



**U.S. OFFICE OF PERSONNEL MANAGEMENT
OFFICE OF THE INSPECTOR GENERAL
OFFICE OF EVALUATIONS**

Final Evaluation Report

**OPM'S PHYSICAL SECURITY RISK
ASSESSMENT PROCESS**

Report Number 4K-FS-00-20-012

May 26, 2020

OFFICE OF
PERSONNEL MANAGEMENT

EXECUTIVE SUMMARY

OPM's Physical Security Risk Assessment Process

Report No. 4K-FS-00-20-012

May 26, 2020

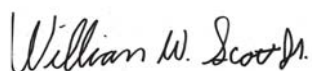
Why Did We Conduct the Evaluation?

Given emergent threats to Federal Government buildings, the U.S. Office of Personnel Management's (OPM) then Acting Director of Facilities, Security, and Emergency Management (FSEM) suggested that we conduct an evaluation of the OPM's physical security risk assessment process. OPM must ensure its employees, contractors, resources, and assets are safe and secure. As a result, we sought to determine: (1) the effectiveness and efficiency of OPM's FSEM's Security Services' process for performing physical security risk assessments and its compliance with the *Executive Order 12977's* Interagency Security Committee's (ISC) standard; and (2) what limitations or challenges, if any, has OPM reported facing in conducting physical security assessments and monitoring the results.

What Did We Find?

Within OPM, the Security Services office under the Facilities, Security, and Emergency Management group is responsible for providing a safe and secure environment for OPM's information, personnel, and operations. The Security Services office manages OPM's physical security, information security, and insider threat programs, including physical access control, threat assessments, and applicable national, industrial, and communications security directives. During our evaluation, we determined that Security Services needed to improve controls for monitoring OPM's physical security risk assessment results. Security Services' staff does not record assessment results, such as the countermeasures recommended for facilities and the status of countermeasures, in its security assessment database. In addition, Security Services' management does not perform ongoing monitoring or separate quality control reviews to ensure program objectives are met.

We made two recommendations to improve controls for monitoring OPM's physical security risk assessment results. Security Services' management concurred with our findings and recommendations and took immediate corrective actions to address our concerns. Based on our analysis of the corrective actions taken we consider both recommendations resolved and closed.



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

ABBREVIATIONS

CIO	Chief Information Office
FSEM	Facilities, Security, and Emergency Management
GAO	Government Accountability Office
HRS	Human Resources Solutions
ISC	Interagency Security Committee
MSAC	Merit System Accountability and Compliance
OIG	Office of the Inspector General
OPM	U.S. Office of Personnel Management
RMP	Risk Management Process for Federal Facilities
ROC	Retirement Operations Center

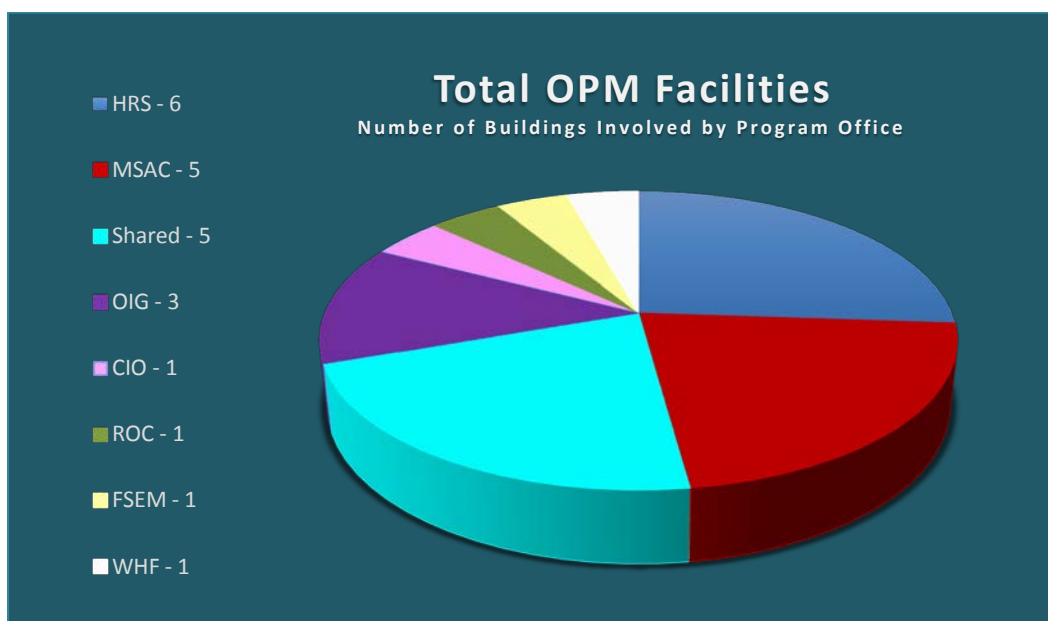
TABLE OF CONTENT

	<u>Page</u>
EXECUTIVE SUMMARY	i
ABBREVIATIONS	ii
INTRODUCTION	1
RESULTS OF EVALUATION	3
1. Controls for Monitoring OPM’s Physical Security Risk Assessment Results Need Improving	3
APPENDIX A: Scope and Methodology	5

