



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

Final Audit Report

**AUDIT OF THE U.S. OFFICE OF PERSONNEL MANAGEMENT'S
PERSONNEL SECURITY ADJUDICATIONS PROCESS**

Report Number 4A-CF-00-17-050

August 20, 2018

EXECUTIVE SUMMARY

Audit of the U.S. Office of Personnel Management's Personnel Security Adjudications Process

Report No. 4A-CF-00-17-050

August 20, 2018

Why Did We Conduct the Audit?

The objectives of our audit were to determine if the U.S. Office of Personnel Management's (OPM) Facilities, Security and Emergency Management Personnel Security office is (1) adjudicating background investigations cases properly and (2) employing a financial process that is effective.

What Did We Audit?

The Office of the Inspector General has completed a performance audit of OPM's personnel security adjudications process. Our audit fieldwork was conducted from November 8, 2017, through February 7, 2018, at OPM headquarters, located in Washington D.C., and the OPM Personnel Security office located in Boyers, Pennsylvania.



Michael R. Esser
Assistant Inspector General for Audits

What Did We Find?

We determined that the Personnel Security office properly adjudicated background investigations cases and that their financial process is effective; however, we identified one area for improvement that, when addressed, could have a positive impact on OPM's Personal Identity Verification process.

- **General Observation:** We determined that Facilities, Security, and Emergency Management's Security Services office's standard operating procedures were not updated, approved and disseminated timely.

In addition, OPM needs to strengthen controls over its personnel security adjudications processes in the following three areas:

1. **Training:** Training records for all 14 Adjudicators and 12 Security Assistants were not properly documented and maintained.
2. **Retention Policy:** Case files are not being destroyed in accordance with the 120-day retention policy for case files. For the 23 submitted case files that we reviewed, 8 files were eligible for destruction and destroyed an average of 56 days after the 120-day retention period. In addition, for the 23 adjudicated case files that we reviewed, 19 were eligible for destruction; however, 18 files were destroyed an average of 64 days after the 120-day retention period, and 1 file had not been destroyed.
3. **Adjudicated Cases:** For the 23 adjudicated case files that we reviewed, all 23 were missing one or more pieces of required information from the applicable forms.

ABBREVIATIONS

COR	Contracting Officer Representative
COTR	Contracting Officer Technical Representative
EPA	Environmental Protection Agency
e-QIP	Electronic Questionnaires for Investigations Processing
FSEM	Facilities, Security, and Emergency Management
GAO	U.S. Government Accountability Office
GSA	U.S. General Services Administration
NBIB	National Background Investigations Bureau
OIG	Office of the Inspector General
OPI	Office of Personnel Management’s Personnel Index
OPM	U.S. Office of Personnel Management
PIV	Personal Identity Verification

TABLE OF CONTENTS

	<u>Page</u>
EXECUTIVE SUMMARY	i
ABBREVIATIONS	ii
I. BACKGROUND	1
II. OBJECTIVES, SCOPE, AND METHODOLOGY	8
III. AUDIT FINDINGS AND RECOMMENDATIONS	12
1. General Observation	12
2. Training	13
3. Retention Policy	15
4. Adjudicated Cases	18
APPENDIX I Facilities, Security and Emergency Management’s response to the draft report, dated April 2, 2018.	
APPENDIX II Personnel Security’s additional response to the draft report, dated April 30, 2018.	
REPORT FRAUD, WASTE, AND MISMANAGEMENT	

I. BACKGROUND

This final audit report details the findings, conclusions, and recommendations resulting from our performance audit of the U.S. Office of Personnel Management's (OPM) personnel security adjudications process. The audit was performed by OPM's Office of the Inspector General (OIG), as authorized by the Inspector General Act of 1978, as amended.

During fiscal year 2016, the Facilities, Security and Contracting office was reorganized and renamed Facilities, Security and Emergency Management (FSEM). OPM's contracting functions remained with the Contracting Office, currently named the Office of Procurement Operations. FSEM is comprised of five offices, including Facilities Management, Emergency Management, Security Services, Administrative Operations, and Personnel Security.

The primary mission of the Personnel Security office is to address all of the security-related requirements of OPM's personnel, both Federal employees and contractors. They also receive work delegated by the Director of OPM for such things as obtaining higher level clearances for senior level OPM employees.

The Personnel Security office's goal is to provide timely processing of background investigation applications for new applicants and contractors through all personnel security-related areas. Areas include, but are not limited to:

- Providing position risk designations;
- Initiating the appropriate level of background investigations;
- Conducting timely re-investigations;
- Processing background investigation information for interim credentialing requirements;
- Processing background investigation information for Personal Identity Verification (PIV) credentials;
- Making final adjudicative determinations of background investigations; and
- Assisting with clearance processing, as appropriate.

