properly Addressed (Audit # 202210009)

This report presents the results of our review to determine whether the Internal Revenue Service (IRS) process for implementing countermeasures recommended in facility security risk assessments ensures that 1) identified security vulnerabilities are addressed or 2) risk acceptance is adequately documented when countermeasures are not implemented. This review is part of our Fiscal Year 2022 Annual Audit Plan and addresses the major management and performance challenge of *Enhancing Security of Taxpayer Data and Protection of IRS Resources*.

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

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 Bryce Kisler, Acting Assistant Inspector General for Audit (Management Services and Exempt Organizations).

## Table of Contents

<a href="#">Background</a> .....	Page 1
----------------------------------	--------

<a href="#">Results of Review</a> .....	Page 6
---	--------

<a href="#">Current Processes Do Not Ensure That Recommended Minimum Security Countermeasures Are Tracked and Considered</a> .....	Page 6
--	--------

<a href="#">Recommendations 1 Through 4:</a> .....	Page 10
--	---------

## Appendices

<a href="#">Appendix I – Detailed Objective, Scope, and Methodology</a> .....	Page 11
---	---------

<a href="#">Appendix II – Outcome Measures</a> .....	Page 13
--	---------

<a href="#">Appendix III – Management’s Response to the Draft Report</a> .....	Page 15
--	---------

<a href="#">Appendix IV – Abbreviations</a> .....	Page 18
---	---------

## **Background**

As the Nation's tax collection agency, the Internal Revenue Service (IRS) is often the target of threats from individuals and organizations looking to do it harm. To safeguard the security and safety of its personnel, facilities, and assets, the IRS develops and implements physical security policies, procedures, and processes to mitigate both current and emerging threats.

The IRS's Facilities Management and Security Services (FMSS) function is a support service organization with the mission of delivering a safe, secure, and optimal work environment that promotes effective tax administration. With a budget of almost \$1 billion, the FMSS function manages 532 locations throughout the United States as of June 2022.<sup>1</sup>

### **Risk assessment process**

As part of the security services contracted by Federal tenants, the Federal Protective Service (FPS) is responsible for performing a Facility Security Assessment (FSA) of all Federally owned or leased property. The FSA is the FPS process of evaluating and documenting credible threats, identifying vulnerabilities, and assessing consequences for a specific facility. FSA results are maintained in the FPS Modified Infrastructure Survey Tool database.<sup>2</sup> The IRS uses the FSA report as the foundation for its Facility Security Assessment Addendum (FSAA).<sup>3</sup> The FSAA includes requirements specific to the Department of the Treasury and the IRS, related findings, and cost estimates for any needed security enhancements to the facilities being assessed. Along with the FSA, the FSAA serves as the official IRS risk assessment for each IRS facility.

The FPS considers the characteristics of each facility and the Federal occupant(s) who inhabit the facility when the Facility Security Level (FSL) is determined.<sup>4</sup> The five factors quantified to determine the FSL are mission criticality, symbolism, facility population, facility size, and threat to tenant agencies. The FSL ranges from Level I (lowest risk) to Level V (highest risk). See Figure 1 for an overview of the characteristics considered when determining the FSL. As directed in the Interagency Security Committee (ISC)<sup>5</sup> standards, an FSA will be conducted at least once every three years for FSL III, IV, and V facilities and at least every five years for FSL I and II facilities.<sup>6</sup>

---

<sup>1</sup> This total includes facilities and parking garages.

<sup>2</sup> The Modified Infrastructure Survey Tool is a proprietary FSA tool and document repository. It includes FSA information that the FMSS function is able to access.

<sup>3</sup> Prior to October 1, 2019, the IRS used the physical security risk assessment process, which was redundant to the FPS process. It was made obsolete in favor of utilizing the FSA process.







<sup>4</sup> The FSL is a categorization, based on the analysis of several security-related facility factors, that serves as the basis for the implementation of physical security measures specified in the Interagency Security Committee standards.

<sup>5</sup> The ISC was established in October 1995. The ISC is chaired by the Department of Homeland Security, consists of 64 departments and agencies, and has a mission to develop security policies, standards, and recommendations for nonmilitary Federal facilities in the United States.

<sup>6</sup> *The Risk Management Process: An Interagency Security Committee Standard* (2021 Edition).

## The Process for Tracking Physical Security Weaknesses Identified in IRS Facilities Does Not Ensure That Vulnerabilities Are Properly Addressed

**Figure 1: Examples of Criteria Characteristics for Determination of an FSL<sup>7</sup>**

 Facility Security Level	I	II	III	IV	V
 Mission Criticality	Administrative activities at a local level	State regulatory operations	Judicial processes	Houses specialized equipment necessary to monitor financial transactions	Merits a degree of protection above that specified for an FSL IV facility
 Symbolism	Not identifiable as a Government facility	Single Federal facility in a rural area	Agency/bureau headquarters	Popular destination for tourists	
 Facility Population	100 or less people	101 to 250 people	251 to 750 people	Over 750 people or facility includes a child care center	
 Facility Size	Up to 10,000 sq. ft.	10,001 to 100,000 sq. ft.	100,001 to 250,000 sq. ft.	More than 250,000 sq. ft.	
 Threat to Tenant Agency	Very low-crime area	Low-crime area	Moderate-crime area	High-crime area	

Source: *The Risk Management Process: An Interagency Security Committee Standard (2021 Edition)*.

