Improvements**********8********
**********8**********

September 21, 2017

Reference Number: 2017-10-056

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:
8 = Law Enforcement Information Related to the Physical Safety of an Individual

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

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

1-800-366-4484

By Web:

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.

Improvements *********8****************
***************************8***************
***************************8****************

Highlights

Final Report issued on September 21, 2017

Highlights of Reference Number: 2017-10-056 to the Internal Revenue Service Chief, Agency-Wide Shared Services.

IMPACT ON TAXPAYERS

The IRS has a responsibility to protect its personnel, facilities, resources, taxpayers, and tax information. This includes protection from incidents, threats, and emergencies that may affect the safety of employees, facilities, and infrastructure. In Fiscal Year 2016, IRS employees and contractors reported to the Situation Awareness Management Center (SAMC) more than 2,400 physical security incidents at its facilities nationwide. The IRS's response to these incidents can affect the safety and security of the resources it is responsible to protect.

WHY TIGTA DID THE AUDIT

The objective of this review was to determine whether proper and timely incident reporting, recording, and response is occurring in order to protect IRS facilities, employees, and taxpayers.

WHAT TIGTA FOUND

IRS employees delay reporting physical security incidents to the SAMC. ***********8**********
**********************8****************************
**********************8****************************
**********************8****************************
**********************8****************************
**********************8****************************
**********************8****************************
**********************8****************************
**********************8****************************
**********************8****************************
**********************8****************************
**********************8****************************
**********************8*************
**********************8*********************************
**********************8*********************************
**********************8****************************** In addition, TIGTA found the incident reporting web page link can be difficult to find.

Also, the SAMC documented reported incidents in its database, as required; *********8*********
************************8*****************************
************************8***************************
**********************8****************************
**********************8****************************
**********************8****************************
**********************8****************************
**********************8****************************
**********************8****************************
**********************8****************************
**********************8****************************
**********************8****************************
**********************8****************************
**********************8****************************
**********************8****************************.

WHAT TIGTA RECOMMENDED

TIGTA recommended that the IRS provide all IRS and contract employees additional incident reporting training. In addition, the IRS should relocate the hyperlink to report incidents to a more visible location on its homepage. ****8****
***********************8***************************
***********************8***************************
***********************8***************************
***********************8***************************
***********************8***************************
***********************8***************************
******8*****

In its response, the IRS agreed with four of TIGTA's recommendations and partially agreed with one. The IRS plans to provide all employees and contractors with additional incident report training, relocate the reporting hyperlink to a more visible location on the IRS homepage, *****************8********************
******************************8*********************
******************************8*********************
******************************8*********************
******************************8*********************
******************************8*********************
******************************8*********************
******************************8*********************
8

TREASURY INSPECTOR GENERAL
FOR TAX ADMINISTRATION

DEPARTMENT OF THE TREASURY
WASHINGTON, D.C. 20220

September 21, 2017

MEMORANDUM FOR CHIEF, AGENCY-WIDE SHARED SERVICES

FROM: Michael E. McKenney
Deputy Inspector General for Audit

SUBJECT: Improvements **********8********** **********8********** (Audit # 201710011)

This report presents the results of our review of the reporting and processing of physical security incidents. The overall objective of this review was to determine whether proper and timely incident reporting, recording, and response is occurring in order to protect Internal Revenue Service (IRS) facilities, employees, and taxpayers. This audit is included in our Fiscal Year 2017 Annual Audit Plan and addresses the major management challenge of Security Over Taxpayer Data and Protection of IRS Resources.

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

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

Background.....Page 1

Results of Review.....Page 7

**********8**********
**********8**********.....Page 7

Recommendations 1 through 3:.....Page 11

Recommendations 4 and 5: .....Page 12

Appendices

Appendix I – Detailed Objective, Scope, and Methodology .....Page 13

Appendix II – Major Contributors to This Report.....Page 15

Appendix III – Report Distribution List .....Page 16

Appendix IV – Management's Response to the Draft Report .....Page 17

Abbreviations

FMSS	Facilities Management and Security Services
FUIR	Follow-Up Incident Report
FY	Fiscal Year
ID	Identification
IRM	Internal Revenue Manual
IRS	Internal Revenue Service
OI	Office of Investigations
SAMC	Situational Awareness Management Center
TIGTA	Treasury Inspector General for Tax Administration
TIRC	Threat Information and Critical Response Initiative Stakeholders

