U.S. OFFICE OF PERSONNEL MANAGEMENT
OFFICE OF THE INSPECTOR GENERAL
OFFICE OF EVALUATIONS AND INSPECTIONS

Final Evaluation Report

EVALUATION OF THE U.S. OFFICE OF PERSONNEL MANAGEMENT'S INSIDER THREAT PROGRAM

Report Number 4K-CI-00-16-053
April 7, 2017

EXECUTIVE SUMMARY

Evaluation of the U.S. Office of Personnel Management's Insider Threat Program

Report No. 4K-CI-00-16-053 **April 7, 2017**

Why Did We Conduct the Evaluation?

This evaluation was conducted at the request of the U.S Office of Personnel Management's (OPM) Insider Threat Program Management to meet the *National Insider Threat Policy and Minimum Standards*' requirement to have an independent internal assessment.

The objective of our evaluation was to determine if OPM's Insider Threat Program is in compliance with the policies and standards of the *National Insider Threat Policy and Minimum Standards* and assess the progress of the program's implementation.

William W. Scott, Jr.
Chief, Office of Evaluations and Inspections

What Did We Find?

We determined that OPM's Insider Threat Program was in compliance with the policies and standards of the *National Insider Threat Policy and Minimum Standards*. However, we identified areas within the program where corrective action was needed. Specifically, we found:

- OPM had not created [redacted] as recommended by the National Insider Threat Task Force's 2016 post-assessment.

- OPM's Office of Security Services (Security Services) did not have a process in place for insider threat personnel to verify that all cleared employees are meeting the training requirements.

- Security Services did not have a process in place to ensure that cleared employees submit their *Employee Foreign Travel Questionnaire* in a timely manner upon their return from foreign travel.

Since the conclusion of our fieldwork, Security Services has addressed these issues and we consider them closed.

In addition to the issues above, we found that the performance standards for all of OPM's senior officials did not reflect their role and responsibility as it relates to the Insider Threat Program, which OPM plans to address.

TABLE OF CONTENTS

INTRODUCTION

This final evaluation report details the results of our evaluation of the *U.S. Office of Personnel Management's (OPM) Insider Threat Program*. This evaluation was conducted by OPM's Office of the Inspector General (OIG), as authorized by the Inspector General Act of 1978, as amended.

OPM established its Insider Threat Program in May 2013, in accordance with Executive Order (E.O.) 13587, *Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information*, and in conjunction with the White House Memorandum of November 21, 2012, *National Insider Threat Policy and Minimum Standards for Executive Branch Insider Threat Programs*, which states that all executive branch departments and agencies that have access to classified information should implement an insider threat detection and prevention program.[1]

To ensure agencies' program implementation reflected the requirements of these legal authorities, the National Insider Threat Task Force developed a *Guide to Accompany the National Insider Threat Policy and Minimum Standards* in November 2013. As outlined in these standards, the insider threat policy and implementation plan should include the following ten steps:

1. Designate a senior official;
2. Obtain visible support from the agency head;
3. Form working group/provide periodic feedback to the community;
4. Review current requirements and guidance;
5. Seek legal input;
6. Protect privacy and civil liberties by applying appropriate safeguards;
7. Identify classified and other critical assets;
8. Write agency policy and implementation plan;
9. Obtain approval, establish a program office and implementation plan; and,
10. Conduct scheduled self-assessments.[2]

The purpose of OPM's Insider Threat Program is to deter, detect, and mitigate actions by their personnel cleared to handle classified information who may present a threat to national security through potential espionage, violent acts against the Government or the nation, or unauthorized

[1] National Insider Threat Task Force, *Guide to Accompany the National Insider Threat Policy and Minimum Standards*, November 2013, p. 1.
[2] Ibid., p. 5-15.

disclosure of classified information.[3] The program primarily relies on educating personnel, promoting awareness, and conducting responsive investigative activities to meet its intended purpose.[4] OPM currently has approximately 2,000 Federal employees and contractors with secret and top secret clearances within its various program offices.

OPM's Insider Threat Program is administered by the Office of Security Services (Security Services), within Facilities, Security, and Emergency Management. The Director of Security Services serves as the Insider Threat Program Manager. OPM's Insider Threat Program involves coordination among key program offices, to include the Office of the Chief Information Officer; Facilities, Security, and Emergency Management; and the Federal Investigative Services.[5] The Office of the Chief Information Officer meets the program's technology needs by implementing and helping to maintain computer specific technology for monitoring personnel activity on OPM's network. Within OPM's Facilities, Security, and Emergency Management, the Personnel Security Office carries out personnel security related actions for all OPM employees and OPM contractors and Security Services manages OPM's physical and information security programs. These offices share personnel information, such as marital status, financial history, and foreign travel, to resolve insider threat matters. The National Background Investigations Bureau provides counterintelligence expertise on related insider threat issues. These three program offices are vital to the detection of insiders who pose a risk to classified information, and mitigation of risks through administrative and investigative responses.