### ISC standards and minimum countermeasures

Executive Order 12977 established the ISC to enhance the quality and effectiveness of physical security at Federal facilities.<sup>8</sup> The ISC standards apply to all nonmilitary Federal facilities in the United States—whether Government owned, leased, or managed; to be constructed or modernized; or to be purchased. The baseline level of protection as defined by the ISC is the degree of security provided by the set of countermeasures for each FSL that must be implemented, unless a deviation is justified by a risk assessment.<sup>9</sup> In compliance with ISC standards for nonmilitary Federal facilities, the FPS has established minimum security standards and requirements for the protection of IRS facilities, personnel, and information. These standards are based on possible threats and identified countermeasures that could minimize the impact of an occurrence. Per the Internal Revenue Manual, ISC standards will be applied as a minimum security standard, but IRS protection requirements may exceed these standards.<sup>10</sup> As such, the IRS has established security guidelines for the reasonable protection of employees, tax information, infrastructure, property, and facilities against disclosure, loss, damage, or destruction without unnecessarily restricting or interfering with its operations.

<sup>7</sup> All five of the factors are considered when determining the overall FSL, and the criteria characteristic examples provided are not an absolute requirement to obtain the identified FSL.

<sup>8</sup> Exec. Order No. 12977, *Interagency Security Committee* (Oct. 1995).

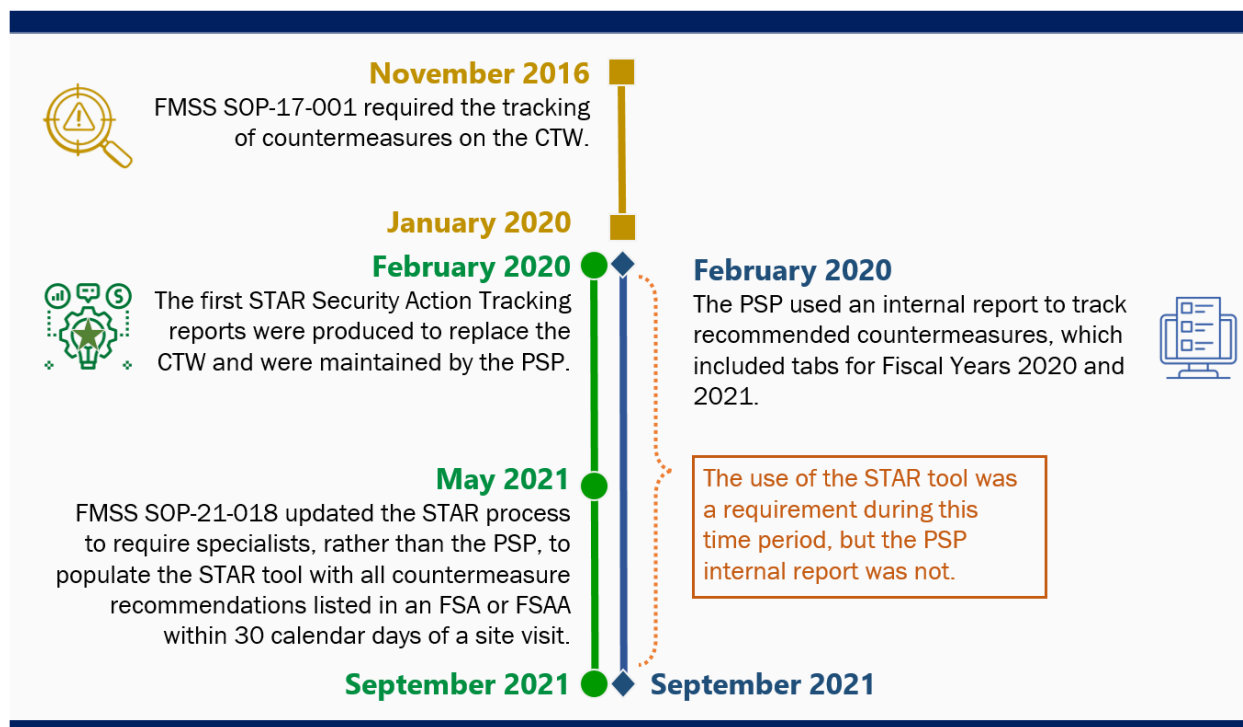
<sup>9</sup> A countermeasure is an action, measure, or device intended to reduce an identified risk, threat, or danger. Examples of countermeasures include the use of gates, entry controls, closed circuit video, and visitor x-ray screening.

<sup>10</sup> Internal Revenue Manual 10.2.11, *Basic Physical Security Concepts* (September 4, 2019).

## Countermeasure tracking and implementation

In response to a recommendation from a prior Treasury Inspector General for Tax Administration (TIGTA) audit report, the FMSS function implemented a Countermeasure Tracking Worksheet (CTW) in November 2016 to track countermeasure recommendations, approvals or denials, and implementation decisions and actions as well as the associated costs of implementation for all countermeasures identified in a risk assessment.<sup>11</sup> Physical Security personnel indicated that the CTW was hard to navigate, and since the Space, Time, and Resources (STAR) tool included a method to track funding, the FMSS function decided to use the STAR tool to track and update countermeasures as well.<sup>12</sup> In February 2020, the FMSS function produced the first STAR Security Action Tracking report to replace the CTW. At that time, Physical Security Program (PSP) personnel added the CTW information to the STAR tool.<sup>13</sup> During the conversion to the STAR tool, PSP personnel also maintained their own internal report to track countermeasures. Figure 2 describes the changes to the countermeasure tracking process.

**Figure 2: Countermeasure Tracking Process Changes**



Source: FMSS Standard Operating Procedure (SOP)-17-001, Physical Security Risk Assessment Program (Nov. 2016); FMSS SOP-19-022-1, FMSS Facility Security Risk Assessment Program (Feb. 2021); FMSS SOP-21-018, FMSS Facility Security Assessment Program (May 2021); and discussions with IRS personnel.