Background

The Federal tax administration system is of vital importance to the economy of the United States. As such, its protection must be assured at all times. The Internal Revenue Service (IRS) has a responsibility to protect its personnel, facilities, resources, taxpayers, and tax information. This includes protection from incidents, threats, and emergencies that may affect the safety of employees, facilities, and infrastructure. In Fiscal Year (FY) 2016, IRS employees and contractors reported more than 2,400 physical security incidents at its facilities nationwide.[1] The IRS's response to these incidents can affect the safety and security of the resources it is responsible to protect.

When the IRS faces an incident, threat, or emergency, multiple offices under the Facilities Management and Security Services (FMSS) office are responsible for reporting and response. The Situational Awareness Management Center (SAMC) is operated under an IRS contract overseen by the FMSS Policy, Planning, and Assessment Office, and the contractor is tasked with promptly reporting all significant security incidents to relevant stakeholders. Their mission is to document and report incidents, threats, and emergencies. Additionally, physical security personnel are responsible for responding to all incidents, including implementing relevant countermeasures. Together, these offices support the FMSS office and IRS law enforcement partners[2] to ensure the safety of employees, facilities, and infrastructure.

Process for reporting, notification, and response to physical security incidents

The IRS response to physical security incidents relies on action from IRS employees or contractors who report incidents, the SAMC that notifies relevant stakeholders, and physical security personnel who respond to incidents in conjunction with IRS law enforcement partners. Figure 1 depicts the reporting, notification, and response process when an incident occurs.

[1] In addition to physical security incidents, IRS employees reported more than 1,600 non-physical security incidents in FY 2016, including facility delays and closures, training exercises, employee illnesses, and taxpayer complaints. This does not account for incidents reported through other mechanisms under the responsibility of the Human Capital; Cybersecurity; or Privacy, Governmental Liaison, and Disclosure offices.
[2] IRS law enforcement partners include the Federal Protective Service, IRS Criminal Investigation, TIGTA Office of Investigations, and local law enforcement.

**********8**********

**********8**********
**********8**********
**********8**********
**********8**********
**********8**********
**********8**********
**********8**********
**********8**********
**********8**********
**********8**********
**********8**********
**********3**********8**********
**********8**********
**********8**********
**********8**********
**********8**********
**********8********** Physical security incidents are incidents and/or threats (direct, indirect, implied), ranging from more serious threats, such as those made by disruptive or disgruntled taxpayers and employees, to less serious office closures or loss of identification (ID) media.[4]

SAMC Watch Standers[5] are contract employees who route incident reports to the appropriate key IRS personnel such as FMSS office Headquarters staff, the Treasury Inspector General for Tax Administration (TIGTA) Office of Investigations (OI), the Senior Executive Team, the Threat Information and Critical Response Initiative Stakeholders (TIRC),[6] and other designated

[3] **********8**********

[4] Identification media include Smart ID cards, pocket commissions, building access cards, *etc*.

[5] Watch Standers are responsible for documenting, reporting, and sending notifications of all incidents and threats.

[6] The TIRC is comprised of staff from the FMSS office, the TIGTA-Criminal Intelligence and Counterterrorism Group; Criminal Investigation; Federal Protective Service; the Computer Security Incident Response Center; and the Office of Privacy, Governmental Liaison, and Disclosure. The mission of the TIRC is to identify and mitigate threats and record countermeasures and mitigation strategies as they pertain to Federal tax administration and the IRS for the protection of service operations.

officials. SAMC Watch Standers also promptly report to the Watch Commander[7] and the TIRC/SAMC Program Manager[8] all incidents and emergencies that result in the need to respond to the Department of the Treasury or the news media. The Watch Commander and the TIRC/SAMC Program Manager are kept apprised of situations that could require their immediate assistance or attention and notification of the Commissioner of the IRS; the Chief, Agency-Wide Shared Services; the Director, FMSS; or other IRS executives.

Physical Security Section Chiefs (hereafter referred to as Section Chiefs) and their support staff in each of the 13 IRS Territories[9] are responsible for responding to incidents in conjunction with other law enforcement personnel. **********8********** **********8********** They are also responsible for completing a Follow-Up Incident Report (FUIR), if required, and the implementation of countermeasures.