With regard to the *National Insider Threat Policy and Minimum Standards*, OPM's Insider Threat Program reached full operating capability on November 29, 2016, making it the sixth Federal program to reach full operating capability.

[3] McCombs, Kevin, Memorandum on *OPM Insider Threat Program Annual Assessment Report*, May 2016, p. 1.
[4] Ibid., p. 2.
[5] As of October 1, 2016, OPM established the National Background Investigations Bureau to replace the functions of the Federal Investigative Services.

RESULTS OF EVALUATION

We determined that OPM's Insider Threat Program is in compliance with the *National Insider Threat Policy and Minimum Standards*. However, we identified areas within the program where corrective action was needed. The following describes the specific areas we identified during our evaluation.

1. One Unimplemented National Insider Threat Task Force Recommendation

In May 2014, the National Insider Threat Task Force conducted an independent assessment of OPM's Insider Threat Program to assess its implementation of the *National Insider Threat Policy and Minimum Standards* and its progress toward reaching initial operating capability and full operating capability. This assessment yielded three initial operating capability recommendations and five full operating capability recommendations. The National Insider Threat Task Force conducted a post-assessment review in February 2016 to determine OPM's progress toward implementing the recommendations contained in its 2014 assessment report. They determined OPM had not addressed the following recommendations:

- [redacted]; and,
- [redacted].

As of May 2016, OPM addressed the recommendation to deploy technical capability to monitor user activity on all classified networks through a memorandum of agreement with the Department of Homeland Security. However, OPM had yet to create [redacted] as recommended by the National Insider Threat Task Force's 2016 post-assessment.

The Office of the Chief Information Officer, which is responsible for this recommendation, has not addressed it due to a lack of adequate staffing and has stated it plans to address the issue in fiscal year 2017, pending the passage of OPM's budget. As a result, OPM's ability to deter, detect, and mitigate insider threats could potentially be compromised due to the lack of [redacted]

Recommendation 1

We recommended that the Office of the Chief Information Officer create [redacted] in accordance with the *National Insider Threat Policy and Minimum Standards*.

Security Services' Comments

Security Services fully concurred with the recommendation. Security Services also provided a standard operating procedure to [redacted], which was submitted to the National Insider Threat Task Force for validation and acceptance in regard to the outstanding recommendation.

OIG Comments

We reviewed the standard operating procedure that was provided. On November 29, 2016, the National Insider Threat Task Force accepted this standard operating procedure and OPM's Insider Threat Program reached full operating capability. We determined that they addressed our recommendation. We consider this recommendation closed.

2. Lack of Procedures to Verify Insider Threat Awareness Training

In accordance with the *National Insider Threat Policy and Minimum Standards*, OPM's *Classified National Security Information Program Manual* requires that all employees granted access to classified national security information receive training within 30 days of initial employment or following the granting of access to classified information, and annually thereafter. During our evaluation, we found that Security Services did not have a process in place for insider threat personnel to verify that all cleared employees are meeting the training requirements. Specifically, we found that 94 cleared employees could not be verified as having completed insider threat awareness training for fiscal year 2016**.**

Security Services tracks all cleared employees' insider threat awareness training via grades generated when cleared employees complete the online training through OPM's Learning Connection website. We compared the fiscal year 2016 training grades to the current list of all OPM-cleared employees, which Security Services tracks in their Bi-weekly Clearance Reports.

Security Services did not have a process to reconcile discrepancies between their Bi-weekly Clearance Reports and training grades to ensure all cleared employees have completed the insider threat awareness training. As a result, cleared employees who have not completed the insider threat awareness training would be unaware of the current and potential threats in their work and personal environment.

Recommendation 2

We recommended that Security Services develop a process for insider threat personnel to ensure all OPM-cleared employees are meeting the annual insider threat awareness training requirement. This process should include reconciling any discrepancies, if information is obtained from more than one source.

Security Services' Comments

Management fully concurred with the recommendation. Security Services developed and provided us with the Classified National Security Information Briefing and Training Standard Operating Procedure.

OIG Comments

We reviewed the written procedure, which provides the policy that Facilities, Security, and Emergency Management will follow to ensure all OPM-cleared employees are meeting the annual insider threat awareness training requirement. We determined that this written procedure addresses our recommendation. We consider this recommendation closed.