In a May 2021 SOP, the responsibility to maintain the STAR tool shifted to the physical security specialists (hereafter referred to as specialist) and established that, once an FSA or FSAA is

<sup>11</sup> TIGTA, Report No. 2016-10-029, *The Process for Addressing Physical Security Vulnerabilities at Internal Revenue Service Facilities Is Ineffective* (Mar. 2016).

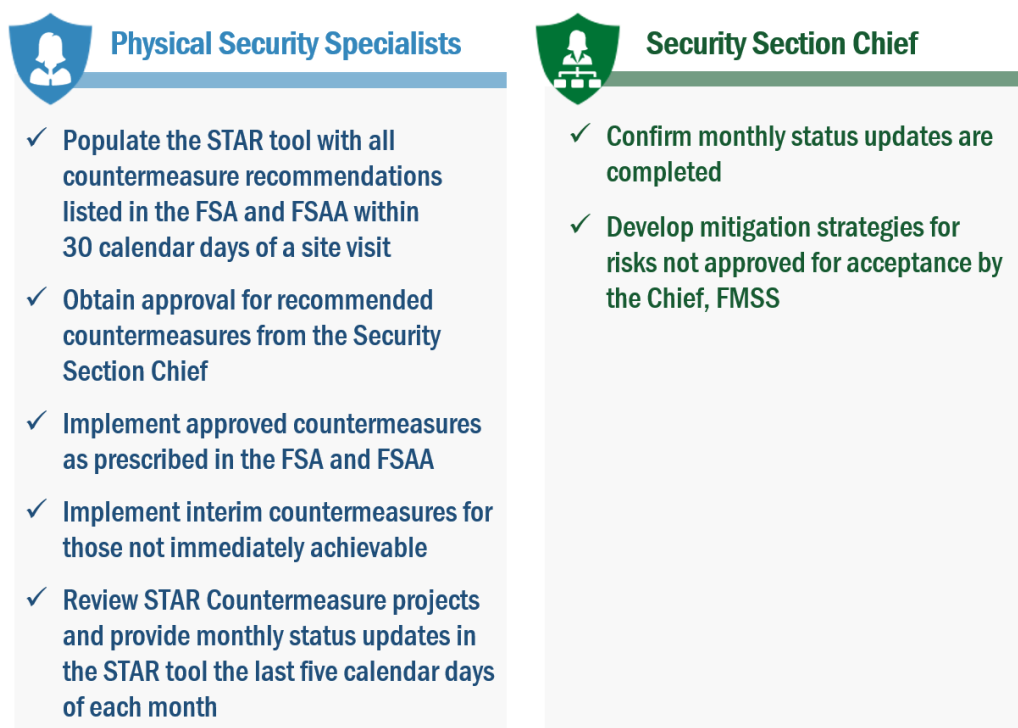
<sup>12</sup> The STAR tool is a project estimating application built to assist FMSS personnel with estimating and tracking projects, including security projects.

<sup>13</sup> The PSP is responsible for IRS physical security programs protecting IRS personnel, facilities, and assets.



complete, the specialist must populate the STAR tool with all countermeasure recommendations listed in the FSA and FSAA within 30 calendar days of a site visit.<sup>14</sup> The specialist is also responsible for obtaining approval for recommended countermeasures from the Security Section Chief and implementing approved countermeasures as prescribed in the FSA and FSAA. For countermeasures that are not immediately achievable, the specialist is required to implement interim countermeasures. The specialist is responsible for reviewing STAR countermeasure projects and providing monthly status updates in the STAR tool the last five calendar days of each month. The Security Section Chief confirms these monthly status updates are completed. Figure 3 describes the key responsibilities related to the tracking of countermeasures.

**Figure 3: Key Countermeasure Tracking Responsibilities**



Source: FMSS SOP-21-018.

### **Risk acceptance when countermeasures implementation is not achievable**

The IRS has formalized the methodology that the specialists must follow while determining and identifying physical security risk acceptance options when the desired level of protection is not achievable, a suggested countermeasure is not used, or a lower-level countermeasure is selected. When a specialist requests risk acceptance, they must complete a Form 14675, *Decision Making Framework Risk Acceptance Form and Tool (RAFT)*. Figure 4 describes the review process of a RAFT. The Security Section Chief is responsible for developing mitigation strategies for risks not approved for acceptance. The Chief, FMSS, is the only approving official for physical security risk acceptance. According to FMSS management, approved RAFTs are reviewed within FMSS and reported to the Office of the Chief Risk Officer during the quarterly data calls.

---

<sup>14</sup> FMSS SOP-21-018.



## The Process for Tracking Physical Security Weaknesses Identified in IRS Facilities Does Not Ensure That Vulnerabilities Are Properly Addressed

Figure 4: Risk Acceptance Review Process



Source: FMSS SOP-21-018.

In the prior March 2016 audit report, TIGTA found that the process for implementing countermeasure improvements did not ensure that known vulnerabilities were addressed, placing IRS personnel, facilities, and taxpayer information at increased risk. The process for implementing recommendations was not effective because the IRS did not track which countermeasures were recommended, approved, or implemented as well as the estimated and actual cost of implementation. The prior audit found [REDACTED] recommended countermeasures that were missing from approval documents and were neither approved nor denied. In addition, the IRS did not document the justification for not implementing approved countermeasures, and the IRS did not implement interim measures when the recommended countermeasures were not immediately achievable.