Levels of physical security incidents

Every incident reported to the SAMC is assigned a threat level by the Watch Stander on duty. These threat levels range from one to three depending on the significance of the incident. The Watch Commander is notified of all incidents, but incidents may also require that additional notifications be sent, depending on the threat. All incidents that have been classified as a level one incident require an FUIR. The impacted Section Chief is the responsible party for submitting the FUIR. **********8********** **********8********** Figure 2 shows the proportion of physical security incidents that occurred in FY 2016 by threat level, and Figure 3 defines the three different levels of threat.

[7] The Watch Commander serves as the security personnel monitoring all incidents and threats to the IRS to assist in identifying the validity of the data reported.
[8] The TIRC Program Manager develops policy and procedures for the purpose of implementing proper mitigation and countermeasures to ensure that all incidents and threats to the IRS have proper mitigation and countermeasures in place to ensure the safety of IRS employees and facilities.
[9] A Territory footprint consists of multiple sites across several States, varying in size, population, and facility security level and may include a combination of Federal and leased buildings.

**********8**********[10]

**********8**********
**********8**********
**********8**********
**********8**********
**********8**********
**********8**********
**********8**********
**********8**********
**********8**********
**********8**********
**********8**********
**********8**********
**********8**********

[10] **********8**********
**********8**********
**********8**********
**********8**********.

Figure 3: Definition of Threat Levels

Level	Definition
One	Imminent threat to an IRS employee, facility, contractor, or IRS infrastructure, such as: direct threat or actual attack/assault against IRS employees (in relation to a known or implied nexus to their employment), facilities, or infrastructure; substantiated bomb threat; hazardous materials; civil disturbance that ends in violence; logical or physical access without permission to network, system, application, data, or other resource; and substantiated ties to domestic or foreign terrorism.
Two	Imminent threat, but no immediate danger against IRS employees or contractors, facilities, or resources, such as: unsubstantiated suspicious packages; robbery of an employee or a taxpayer on IRS property; burglary of IRS property; demonstrations; closures of IRS facilities due to acts of nature (tornados, hurricanes, snow, *etc*.); threat to employee(s) with no direct imminent or known ability to carry out the threat; unsubstantiated hazardous materials; cyberattacks that successfully prevent or impair normal authorized functionality of networks and systems; and high-impact loss, theft, or disclosure of sensitive data.
Three	Not an imminent threat. This level primarily includes training exercises and the loss of IDs and badges. This level also involves efforts to intimidate the IRS or to obstruct IRS operations through the use of frivolous liens or other financial instruments that fall into this category. In addition, disgruntled taxpayers and suicide threats are categorized in this level.

Source: The SAMC Reference Binder, IRS Incident Types and Level (May 2016).

**********8**********

**********8**********[11] ****
**********8**********
**********8**********
**********[12] **********8**********
**********8**********
**********8**********
**********8**********
**********8**********
**********8**********
**********8**********

**********8**********
**********8**********

[11] **********8**********
[12] **********8**********
**********8**********

**********8**********
8.

**********8**********

**********8**********
**********8**********
**********8**********
**********8**********
**********8**********
**********8**********
**********8**********
**********8**********
**********8**********
**********8**********
**********8**********
**********8**********
**********8**********
**********8**********
**********8**********
**********8**********
**********8**********
**********8**********
**********8**********.[13]

This review was performed at the IRS Headquarters in the FMSS Office in Washington, D.C., during the period October 2016 through May 2017. 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.

[13] The percentages in Figure 4 total 99.9% due to rounding.

Results of Review

**********8**********
**********8**********

**********8**********. IRS policy[14] requires the FMSS office to establish and manage a process for properly identifying, protecting, processing, handling, and analyzing all incidents and threats within the IRS; **********8**********
**********8********* Proper and timely incident reporting is essential to assist IRS management to make operational decisions on how to respond to physical security incidents and reduce the effects of threats to IRS personnel, facilities, and property.

**********8**********

**********8**********[15]
**********8**********
**********8**********
**********8**********[16]

We reviewed incident report documentation maintained by the SAMC and compared the time the reporter stated that the incident occurred to the time that the incident report was e-mailed to the SAMC to determine the incident reporting time. **********8**********
**********8**********
****8****.