3. Lack of Procedures for Conducting Post-Travel Debriefings

As part of the implementation of the Insider Threat Program, the Offices of Security Services and Personnel Security signed a memorandum of agreement to coordinate efforts for reporting official and unofficial foreign travel conducted by cleared employees. As outlined in the memorandum of agreement, Personnel Security shares cleared employees' foreign travel plans with Security Services to determine whether cleared employees encountered any threats during their travel. Prior to their departure, Security Services provides cleared employees with an emailed briefing, which includes a summary of the significant security threats in the intended travel location; and in accordance with the *National Insider Threat Policy and Minimum Standards*, a copy of the *Employee Foreign Travel Questionnaire*, which serves as a post-travel

debriefing to be completed upon return. The questionnaire allows cleared employees to report any unusual incidents that occurred during their trip, and depending on the responses, allows Security Services to determine if a more detailed debriefing is necessary. Security Services tracks when a cleared employee completes and returns the *Employee Foreign Travel Questionnaire*, and maintains a file of all completed questionnaires.

We found that, Security Services did not have a process in place to ensure that cleared employees submit their *Employee Foreign Travel Questionnaire* in a timely manner upon their return from foreign travel. Specifically, we found 20 instances in 2016,[6] where cleared employees reported foreign travel but Security Services had not received a completed *Employee Foreign Travel Questionnaire*.

As a result of not having a process in place to ensure foreign travel questionnaires are returned, Security Services may be unaware if a cleared employee encountered an unusual incident during travel, which may be considered a threat and requires the cleared employee to receive a more detailed debriefing.

Recommendation 3

We recommend Security Services establish a process, to include a deadline for Employee Foreign Travel Questionnaires to be returned, to ensure that all cleared employees are debriefed upon their return from foreign travel.

Security Services' Comments

Security Services fully concurred with the recommendation. Security Services developed procedures for employees to complete and return their Employee Foreign Travel Questionnaires within 5 days after returning from foreign travel.

OIG Comments

We reviewed the procedures and determined that they addressed our recommendation. We consider this recommendation closed.

[6] These 20 instances include all cleared employees who traveled from January – September 2016 as reported on Security Services' *Foreign Travel Tracker*, which we obtained on October 3, 2016.

4. Senior Officials' Performance Standards Do Not Reflect Their Insider Threat Responsibility

In accordance with the National Insider Threat Task Force's guidance, OPM designated three Insider Threat senior officials because elements of its Insider Threat Program required coordination among multiple program offices. The senior officials include OPM's:

- Associate Director of the Federal Investigative Services;[7]
- Director of Facilities, Security Emergency Management; and,
- Chief Information Officer.

OPM's senior officials have equal responsibility and authority for the direction and management of its Insider Threat Program. However, during our evaluation we found that the performance standards for all of OPM's senior officials do not reflect their role and responsibility as it relates to the Insider Threat Program, despite sharing equal responsibility for the program. More specifically, only one of the three senior official's performance standards included the Insider Threat Program as a performance element.

We were unable to determine why all senior officials' performance standards were not reflective of their responsibility and authority for the direction and management of the Insider Threat Program. By not having the Insider Threat Program as a performance element on all senior officials' performance standards, there could be a lack of coordination between the senior officials to address insider threat issues such as, the outstanding National Insider Threat Task Force recommendation to achieve full operating capability, and ultimately, OPM's Insider Threat Program's operational functions could be hindered.

Recommendation 4

We recommended that all designated OPM senior officials' performance standards reflect their responsibility and authority for the direction and management of its Insider Threat Program.

[7] As a result of OPM establishing the National Background Investigations Bureau to replace the functions of the Federal Investigative Service in October 2016, the Associate Director of the Federal Investigative Services as an Insider Threat senior official has been replaced by the Director of the National Background Investigations Bureau.

Security Services' Comments

Management fully concurred with the recommendation. Security Services plans to modify the performance agreements for the three OPM Insider Threat senior officials by March 1, 2017 to incorporate Insider Threat responsibilities.[8]

[8] On March 30, 2017, OPM notified us that, due to administrative delays, they plan to modify the performance agreements for the three OPM Insider Threat senior officials by June 1st, 2017.

APPENDIX A: SCOPE AND METHODOLOGY

We conducted this evaluation in accordance with the *Quality Standards for Inspection and Evaluation*, January 2012, approved by the Council of the Inspectors General on Integrity and Efficiency.

We performed our evaluation fieldwork from June 28, 2016 through October 19, 2016 at the OPM Headquarters in Washington, DC.

The scope of this evaluation was fiscal year 2016. To assess OPM's implementation of its Insider Threat Program, we reviewed the *National Insider Threat Policy and Minimum Standards.* Using these standards, we focused our evaluation on the following areas: (1) Management and Security, (2) Monitoring and Reporting of Suspicious Activity, (3) Policies and Procedures, (4) Classified and Unclassified Networks Critical to the Mission, (5) Training, and (6) Foreign Travel.