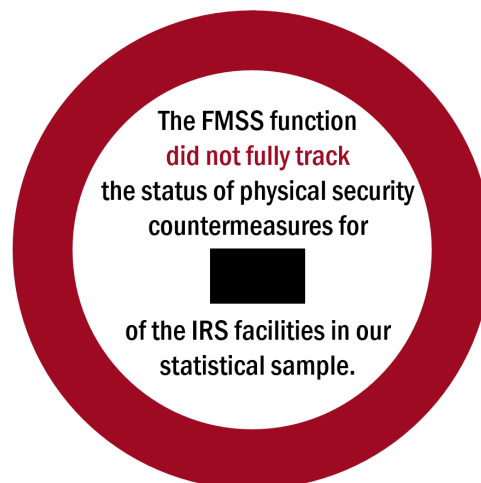
TIGTA recommended that the IRS enhance its countermeasure implementation process by developing and implementing a centralized system to track recommendations, approvals or denials, implementation decisions and actions, and timeliness of actions as well as the associated costs. In addition, TIGTA recommended that the IRS update the SOP to reflect the changes in the organization and implement or document the reason for accepting the risk mitigated by the recommended and approved countermeasures that were not implemented.

## Results of Review

### Current Processes Do Not Ensure That Recommended Minimum Security Countermeasures Are Tracked and Considered

In response to the 2016 TIGTA audit, the IRS implemented a process to track the status of physical security countermeasures recommended by the FPS and to address security vulnerabilities. However, the improvements did not ensure that the countermeasures were tracked and considered for IRS facilities.<sup>15</sup> The IRS's processes do not provide for consistent tracking of physical security countermeasure recommendations, approvals, implementation actions, and associated costs in a centralized system. Because of these limitations, TIGTA was unable to determine the status of all current physical security countermeasures recommended in [REDACTED] of the IRS facilities reviewed.<sup>16</sup> Moreover, we could not determine whether the FMSS function intended to implement all countermeasures based on the documentation provided. The Government

Accountability Office's *Standards for Internal Control in the Federal Government* states that management should use quality information to make informed decisions to address risks.<sup>17</sup> Without effective management and documentation of the countermeasure tracking and approval process for known security vulnerabilities, IRS employees and facilities may be at increased risk if a necessary countermeasures was not implemented.



### The IRS did not consistently track the status of recommended physical security countermeasures

The FMSS function did not fully track the status of physical security countermeasures that were recommended in risk assessments between November 2016 and September 2021 for [REDACTED] of the 54 facilities in our statistical sample as required.<sup>18</sup> In addition, there was no documentation to support that the recommended countermeasures were considered for [REDACTED] of the 54 facilities tested.<sup>19</sup> For example, the FMSS function did not provide documentation to support that it considered minimum security countermeasures such as [REDACTED]

---

<sup>15</sup> TIGTA determined that a countermeasure had been considered if the IRS documented the countermeasure status, approval, or denial.

<sup>16</sup> For each facility, at least one recommended countermeasure was not tracked in accordance with FMSS policy.

<sup>17</sup> Government Accountability Office, GAO-14-704G, *Standards for Internal Control in the Federal Government* (Sept. 2014).

<sup>18</sup> We determined that [REDACTED] of the 380 physical security countermeasures recommended for the IRS facilities in our sample were not tracked.

<sup>19</sup> We determined that [REDACTED] of the 380 physical security countermeasures recommended for the IRS facilities in our sample were not considered.

Based on our results, we estimate that countermeasures for [REDACTED] of the 179 FSL III, IV, and V facilities were not properly tracked,<sup>20</sup> and countermeasures for [REDACTED] facilities were not considered.<sup>21</sup>

### **Countermeasure tracking procedures were not always followed**

The FMSS function indicated that it began using the CTW in November 2016 to track recommended countermeasures identified in risk assessments. However, FMSS personnel could not locate an official copy of the CTW for Fiscal Year (FY) 2017 and provided incomplete copies of CTWs for FYs 2018 and 2019.<sup>22</sup> As a result, it is unclear whether the countermeasures recommended in the FSAs and FSAs during this time frame were implemented or remain outstanding.

In February 2020, the FMSS function replaced the CTW with the STAR tool to track recommended countermeasures. In May 2021, updated guidance required that the specialists include all countermeasures listed in an FSA or FSAA in the STAR tool within 30 calendar days of a site visit.<sup>23</sup> The PSP also used an internal tracking report to track countermeasures. The PSP internal tracking report included many of the countermeasures identified in FYs 2020 and 2021 FSAs and FSAs, but those countermeasures were not included in the STAR tool as required. Due to the reliance on the PSP internal tracking report, fewer countermeasures from FYs 2020 and 2021 were properly tracked and updated in the STAR tool. Furthermore, the FMSS function was unable to provide support for countermeasure considerations in the form of Facility Security Committee votes, meeting minutes, or discussion e-mails.<sup>24</sup> This information may have shown that countermeasures were considered by progressing through the Facility Security Committee approval and denial process.

### **Specialists had difficulty complying with provided FMSS guidance**

We interviewed various specialists in the field to discuss their understanding and use of the STAR tool. During our interviews, the specialists identified several issues they have had with the STAR tool and provided recommendations to make the application more user friendly. Figure 5 provides a summary of these observations.

---

<sup>20</sup> Our sample was selected using a 95 percent confidence interval, a 5 percent error rate, and a  $\pm 5$  percent precision factor. When projecting the results of our statistical sample, we are 95 percent confident that the actual total amount is between [REDACTED].