POLICIES AND PROCEDURES

The workload requirements for initiating and adjudicating cases involve numerous internal Personnel Security processes and are based on various Executive Orders and Regulations establishing personnel security requirements, including the following:

- Executive Order 13467, *Reforming Process Related to Suitability for Government Employment, Fitness for Contractor Employees, and Eligibility for Access to Classified Information* - Establishes the Director of OPM as the Suitability Executive Agent responsible for developing and implementing uniform and consistent policies and procedures to ensure effective, efficient, and timely completion of investigations and adjudications for determinations of suitability and logical and physical access. Requires that background investigations and adjudications be mutually and reciprocally accepted by all agencies.
- Executive Order 13488, *Granting Reciprocity on Excepted Service and Federal Contractor Employee Fitness and Reinvestigating Individuals in Positions of Public Trust* - Requires alignment of suitability standards and reciprocity when making fitness determinations for excepted service and contractors. Agency heads shall take into account OPM guidance when establishing agency criteria that are equivalent to suitability standards established by OPM. This requirement also establishes reinvestigation authority for Public Trust¹ positions.
- Intelligence Reform and Terrorism Prevention Act of 2004 - The statutory basis for security and suitability, which reformed the intelligence community activities of the United States Government including establishing timeliness standards for security clearances. Specifically, the timeliness standard for Personnel Security to begin the initiation process is 14 days. Once NBIB completes and sends an applicant's background investigation to Personnel Security, adjudicators have 20 days to complete the adjudications process.
- Security Executive Agent Directive 4, *National Security Adjudicative Guidelines* - "... establishes the single, common adjudicative criteria for all covered individuals who require initial or continued eligibility for access to classified information or eligibility to hold a sensitive position."

¹ Public Trust is a security clearance that refers to a status granted to individuals which allows them to gain access to classified information such as state secrets and military classified data.

PROGRAM PARTICIPANTS

Personnel Security is led by the Director of Personnel Security, who oversees the following three groups, located in Boyers, Pennsylvania:

Adjudications and Clearance Processing Group: Responsible for processing work for OPM contractors and processing adjudications for OPM contract and Federal personnel. Their work includes: selecting cases for adjudications review, writing removal letters, training staff, requesting additional information from new applicants, processing clearance nominations, processing new position designations, and completing special projects as assigned by the Director of Personnel Security.

Adjudications and Compliance Group: Responsible for the initiation process, which is the first step of the adjudications process. The initiation process is a screening process that ensures the Electronic Questionnaires for Investigations Processing (e-Qip)² are completed by the new applicant. The initiation process also includes: initiating e-Qip for new applicants, making and receiving phone calls, reviewing completed information submitted by the new applicant from e-Qip, releasing the case for scheduling, fingerprinting applicants, receiving fingerprint cards from contractor employees, running reinvestigation reports, destroying OPM employee records three years after separation, and sorting incoming mail.

Special Agreements and Identity Processing Group: Responsible for processing adjudications for the U.S. General Services Administration (GSA), Environmental Protection Agency (EPA), and seven other agencies, as established by interagency agreements between OPM and the agencies. Their work includes: receiving e-Qip information from the agencies, receiving fingerprints from new applicants, and sending e-Qip information to the National Background Investigations Bureau (NBIB)³ for processing of the background investigation.

Personnel Security responsibilities are carried out by staff in several different positions, as listed below:

Supervisory Personnel Security Specialist (Adjudicator): Provides oversight of their branches' day to day activities, such as monitoring workloads; providing guidance on assignments; monitoring individual work performance; communicating workload status and

² The Electronic Questionnaires for Investigations Processing is a secure website managed by OPM that is designed to automate the common security questionnaires used to process Federal background investigations.

³ On October 1, 2016, NBIB, formerly known as Federal Investigative Services, was established as the primary service provider of government-wide background investigations.

coordinating any concerns or changes in processing with the Director of Personnel Security; and performs other duties as assigned.

Senior Personnel Security Specialist/Personnel Security Specialist (Adjudicator): Performs adjudicative case reviews for initial hires and reinvestigations; trains and guides adjudicative staff; provides status requests, processes self-reports and drafts adjudicative correspondence to subjects; performs follow-up on incomplete cases; and performs other duties as assigned. Senior Personnel Security Specialists also conduct clearance upgrades and perform position risk designations.

Security Assistant: Initiates investigations; screens and releases investigative requests; provides assistance to personnel undergoing investigations; coordinates reciprocity reviews; provides various case maintenance type duties; addresses status requests; serves as registrars for the PIV process; and performs other duties as assigned.

Contract Security Assistant: Assists with workloads associated with other Federal agencies, including screening submitted investigative paperwork; provides help desk support to other agency personnel; completes paperwork; performs case maintenance of other agency workloads; and performs other duties as assigned.