I. INTRODUCTION

This final evaluation report details the results from our evaluation of the U.S. Office of Personnel Management's (OPM) physical security risk assessment process. This evaluation was conducted by the OPM Office of the Inspector General (OIG), as authorized by the Inspector General Act of 1978, as amended.

OPM employees and contractor personnel conduct work at 30-leased locations involving 23 buildings throughout the United States (as of January 2020). The graph below shows the breakdown of buildings by program office.



Source: OIG Analysis - OPM Facilities as of January 2020.

Within OPM, the Security Services office under the Facilities, Security, and Emergency Management group is responsible for providing a safe and secure environment for OPM's information, personnel, and operations. The Security Services office manages OPM's physical security, information security, and insider-threat programs, including physical access control, threat assessments, and applicable national, industrial, and communications security directives.¹

Attacks on Federal facilities and their occupants substantiate the importance that agencies use risk-based methodologies to assess the physical security needs of Federal facilities.² To help Federal agencies protect and assess risks, *Executive Order 12977*, dated October 19, 1995, established the Interagency Security Committee (ISC)—a Department of Homeland Security-chaired organization comprised of 53 member agencies. The Executive Order requires executive

¹ Intranet - THEO: Team OPM Facilities, Security, and Emergency Management under Security Services.

² GAO-18-72, *Federal Facility Security: Selected Agencies should Improve Methods for Assessing and Monitoring Risk*, p. 1.

branch departments and agencies to cooperate and comply with ISC's policies and recommendations, including any standards that it sets.³ The following two bullets describe ISC's work:

- In August 2013, ISC combined six existing ISC standards—including *The Design Basis Threat, Facility Security Level Determinations for Federal Facilities*, and *Physical Security Criteria for Federal Facilities*—into a single standard, *The Risk Management Process for Federal Facilities (RMP)*.⁴
- In November 2016, the updated *RMP: An Interagency Security Committee Standard, 2nd Edition* was issued. The standard applies to all buildings and facilities in the United States occupied by Federal employees for nonmilitary activities.⁵

In its March 2014 report on *Federal Facility Security: Additional Actions Needed to Help Agencies Comply with Risk Assessment Methodology Standards*, the United States Government Accountability Office (GAO) compared OPM's risk assessment methodology to ISC's risk assessment standards outlined in the *RMP*. These standards generally require agencies to consider, at a minimum, all the undesirable events in the *RMP* and assess the threat, consequences, and vulnerability to specific undesirable events. GAO reported that OPM's risk assessment methodologies did not fully align with ISC's standards because OPM did not consider all of the undesirable events listed in the *RMP*. GAO made specific recommendations to ISC but not to OPM. Nevertheless, OPM modified its methodology to include all of the undesired events in the *RMP* and implemented a Facility Security Risk Manager Tool to address GAO's concerns and comply with ISC standards.⁶ ISC approved and certified OPM's Facility Security Risk Manager Tool on January 4, 2016.

During our evaluation, we contacted each OPM program office's point of contact to obtain their feedback on OPM's physical security risk assessment process. A majority of the respondents were satisfied with OPM's physical security risk assessment process indicating that OPM's Security Services' staff provided a timely and quality risk assessment report.

³ GAO-14-86, *Federal Facility Security: Additional Actions Needed to Help Agencies Comply with Risk Assessment Methodology Standards*, p. 1.

⁴ *Id.* p. 5.

⁵ *The Risk Management Process for Federal Facilities: An Interagency Security Committee Standard, 2nd Edition November 2016*, pp. iii and iv.

⁶ GAO-14-86, *Federal Facility Security: Additional Actions Needed to Help Agencies Comply with Risk Assessment Methodology Standards*, pp. 2-3, 9, 11, and 17.

II. RESULTS OF EVALUATION

This section details the results of our evaluation of the OPM's physical security risk assessment process. We determined that Security Services' staff uses a Facility Security Risk Manager Tool to ensure an effective and efficient process exists for performing physical security risk assessments and compliance with the ISC's standard. No limitations or challenges came to our attention that hamper its physical security risk assessment process. However, we discuss below one area in which Security Services can improve.