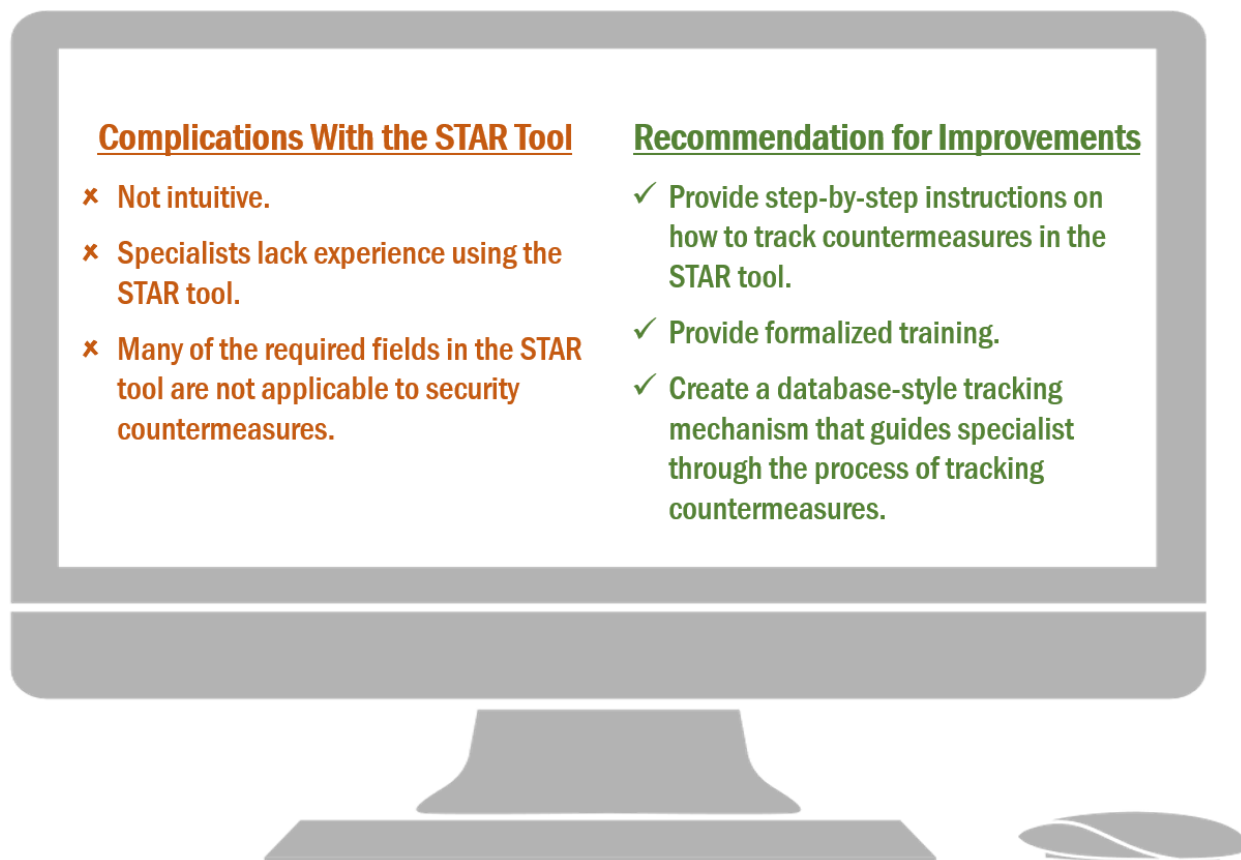
<sup>21</sup> Our sample was selected using a 95 percent confidence interval, a 5 percent error rate, and a  $\pm 5$  percent precision factor. When projecting the countermeasures tracking results of our statistical sample, we are 95 percent confident that the actual total amount is between [REDACTED].

<sup>22</sup> A fiscal year is any yearly accounting period, regardless of its relationship to a calendar year. The Federal Government's fiscal year begins on October 1 and ends on September 30. The FY 2018 CTW was dated May 2018, and the FY 2019 CTW was dated August 2019.

<sup>23</sup> FMSS SOP-21-018.

<sup>24</sup> The Facility Security Committee is responsible for addressing facility-specific security issues and approving the implementation of security measures and practices in multitenant facilities. The Facility Security Committee consists of representatives of all Federal tenants in the facility, the security organization, and the owning or leasing department or agency.

Figure 5: Summary of Specialist Observations Concerning the STAR Tool



<u>Complications With the STAR Tool</u>	<u>Recommendation for Improvements</u>
✗ Not intuitive.	✓ Provide step-by-step instructions on how to track countermeasures in the STAR tool.
✗ Specialists lack experience using the STAR tool.	✓ Provide formalized training.
✗ Many of the required fields in the STAR tool are not applicable to security countermeasures.	✓ Create a database-style tracking mechanism that guides specialist through the process of tracking countermeasures.

Source: TIGTA's analysis of various interviews with the specialists.

Based on discussions with the specialists, a lack of detailed procedures and formalized training has made the countermeasure tracking process confusing and convoluted for users. Furthermore, the specialists have received conflicting guidance on tracking countermeasures specifically resulting from FSA recommendations. The PSP internal tracking report included 150 countermeasures from various facilities with instructions from the [REDACTED] that there was no need to go through the STAR tool as each tenant agency pays their portion of the countermeasure implementation cost to the FPS. The disconnect between written policies and instructions provided during actual countermeasure tracking has increased confusion and undermined current guidance.

FMSS management's ability to oversee the implementation of recommended physical security countermeasures is hindered because not all countermeasures identified in an FSA or FSAA are tracked. In addition, poor record keeping has limited the FMSS function's ability to provide the status of countermeasures recommended between FYs 2017 and 2019. It is important for the IRS to track the status of countermeasures to ensure that known security vulnerabilities are mitigated. However, the FMSS function is unable to accurately determine where countermeasures were tracked and cannot ensure that those countermeasures were addressed. Due to incomplete tracking, the FMSS function does not have a method to determine the age, estimated costs, or number of outstanding countermeasures. These issues could affect the FMSS function's ability to prioritize the implementation of countermeasures and could cause a countermeasure to go unimplemented until a new risk assessment is completed.

Unimplemented recommended countermeasures may increase risks to IRS personnel, facilities, taxpayers, and taxpayer information.