PERSONNEL SECURITY PROCESSES

Initiation Process for Federal, Contractor, and Special Agreement Employees:

The initiation process begins the background investigation process for new applicants. OPM's Employee Resources - Human Resources staff enters basic identifiers for the applicant into the Office of Personnel Management's Personnel Index (OPI)⁴ system. The Security Assistant verifies that the applicant's resumé and *Declaration for Federal Employment*, Optional Form 306,⁵ have been input into OPI. The Security Assistant then accesses the Personnel Investigations Processing Systems⁶ and emails OPM's Human Resources office to determine if the Questionnaire for Non-Sensitive Positions (SF85⁷) or Questionnaire for National Security

⁴ The Office of Personnel Management's Personnel Index system is a database that maintains security file information for OPM contractors and Federal personnel to include clearance information. Information is entered by the Personnel Security staff.

⁵ The *Declaration for Federal Employment*, Optional Form 306, is used to determine an applicant's acceptability for Federal and Federal contract employment.

⁶ The Personnel Investigations Processing System is a system used to view information, schedule initial and additional investigations, close cases, etc.

⁷ The Standard Form SF85 is primarily used for non-sensitive investigations.

Positions (SF86⁸) needs to be completed by the applicant for a background investigation. Once e-Qip is completed by the applicant it is sent to NBIB to begin the background investigation.

OPM contractors and applicants hired by a special agreement agency follow the aforementioned process, except that:

- For contractors, e-Qip initiation is completed by the Personnel Security Adjudications Branch and the Contracting Officers Representative (COR)/ Contracting Officer's Technical Representative⁹ (COTR) completes the *New Hires Initiation for Contractors and Detailees*, Form 1715. Form 1715 is then submitted to Personnel Security to begin the initiation process. If the Form 1715 is not filled out completely, it is sent back to the COR/COTR to complete. If the information is never completed, the applicant's case is not initiated.
- For special agreements, the initiation of e-Qip is completed by the requesting agency. If there is information that has not been received, the e-Qip is rejected and a letter is sent to the applicant and requesting agency.

Adjudications Process for Federal, Contractor, and Special Agreement Employees:

Once NBIB completes the applicant's background investigation, the case is considered closed and ready to be adjudicated by Personnel Security. Adjudicators make a favorable or unfavorable determination based on applicable standards identified in Title 5 of the Federal Code of Regulations, Part 731, and the National Security Adjudicative Guidelines, Homeland Security Directive 12, as well as various memorandums. Some of the information Adjudicators use to complete their review includes the case file information related to background investigations and credit and employment histories. If no serious issues are identified during the Adjudicator's review, an interim clearance is granted to the applicant who is then cleared to begin work. If the adjudicator identifies any serious issues¹⁰, an interim clearance is not granted.

The same process is followed for OPM's contractors, as well as the special agreement employees, except that:

⁸ The Standard Form SF86 is primarily used for national security investigations.

⁹ The Contracting Officers Representative / Contracting Officer's Technical Representative is a business communications liaison between the United States government and a private contractor.

¹⁰ Serious issues are issues dealing with foreign influences/preferences, sexual behavior, personal conduct, financial considerations, alcohol consumption, drug involvement, emotional/mental/personality disorders, criminal conduct, security violations, outside activities, and misuse of information technology systems.

- Once contractors are cleared for duty, an email is sent to the COR/COTR for eligibility of employment.
- For special agreement employees, all information relayed to GSA is transmitted through the NP2¹¹ portal. EPA, and other agencies with lesser workloads, can also access this portal.

Position Designation Automated Tool:

OPM's position designation automated tool is used to determine clearance levels based on job descriptions. For new position descriptions, or changes in a position description, OPM Form 1479, *Position Description*, is completed by the program office and sent to Human Resources, which assigns a position description number. Human Resources submits Form 1479, along with any position details, to the Supervisory Personnel Security Specialist in the Adjudications and Clearance Processing group, who enters information from Form 1479 and additional details into the position designation automated tool. Once all required information is accurately entered into the automated tool, the system automatically generates the appropriate security clearance tier level required for the position, based on a point system. Personnel Security emails the completed form back to Human Resources with the designation security clearance information.

Clearance Process:

*OPM's Issuance of Security Clearance*¹², Form 1680, is required to begin the process to obtain a higher level clearance than an employee presently holds. The nominee's Division or Office is responsible for providing the completed form to FSEM. The approving officials review the position description and background investigation file to ensure the employee is eligible for a higher clearance. A briefing is held between the employee and Security Services to discuss how to handle classified information and a *Non-Disclosure Agreement*¹³ Form SF312 is signed, after which a clearance is granted. The employee cannot work on projects requiring the higher clearance level until the process is completed.