[14] IRM 10.2.8.3, *Incident Reporting* (May 31, 2016).
[15] **********8**********
**********8**********
**********8**********
******8*******
[16] **********8**********
**********8**********
******8*******

**********8**********
**********8**********
**********8**********
**********8**********
**********8**********
**********8**********
**********8**********
**********8**********

**********8**********
**********8**********
**********8**********
**********8**********

**********8**********
**********8**********
**********8**********
**********8**********
**********8**********
**********8**********
8.

**********8********** the FMSS office provides e-mail notices for security-related issues, and annual security awareness training is required for all IRS employees. ****8**** we found that the incident reporting hyperlink is difficult to find—requiring six clicks to navigate from the IRS homepage to the location of the incident reporting page. **********8**********
**********8**********
**********8**********
**********8**********.

**********8**********
**********8**********

**********8**********
**********[17] **********8**********
**********8**********
**********8**********
**********8**********[18] Watch Standers are alerted of a reported incident by e-mail, which they use to enter incident information

[17] The SAMC's data system provides a platform to capture, monitor, and track threats against the organization.
[18] **********8**********
**********8**********

into the SAMC's data system. The Watch Stander then sends a notification e-mail to comply with the requirement to inform IRS stakeholders of incidents in order to ensure the safety of IRS employees, facilities, and infrastructure.

We compared the population of reported physical security incidents to the SAMC's data system,
**********8**********
**********8**********
**********8**********
**********8**********
**********8**********
**********8**********
**********8**********
**********8**********

**********8**********
**********8**********
**********8**********
**********8**********
**********8**********
**********19*****8**********
******8********

**********8**********

*********8*********	***8***
*****8*****	**********8********** ***********8********
*****8*****	**********8**********
*****8*****	**********8********** **********8**********

**********8**********

**********8**********
**********8**********
**********8**********
**********8**********
**********8**********.

[19] **********8**********
**********8**********
*****8*****

**********8**********
**********8**********
**********8*********[20] **********
**********8**********
**********8**.[21] IRS policy[22] requires that personnel identified for their role in security matters or continuity of operations responsibilities within the IRS will be notified of incidents to ensure the safety of IRS employees, facilities, and infrastructure. All level one and select level two and three incidents require an e-mail notification.

**********8**********
**********8**********. Prior to March 2016, the SAMC did not require Watch Standers to maintain copies of notifications in its data system. *8*
**********8**********
**********8**********
**********8**********
**********8**********
**********8**********
**********8**********
**********8**********
**********8**********.

Especially for the most serious incidents, IRS stakeholders may be notified of the threat by means other than the SAMC. **********8**********
**********8********** personnel within the IRS were notified by other means such as TIGTA, allowing them to respond; ensure the safety of IRS employees, facilities, and infrastructure; and take action when required. **********8**********
**********8**********

**********8**********

**********8**********
**********8**********
**********8**********
**********8**********
**********8**********

[20] **********8**********
**********8**********
**********8**********.

[21] **********8**********
**********8**********
*******8******

[22] IRM 10.2.8.9(1), *Incident Notifications* (May 31, 2016).

**********8**********
**********8**********. IRS policy[23] states that all incidents classified as a level one threat require an FUIR. The FUIR includes details about the incident, the reporter, investigative findings and analysis, and any mitigation recommendations or actions taken. **********8**********
**********8**********
**********8**********
**********8**********
**********8**********
**********.[24]**8**********
**********8**********
**********8**********
****8***. These reports provide FMSS with information that allow Security Specialists to implement mitigation actions and identify trends to develop effective countermeasures that minimize the effect of future disruptions.

Recommendations

The Director, FMSS, should:

Recommendation 1: Provide all IRS and contract employees additional incident reporting training and reminders of incident reporting requirements.

> ***Management Response:*** The IRS agreed with this recommendation and stated that it will ensure that all IRS employees and SAMC contractors receive additional incident reporting training and reminders of incident reporting requirements.

Recommendation 2: Coordinate with Communications and Liaison to relocate the SAMC's reporting hyperlink to a more visible location on the IRS homepage.