In response to issues identified during the course of our audit by TIGTA auditors and FMSS personnel, the FMSS function began developing a new countermeasure tracking tool that will be used to track and manage countermeasure recommendations from FSAs and FSAsAs. As of July 2022, the FMSS function is in the late stages of development, with an anticipated implementation date of October 2022.

### **Countermeasure documentation did not always indicate when specialists requested risk acceptance**

Per IRS policy, when risk acceptance is the logical risk management option for findings and vulnerabilities, a RAFT must be completed.<sup>25</sup> This form outlines the process for documenting the risk and ultimately requesting risk acceptance approval. The IRS provided documentation showing that risk was accepted using a RAFT for three countermeasures between January 2017 and October 2021. The IRS documented agencywide risk acceptance [REDACTED] at 121 facilities, agencywide risk acceptance for the [REDACTED] at 56 facilities, and risk acceptance related to the [REDACTED] When the IRS completed a RAFT, the documentation was clear, and appropriate levels of review were completed.

However, we identified two countermeasures related to [REDACTED] in our statistical sample of 54 IRS facilities for which the IRS appeared to accept the risk, but the specialist did not document risk acceptance in accordance with IRS policy.<sup>26</sup> In both instances, the status in the STAR tool indicated that implementing the recommended countermeasure would not be cost effective, but a RAFT was not completed to document the risk acceptance. FMSS management clarified that risk had not been accepted for these countermeasures and that a project was in process for each. However, the FMSS function was unable to provide any documentation to support that the projects were ongoing. In addition, the status in the STAR tool was not updated to indicate that a project exists; therefore, the specialist's decision was not properly documented. As of June 2022, the risk was unmitigated, and the [REDACTED]

27

We also identified six instances at three facilities in which the IRS chose not to implement a recommended countermeasure that was identified in an FSA. FMSS management indicated that a RAFT was not required in these instances because the risk assessment included a recommended security enhancement rather than a required countermeasure. FMSS policy documents do not include a distinction between a requirement or a recommendation, nor do they outline the process to reject a recommendation made in an FSA.

Without a process that requires specialists to document their rationale and obtain approval for rejecting a recommended countermeasure, specialists may choose not to implement a

---

<sup>25</sup> FMSS SOP-21-018.

<sup>26</sup> Both countermeasures were identified in a May 2020 FSA.

<sup>27</sup> After we presented this concern to the FMSS function in January 2022, they updated the status of this project in the STAR tool. As of June 2022, they have received a cost estimate to complete the project.

countermeasure that is required per the ISC standards, thereby increasing risk to IRS personnel and facilities.

The Chief, FMSS, should:

**Recommendation 1:** Ensure that countermeasure recommendations, approvals or denials, implementation decisions and actions, risk acceptance decisions, and the associated cost of countermeasure implementation are adequately tracked and maintained in a central location.

**Management's Response:** The IRS agreed with this recommendation and will ensure that countermeasure recommendations, approvals or denials, implementation decisions and actions, risk acceptance decisions, and the associated cost of countermeasure implementation are adequately tracked and maintained in a central location.

**Recommendation 2:** Update the policies and procedures for any changes related to the tracking of countermeasures identified in an FSA or FSAA and provide formalized training to the physical security specialists.

**Management's Response:** The IRS agreed with this recommendation and will update the policies and procedures for any changes related to the tracking of countermeasures identified in an FSA or FSAA and provide formalized training to the physical security specialists.

**Recommendation 3:** Ensure that all recommended countermeasures identified in the most recent risk assessment (*i.e.*, FSA or FSAA) for each facility are tracked until a new risk assessment is completed using the new countermeasure tracking mechanism.

**Management's Response:** The IRS agreed with this recommendation and will validate that all recommended countermeasures identified in the most recent risk assessment (*i.e.*, FSA or FSAA) for each facility are tracked using the new countermeasure tracking mechanism until a new risk assessment is completed.

**Recommendation 4:** Ensure that the countermeasure tracking mechanism requires physical security specialists to document the reason and obtain approval for rejecting a recommended countermeasure.

**Management's Response:** The IRS agreed with this recommendation and will ensure that the countermeasure tracking mechanism requires physical security specialists to document the reason and obtain approval for rejecting a recommended countermeasure.



## **Appendix I**

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

The overall objective of this audit was to determine whether the IRS process for implementing countermeasures recommended in facility security risk assessments ensures that 1) identified security vulnerabilities are addressed or 2) risk acceptance is adequately documented when countermeasures are not implemented. To accomplish our objective, we:

- Determined whether the IRS updated countermeasure implementation policies and procedures since December 2016. We reviewed the Internal Revenue Manual and SOPs as well as desk procedures and noted several updates related to countermeasure implementation.
- Determined whether documentation supported the decision to accept risk for unimplemented countermeasures.
- Evaluated the process by which the FMSS function considered, and approved or denied, countermeasures recommended during the risk assessment process by reviewing a statistical sample of 54 of 179 IRS facilities.<sup>1</sup> TIGTA's contract statistician assisted with developing the sampling plan and projections.
- Interviewed specialists to obtain an understanding of how they utilize guidance and the STAR tool to implement recommended countermeasures, how they prioritize countermeasures, and any barriers to implementation.

### **Performance of This Review**

TIGTA performed this review with information obtained from the FMSS function offices located throughout the United States during the period September 2021 through June 2022. TIGTA 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.

Major contributors to the report were Bryce Kisler, Acting Assistant Inspector General for Audit (Management Services and Exempt Organizations); Glen Rhoades, Director; Melinda Dowdy, Audit Manager; Zachary Orrico, Lead Auditor; and Euneke Coutts, Auditor.