We interviewed OPM's Insider Threat Program manager and key program personnel to gain an understanding of the program's stakeholders, OPM's network and monitoring capabilities, periodic self-assessments, results of the National Insider Threat Task Force assessments, promotion and tracking of insider threat awareness training for cleared employees, and its foreign travel program. We also met with the program manager for the Office of the Chief Information Officer's Security Operations to understand the role of the Office of the Chief Information Officer as it relates to the Insider Threat Program.

As part of our assessment of OPM's implementation of its Insider Threat Program, we reviewed and analyzed OPM's insider threat policy, implementation plan, approved manual, related memoranda of agreement, awareness training materials, and foreign travel materials. We also reviewed the results of all National Insider Threat Task Force assessments to determine if OPM has addressed all their recommendations. We conducted a review of OPM's Insider Threat senior officials' performance standards to determine whether their standards reflected their role and responsibility as it relates to the Insider Threat Program.

To verify OPM met the *National Insider Threat Policy and Minimum Standards* related to awareness training, foreign travel and physical security, we performed the following:

- Compared the fiscal year 2016 insider threat awareness training grades to Security Services' Bi-weekly Clearance Report, which included a list of all OPM-cleared employees as of July 14, 2016;

- Reviewed and analyzed Security Services' tracking system for conducting post-travel debriefings for cleared employees; and,

- Conducted a physical site inspection of all classified systems to verify that they displayed the required warning banner for all cleared users.

Due to the nature of the evaluation, we did not verify the reliability of the information within Security Services' reports and lists of cleared employees. However, while analyzing this information, nothing came to our attention to cause us to doubt their reliability. We believe that the reports and lists provided were sufficient to achieve our evaluation objective.

APPENDIX B: MANAGEMENT COMMENTS

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT
Washington, DC 20415

December 21, 2016

MEMORANDUM FOR WILLIAM S. SCOTT, JR.
Chief, Office of Evaluations and Inspections
Office of the Inspector General

FROM: DEAN S. HUNTER
Director
Facilities, Security & Emergency Management

CHARLES S. PHALEN, JR.
Director
National Background Investigations Bureau

DAVID L. DEVRIES
Chief Information Officer

DAVID DEVRIES
Digitally signed by DAVID DEVRIES
Date: 2016.12.29 16:47:39 -05'00'

SUBJECT: Response to Draft Report on Evaluation of the U.S. Office of Personnel Management's Insider Threat Program
(Report No. 4K-CI-00-16-053)

Thank you for the opportunity to respond to the Office of Inspector General's (OIG) evaluation of the U.S. Office of Personnel Management's (OPM) Insider Threat Program. OPM fully concurs with the recommendations. Our responses and action plans to address the two outstanding recommendations are provided below:

1. Lack of Procedures to Verify Insider Threat Awareness Training

   We recommend that Security Services develop a process for insider threat personnel to ensure all OPM employees are meeting the annual insider threat awareness training requirement. This process should include reconciling any discrepancies, if information is obtained from more than one source.

   Corrective Action Plan: The attached *Classified National Security Information Briefing and Training Standard Operating Procedure* provides the policy FSEM will follow to ensure that annual insider threat awareness training requirements are met.

2. Senior Officials' Performance Standards Did Not Reflect Insider Threat Responsibility

   OPM's Insider Threat Senior Officials have equal responsibility and authority for the direction and management of the Inside Threat Program. However, during the evaluation, only one of the three senior officials' performance standards included the Insider Threat Program as a performance element.

   Corrective Action Plan: The performance agreements for the three OPM Insider Threat Senior Officials will be modified by March 1, 2017 to incorporate Insider Threat responsibilities.

It is worth noting that on November 29, 2016, the National Insider Threat Task Force (NITTF) determined that the OPM Insider Threat Program had fulfilled all programmatic requirements established by the National Policy and Minimum Standards and had reached full operating capability. Additionally, the draft report has been submitted to the National Counterintelligence Executive (NCIX)/NITTF, who is designated the original classification authority for U.S. insider threat activities undertaken in accordance with Executive Order 13587, to determine if the public release of the final evaluation report on the OIG webpage, poses a concern.

If you have any questions regarding this response, please contact Kevin McCombs, Director, Security Services, on [redacted] or via email at [redacted]@opm.gov.

Report Fraud, Waste, and Mismanagement

Fraud, waste, and mismanagement in the Government concerns everyone: Office of the Inspector General staff, agency employees, and the general public. We actively solicit allegations of any inefficient and wasteful practices, fraud, and mismanagement related to OPM programs and operations. You can report allegations to us in several ways:

By Internet: http://www.opm.gov/our-inspector-general/hotline-to-report-fraud-waste-or-abuse

By Phone: Toll Free Number: (877) 499-7295
Washington Metro Area: (202) 606-2423

By Mail: Office of the Inspector General
U.S. Office of Personnel Management
1900 E Street, NW
Room 6400
Washington, DC 20415-1100