> ***Management Response:*** The IRS agreed with this recommendation and stated that it will coordinate with Communications and Liaison to relocate the SAMC's reporting hyperlink to a more visible location on the IRS homepage.

Recommendation 3: **********8**********
**********8**********
**********8**********
**********8**********

[23] IRM 10.2.8.6(1), *Incident Report* (May 31, 2016).
[24] **********8**********
********8**********.

Management Response: *********8**********
**********8**********
**********8**********
**********8**********
**********8**********.

Recommendation 4: **********8**********
**********8**********
**********8**********.

Management Response: *******8**********
**********8**********
**********8**********
**********8**********
**********8**********
**********8**********

Office of Audit Comment: ****8**********
**********8**********
**********8**********
**********8**********
**********8**********
**********8**********

Recommendation 5: **********8**********
**********8**********
**********8**********.

Management Response: ******8**********
**********8**********
**********8**********
******8******.

Appendix I

Detailed Objective, Scope, and Methodology

Our overall objective was to determine whether proper and timely incident reporting, recording, and response is occurring in order to protect IRS facilities, employees, and taxpayers. To accomplish our objective, we:

I. Determined the IRS's criteria and process for reporting and responding to physical security incidents.

A. Identified the appropriate Federal laws and regulations pertaining to physical security incident reporting and responding.

B. Identified applicable IRS policies and Standard Operating Procedures regarding physical security incident reporting, responding to reported incidents, and follow-up procedures.

C. Interviewed IRS personnel to understand the process, roles, and responsibilities for reporting and responding to incidents.

II. Determined the effectiveness of the IRS's process for recording incidents, providing timely notification, and responding to identified threats.

A. Evaluated the SAMC process for recording incidents and providing timely notification.

1. Obtained an extract of SAMC records for all incidents reported in FY 2016. We assessed the reliability of the SAMC incident data by 1) performing electronic testing of required data elements, 2) observing the extraction of the records from the system that produced them, and 3) interviewing agency officials knowledgeable about the data. We determined that the data were sufficiently reliable for purposes of this report.

2. Obtained records of all incidents reported through the SAMC web in FY 2016. We assessed the reliability of the SAMC reporting data by 1) performing electronic testing of required data elements and 2) interviewing agency officials knowledgeable about the data. We determined that the data were sufficiently reliable for purposes of this report.

3. Determined whether all incidents reported through the SAMC web hyperlink and via e-mail from TIGTA were recorded in the SAMC's data system.

4. **********8**********
**********8**********

**********8**********.[1] **********
**********8**********
**********8**********
**********8**********
**********8**********
**********8**********
**********8**********

a. **********8**********

b. **********8**********
**********8**********

B. Evaluated the IRS response to identified threats.

1. Determined whether an FUIR was prepared for each level one incident.
2. For the stratified sample of levels one, two, and three incidents recorded in the SAMC's data system, determined whether the IRS responded to the incident, including sending notifications and taking action when required.
3. For the most common incident types observed in FY 2016, interviewed IRS personnel and requested documentation to support whether the IRS has a standard process in place to respond to and reduce the occurrence of those incidents.

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: Agency-Wide Shared Services, FMSS office policies, procedures, and practices for determining whether proper and timely incident reporting, recording, and response was occurring. We evaluated these controls by interviewing FMSS office management and SAMC contractors responsible for incident reporting, analyzing the SAMC incident and reporting data, and evaluating the sampled incident case files.

[1] **********8**********
**********8**********
**********8**********
**********8**********
**********8**********

Appendix II

Major Contributors to This Report

Gregory D. Kutz, Assistant Inspector General for Audit (Management Services and Exempt Organizations)
Jonathan T. Meyer, Director
Deanna G. Lee, Audit Manager
Zachary P. Orrico, Lead Auditor
Gene A. Luevano, Senior Auditor

Appendix III

Report Distribution List

Commissioner
Office of the Commissioner – Attn: Chief of Staff
Deputy Commissioner for Operations Support
Director, Facilities Management and Security Services
Director, Office of Audit Coordination

Appendix IV

Management's Response to the Draft Report

DEPARTMENT OF THE TREASURY
INTERNAL REVENUE SERVICE
WASHINGTON, DC 20224

CHIEF
AGENCY-WIDE
SHARED SERVICES

August 8, 2017

MEMORANDUM FOR MICHAEL E. MCKENNEY
DEPUTY INSPECTOR GENERAL FOR AUDIT

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

SUBJECT: Improvements ****8***** *******8**********
(TIGTA Audit # 201710011)

Thank you for the opportunity to respond to the subject draft audit report.