### **Validity and Reliability of Data From Computer-Based Systems**

We performed tests to assess the reliability of data from the FPS Modified Infrastructure Survey Tool database, the PSP internal tracking report, and the STAR tool. We evaluated the data by: 1) ensuring that the Modified Infrastructure Survey Tool data included entries for the building number, FSL, and last FSA date for all buildings; 2) interviewing agency officials knowledgeable

---

<sup>1</sup> Our sample size was determined using a 95 percent confidence interval, a 5 percent error rate, and a  $\pm 5$  percent precision factor. A statistical sample was used in order to support a statistically valid projection to the population of facilities if exceptions were found during the review.



about the STAR tool; 3) performing electronic testing of required data fields; and 4) comparing completed risk assessments to the Security Action Tracking Report and the PSP internal tracking report. We determined that the data were sufficiently reliable for purposes of this report; however, the STAR tool data do not contain the necessary information for TIGTA to determine the number, age, and cost of all outstanding countermeasures.

### **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 objective: FMSS policies and procedures to track physical security countermeasures identified in an FSA or FSAA as well as to adequately document risk acceptance. Our audit evaluated the controls by reviewing risk assessments for a statistical sample of IRS facilities and determining whether identified physical security countermeasures were tracked in a centralized tracking mechanism or if risk was accepted. In addition, we interviewed FMSS personnel responsible for the design of the tracking mechanism as well as the specialists who use the tracking mechanism.

## Appendix II

### Outcome Measures

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

#### Type and Value of Outcome Measure:

Reliability of Information – Potential; [REDACTED] facilities had recommended countermeasures that were included in risk assessments between FYs 2017 and 2021 but were not tracked using a centralized system (see Recommendation 1).

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

We reviewed risk assessments for a statistical sample of 54 IRS facilities and found that recommended countermeasures were not tracked for [REDACTED] of the facilities.<sup>1</sup> Our exceptions resulted in a higher than expected error rate. We consulted with TIGTA's contract statistician to project the error rate to the overall population. Based on a 95 percent confidence interval, we estimate that risk assessments for [REDACTED] of the 179 facilities contain recommended countermeasures that were not properly tracked.<sup>2</sup> See Figure 1 for additional details.

**Figure 1: Calculation of Estimated Number of Facilities With Untracked Countermeasures**

Strata	Sample Size	Total Population of Facilities	[REDACTED]	[REDACTED]
FSL III	21	70	[REDACTED]	[REDACTED]
FSL IV	32	108	[REDACTED]	[REDACTED]
FSL V	1	1	[REDACTED]	[REDACTED]
Totals	54	179	[REDACTED]	[REDACTED]

Source: Statistician projections provided based on audit results.

#### Type and Value of Outcome Measure:

Protection of Resources – Potential; [REDACTED] facilities had recommended countermeasures that were included in risk assessments between FYs 2017 and 2021 but were not properly considered (see Recommendation 1).

<sup>1</sup> The 54 facilities include 21 FSL III, 32 FSL IV, and one FSL V.

<sup>2</sup> Our sample was selected using a 95 percent confidence interval, a 5 percent error rate, and a  $\pm 5$  percent precision factor. When projecting the countermeasures tracking results of our statistical sample, we are 95 percent confident that the actual total amount is between [REDACTED].

## Methodology Used to Measure the Reported Benefit:

We reviewed risk assessments for a statistical sample of 54 IRS facilities and found that recommended countermeasures were not considered for [REDACTED] of the facilities.<sup>3</sup> Our exceptions resulted in a higher than expected error rate. We consulted with TIGTA's contract statistician to project the error rate to the overall population. Based on a 95 percent confidence interval, we estimate that risk assessments for [REDACTED] of the 179 facilities that include countermeasures were not properly considered.<sup>4</sup> These issues could affect the FMSS function's ability to prioritize the implementation of countermeasures and could cause a countermeasure to go unimplemented until a new risk assessment is completed. Unimplemented recommended countermeasures may increase risks to IRS personnel, facilities, taxpayers, and taxpayer information. See Figure 2 for additional details.

**Figure 2: Calculation of Estimated Number of  
Facilities With Improperly Considered Countermeasures**

Strata	Sample Size	Total Population of Facilities	[REDACTED]	
			[REDACTED]	[REDACTED]
FSL III	21	70	[REDACTED]	[REDACTED]
FSL IV	32	108	[REDACTED]	[REDACTED]
FSL V	1	1	[REDACTED]	[REDACTED]
<b>Totals</b>	<b>54</b>	<b>179</b>	<b>[REDACTED]</b>	<b>[REDACTED]</b>

Source: Statistician projections provided based on audit results.

<sup>3</sup> The 54 facilities include 21 FSL III, 32 FSL IV, and one FSL V.

<sup>4</sup> Our sample was selected using a 95 percent confidence interval, a 5 percent error rate, and a  $\pm 5$  percent precision factor. When projecting the countermeasures consideration results of our statistical sample, we are 95 percent confident the actual total is between [REDACTED]

## Appendix III

### Management's Response to the Draft Report



CHIEF  
FACILITIES MANAGEMENT AND  
SECURITY SERVICES

DEPARTMENT OF THE TREASURY  
INTERNAL REVENUE SERVICE  
WASHINGTON, DC 20224

August 15, 2022

MEMORANDUM FOR: HEATHER M. HILL  
DEPUTY INSPECTOR GENERAL FOR AUDIT

FROM: Richard L. Rodriguez  
Richard L. Rodriguez  
Chief, Facilities Management & Security Services

SUBJECT: Draft Audit Report – The Process for Tracking Physical Security Weaknesses Identified in IRS Facilities Does Not Ensure That Vulnerabilities Are Properly Addressed (Audit # 202210009)

Digitally signed by Richard L. Rodriguez  
Date: 2022.08.15 09:42:52 -04'00'

Thank you for the opportunity to review and comment on the draft audit report. We appreciate that your report acknowledged that the IRS updated security countermeasure procedures and formalized the methodology that the physical security specialists must follow while determining and identifying physical security risk acceptance options. We are committed to the security of our offices and the employees and taxpayer information they contain. Your recommendations will assist us in our efforts to ensure the protection of resources and increased reliability of information for our facilities.