1. Controls for Monitoring OPM's Physical Security Risk Assessment Results Need Improving

Security Services needs to improve controls for monitoring OPM's physical security risk assessment results. Security Services' staff does not record assessment results, such as the countermeasures recommended for facilities and the status of countermeasures, in its security assessment database for the assessments it conducts. In addition, Security Services' management does not perform ongoing monitoring or separate quality control reviews to ensure program objectives are met.

GAO's *Standards for Internal Controls in the Federal Government*, September 2014, indicate that:

12.05 "Management periodically reviews policies, procedures, and related control activities for continued relevance and effectiveness in achieving the entity's objectives or addressing related risks. If there is a significant change in an entity's process, management reviews this process in a timely manner after the change to determine that the control activities are designed and implemented appropriately."⁷

16.04 "Management monitors the internal control system through ongoing monitoring and separate evaluations. Ongoing monitoring is built into the entity's operations, performed continually, and responsive to change. Separate evaluations are used periodically and may provide feedback on the effectiveness of ongoing monitoring."⁸

The internal procedures for Security Services' staff do not include data collection and analysis requirements, indicating what data they will be tracking and how they use the physical security risk assessment results. In addition, internal procedures do not indicate how ongoing monitoring or separate quality control reviews will be conducted.

⁷ GAO *Standards for Internal Controls in the Federal Government* (GAO-14-704G, September 2014), p. 56

⁸ *Id.* p. 65

Without improved monitoring and comprehensive data across the entire portfolio, Security Services is not equipped to assess program effectiveness and may leave OPM facilities' vulnerabilities unaddressed.

Recommendation 1

We recommend that Security Services' management update its internal procedures to include data collection and analysis requirements for monitoring the physical security risk assessment results.

Recommendation 2

We recommend that the Security Services' management build ongoing monitoring and quality control measures to ensure compliance and assess overall performance.

OIG Comment:

Security Services' management took immediate corrective actions to address our findings and recommendations. Security Services' management chose not to provide a response to our draft report beyond the corrective actions taken during our field work. Based on our analysis of the evidence provided for the corrective actions taken we consider both recommendations resolved and closed. No further action is required.

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.

The objectives of this evaluation were to determine: (1) the effectiveness and efficiency of OPM's Security Services' process for performing physical security risk assessments and its compliance with the ISC's standard; and (2) what limitations or challenges, if any did OPM reported facing in conducting physical security assessments and monitoring the results.

We performed this evaluation at the OPM Headquarters in Washington, D.C. between November 2019 and April 2020. Our evaluation included information and statistics from October 1, 2019 to the present.

As part of the planning phase of this evaluation, we met with Security Services' officials responsible for the management and oversight of the process to obtain an understanding of their roles, responsibilities, policies and procedures, process activities, and program statistics. We reviewed laws, regulations, and policies and procedures governing the process and examined prior reports regarding OPM's physical security risk assessment process. We also gathered supporting documentation to verify current and future operations. In addition, we obtained program data captured by Security Services' staff as of January 2020 to confirm whether the data was complete and accurate. Our results are limited by the scope and methodology that we employed to meet our evaluation objectives and not to verify Security Services' past conditions or predict future actions.

To answer our objectives, we performed the following procedures:

- Met with Security Services' officials responsible for the physical security risk assessment policies, procedures, process activities, and methodologies;
- Contacted each OPM program office's point of contact representing the Chief Information Office, Facilities, Security, and Emergency Management, Human Resources Solutions, Merit System Accountability and Compliance, Office of the Inspector General, Retirement Operations Center, and White House fellows to obtain their feedback on the process, deliverables, concerns, needs, areas for improvement, and satisfaction with Security Services;
- Evaluated Security Services' policies and procedures to ensure the ISC standards were mentioned, all of the undesirable events were considered, threat, consequences and vulnerability rating of specific undesirable events were assessed, and Security Services provided sufficient justification for facilities not assessed;

- Analyzed statistics, processes, and controls to identify trends and determine whether program data was reliable for the purpose of our objectives; and
- Compared OPM's risk assessment methodologies and supporting documentation to the ISC's risk assessment standard, as outlined in the RMP and its appendices.

We selected a judgmental sample of 3 out of 20 physical security risk assessments conducted by Security Services as of January 2020, to evaluate the effectiveness and efficiency of the process and determine whether Security Services completed assessments in accordance with the RMP. We selected the sample based on the type of facility (Federal versus commercial), the program offices involved, facility security levels, amounts of people, and location. In addition, we verified data captured for two of the three facilities not assessed to ensure it was supported by source documents and Security Services maintained justification why facilities were not assessed.

We determined the data we used to support the findings, conclusions, and recommendations was reliable. The evidence obtained provides a reasonable basis for our findings and conclusions based upon our objectives.



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