**********8**********8**********8**********. The Situational Awareness Management Center (SAMC) is designed to provide IRS leadership awareness of threats and incidents that may impact IRS operations. This awareness allows IRS leaders to direct appropriate activities to prevent further occurrences or to mitigate the effects of future incidents. The SAMC does not provide emergency alert notifications nor does it dispatch emergency responders. In most cases, by design, emergency response personnel and other IRS stakeholders are alerted to an incident and are in action before notifications are made to the SAMC. **********8**********8*****8*******. Independent of the SAMC notifications, there are designated first responder and emergency alert notification systems that play a critical role in the timely response to incidents.

We agree with all five recommendations and will develop and 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 202-317-7500, or a member of your staff may contact Richard L. Rodriguez, Director, Facilities Management and Security Services, at 703-414-2143. For matters concerning audit procedural follow-up, please contact Amy Favara at 313-234-1565 or Dani Stonehocker at 801-388-8285, Office of Strategic Planning & Controls, Agency-Wide Shared Services.

Attachment

Attachment

RECOMMENDATION 1:

The Director, FMSS, should provide all IRS and contract employees, additional incident reporting training and reminders of incident reporting requirements.

CORRECTIVE ACTION:

The IRS agrees with this recommendation. The Director, FMSS, will ensure that all IRS employees and SAMC contractors receive additional incident reporting training and reminders of incident reporting requirements.

IMPLEMENTATION DATE:

September 30, 2018

RESPONSIBLE OFFICIAL:

Director, Facilities Management & Security Services, AWSS

CORRECTIVE ACTION MONITORING PLAN:

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:

The Director, FMSS, should coordinate with Communications & Liaison, to relocate the SAMC's reporting hyperlink to a more visible location on the IRS homepage.

CORRECTIVE ACTION:

The IRS agrees with this recommendation. The Director, FMSS, will coordinate with Communications & Liaison to relocate the SAMC's reporting hyperlink to a more visible location on the IRS homepage.

IMPLEMENTATION DATE:

January 31, 2018

RESPONSIBLE OFFICIAL:

Director, Facilities Management & Security Services, AWSS

CORRECTIVE ACTION MONITORING PLAN:

AWSS will enter accepted corrective actions into JAMES. These corrective actions are monitored on a monthly basis until completion.

2

RECOMMENDATION 3:

**********8**********
**********8**********
**********8******
**********8**********
*.

CORRECTIVE ACTION:

The IRS agrees with this recommendation. **********8********
**********8**********
**********8**********
**********8**********

IMPLEMENTATION DATE:

January 31, 2018

RESPONSIBLE OFFICIAL:

Director, Facilities Management & Security Services, AWSS

CORRECTIVE ACTION MONITORING PLAN:

AWSS will enter accepted corrective actions into JAMES. These corrective actions are monitored on a monthly basis until completion.

RECOMMENDATION 4:

**********8**********
**********8**********
****
8**********.

CORRECTIVE ACTION:

The IRS partially agrees with this recommendation. **********8**********
**********8**********
**********8**********
**********8**********
**********8********** .

IMPLEMENTATION DATE:

September 30, 2018

RESPONSIBLE OFFICIAL:

Director, Facilities Management & Security Services, AWSS

CORRECTIVE ACTION MONITORING PLAN:

AWSS will enter accepted corrective actions into JAMES. These corrective actions are monitored on a monthly basis until completion.

RECOMMENDATION 5:

**********8**********
**********8**********
**********8**********.

CORRECTIVE ACTION:

The IRS agrees with this recommendation. **********8**********
**********8**********
**********8**********.

IMPLEMENTATION DATE:

January 31, 2018

RESPONSIBLE OFFICIAL:

Director, Facilities Management & Security Services, AWSS

CORRECTIVE ACTION MONITORING PLAN:

AWSS will enter accepted corrective actions into JAMES. These corrective actions are monitored on a monthly basis until completion.