We agree with your four recommendations. We have developed corrective actions to remediate the report findings and have already begun making progress on multiple recommendations included in the report. Facilities Management & Security Services developed the Countermeasure Tool that will track and maintain all countermeasures in a central location. We have completed testing and are currently in the final stages of implementing this tool. Updates to our policies and procedures are drafted and we are in the process of planning the formalized training for our physical security specialists. We expect to begin the new process the first quarter of Fiscal Year 2023.

Attached is our corrective action plan describing how we plan to address your recommendations.

We appreciate the continued support and assistance provided by your office. If you have any questions, please contact me at 202-317-4480, or a member of your staff may contact Brian Soloman, Associate Director, Security, Facilities Management and Security Services at 231-932-2056.

Attachment

**The Process for Tracking Physical Security Weaknesses Identified in  
IRS Facilities Does Not Ensure That Vulnerabilities Are Properly Addressed**

---

**Attachment**

**RECOMMENDATION #1:**

The Chief, FMSS, should ensure that countermeasure recommendations, approvals or denials, implementation decisions and actions, risk acceptance decisions, and the associated cost of countermeasure implementation are adequately tracked and maintained in a central location.

**CORRECTIVE ACTION #1:**

We agree with this recommendation. By October 15, 2023, FMSS will ensure that countermeasure recommendations, approvals or denials, implementation decisions and actions, risk acceptance decisions, and the associated cost of countermeasure implementation are adequately tracked and maintained in a central location.

**IMPLEMENTATION DATE:**

October 15, 2023

**RESPONSIBLE OFFICIAL:**

Chief, Facilities Management and Security Services

**CORRECTIVE ACTION MONITORING PLAN:**

Corrective actions are entered into the Joint Audit Management Enterprise System (JAMES) and are monitored monthly through completion.

**RECOMMENDATION #2:**

The Chief, FMSS, should update the policies and procedures for any changes related to the tracking of countermeasures identified in a Facility Security Assessment (FSA) or Facility Security Assessment Addendum (FSAA) and provide formalized training to the physical security specialists.

**CORRECTIVE ACTION #2:**

We agree with this recommendation. By November 15, 2022, FMSS will update the policies and procedures for any changes related to the tracking of countermeasures identified in an FSA or FSAA and provide formalized training to the physical security specialists.

**IMPLEMENTATION DATE:**

November 15, 2022

**RESPONSIBLE OFFICIAL:**

Chief, Facilities Management and Security Services

**CORRECTIVE ACTION MONITORING PLAN:**

Corrective actions are entered into the Joint Audit Management Enterprise System (JAMES) and are monitored monthly through completion.

**RECOMMENDATION #3:**

The Chief, FMSS, should ensure that all recommended countermeasures identified in the most recent risk assessment (*i.e.*, FSA or FSAA) for each facility are tracked until a new risk assessment is completed using the new countermeasure tracking mechanism.

**CORRECTIVE ACTION #3:**

We agree with this recommendation. By October 15, 2023, FMSS will validate that all recommended countermeasures identified in the most recent risk assessment (*i.e.*, FSA or FSAA) for each facility are tracked using the new countermeasure tracking mechanism until a new risk assessment is completed.

**IMPLEMENTATION DATE:**

October 15, 2023

**RESPONSIBLE OFFICIAL:**

Chief, Facilities Management and Security Services

**CORRECTIVE ACTION MONITORING PLAN:**

Corrective actions are entered into the Joint Audit Management Enterprise System (JAMES) and are monitored monthly through completion.

**RECOMMENDATION #4:**

The Chief, FMSS, should ensure that the countermeasure tracking mechanism requires physical security specialists to document the reason and obtain approval for rejecting a recommended countermeasure.

**CORRECTIVE ACTION #4:**

We agree with this recommendation. By November 15, 2022, FMSS will ensure that the countermeasure tracking mechanism requires physical security specialists to document the reason and obtain approval for rejecting a recommended countermeasure.

**IMPLEMENTATION DATE:**

November 15, 2022

**RESPONSIBLE OFFICIAL:**

Chief, Facilities Management and Security Services

**CORRECTIVE ACTION MONITORING PLAN:**

Corrective actions are entered into the Joint Audit Management Enterprise System (JAMES) and are monitored monthly through completion.

## **Appendix IV**

### **Abbreviations**

CTW	Countermeasure Tracking Worksheet
FMSS	Facilities Management and Security Services
FPS	Federal Protective Service
FSA	Facility Security Assessment
FSAA	Facility Security Assessment Addendum
FSL	Facility Security Level
FY	Fiscal Year
IRS	Internal Revenue Service
ISC	Interagency Security Committee
PSP	Physical Security Program
RAFT	Risk Acceptance Form and Tool
SOP	Standard Operating Procedure
STAR	Space, Time, and Resources
TIGTA	Treasury Inspector General for Tax Administration





**To report fraud, waste, or abuse,  
call our toll-free hotline at:**

(800) 366-4484

**By Web:**

[www.treasury.gov/tigta/](http://www.treasury.gov/tigta/)

**Or Write:**

Treasury Inspector General for Tax Administration  
P.O. Box 589  
Ben Franklin Station  
Washington, D.C. 20044-0589

Information you provide is confidential, and you may remain anonymous.