PIV Process:

The PIV process is completed to provide employees with identification to access the hiring agency's building and equipment. Once an employee is cleared and approved to receive their

¹¹ NP2 is a communication portal between GSA and Personnel Security for adjudications information.

¹² The OPM Issuance of Security Clearance form is used by FSEM to certify that the employee has undergone the level of investigation required to support the requested level of clearance, based on the nature of their duties.

¹³ The Non-Disclosure Agreement Form is for briefing and debriefing an employee on classified information.

PIV card, they are sponsored by the Personnel Security office with directions on enrolling their card. Once the card is printed, the employee is given instructions on how to pick up and activate the card. The employee then activates the card with a personal identification number. PIV cards will not work until they are activated and they expire five years after issuance. After 10 years, employees must be re-photographed and re-fingerprinted.

Financial Process:

When agencies need investigative and adjudication services performed, an Inter-Agency Agreement is negotiated between a senior official from the requesting agency and the Director of OPM's Facilities, Security and Emergency Management office. Once terms are agreed upon, the Inter-Agency Agreement is signed by both parties and processed by OPM's Office of the Chief Financial Officer. The Director of Personnel Security's Administrative Operations is notified by the Chief Financial Officer that the Inter-Agency Agreement has been processed, after which work is initiated. The Inter-Agency Agreement amount is included as a receivable on OPM's financial statements, and an invoice is created for Personnel Security to obtain reimbursement as work is completed.

TRAINING

In 2012, OPM issued a memorandum titled *National Suitability Adjudicator Training Program*, which requires NBIB, formerly the Federal Investigative Services, to provide training to all Federal government adjudicators in the areas of reviewing, analyzing, evaluating, and adjudicating cases for suitability determinations. The training is taken one time and no refresher training is provided. Federal Adjudicators who have not taken the suitability training must have completed equivalent training in suitability and adjudication areas. Personnel Security also provides on-the-job training for their Security Assistants and Adjudicators.

PREVIOUS OFFICE OF THE INSPECTOR GENERAL REPORTS

In fiscal year 2004, the Office of the Inspector General conducted an audit related to background investigations. The final report for the Audit of [the] Background Investigations Process [for] OPM's Employees and Contractors¹⁴ was issued in 2007 and all recommendations have been closed.

¹⁴ OPM Office of the Inspector General Audit Report Number 4A-IS-00-04-080.

II. OBJECTIVES, SCOPE, AND METHODOLOGY

OBJECTIVES

The objectives of our audit were to determine if the Personnel Security office is (1) adjudicating background investigations cases properly and (2) employing a financial process that is effective. Specifically, our objectives were to determine if the Personnel Security office:

- Follows their documented adjudications and clearance processes;
- Complies with the Intelligence Reform and Terrorism Prevention Act timeliness standards;
- Ensures that their financial process is effective and efficient; and
- Ensures that staff are trained to perform their duties.

The recommendations included in this final report address these objectives.

SCOPE AND METHODLOGY

We conducted this performance audit in accordance with generally accepted government auditing standards as established by the Comptroller General of the United States. These standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives.

The scope of our audit covered Tiers 1¹⁵, 2¹⁶ and 4¹⁷ OPI scheduled, submitted, and adjudicated cases from October 1, 2016, through September 30, 2017, for the areas listed in the table below. Although we did not review Tier 3¹⁸ and 5¹⁹ cases, secret clearances and top secret, respectively, the adjudications process is the same for all cases.

¹⁵ Tier 1 cases are low risk (non-sensitive).

¹⁶ Tier 2 cases are moderate risk.

¹⁷ Tier 4 cases are positions of high risk.

¹⁸ Tier 3 cases are non-critical sensitive risk.

¹⁹ Tier 5 cases are position critical and special sensitive risk.

Audit Area	Total Universe
Cases Adjudicated for Federal Employees and OPM Federal Contractors	2,545
Cases Adjudicated for GSA and EPA	16,455
GSA and EPA Cases Submitted to OPM	18,022
Federal and Contractor Scheduled Cases ²⁰	1,540

In addition, the scope of our audit covered October 1, 2016, through September 30, 2017, for the following areas:

Audit Area	Total Universe
Position Designation Automated Tool Review	1,289 position designations
Financial Process	12 months of fiscal year 2017 Status of Funds reports
Training	All personnel security staff

We performed our audit fieldwork from November 8, 2017, through February 7, 2018, at OPM headquarters located in Washington, D.C. and the Personnel Security office located in Boyers, Pennsylvania.

To accomplish our audit objectives noted above, we:

- Interviewed Adjudications personnel, as necessary;

²⁰ Federal and Contractor Scheduled Cases are cases initiated by Personnel Security to be sent to NBIB for a background investigation.

- Tested scheduled, submitted, and adjudicated cases and the adjudications and clearance process to determine if Personnel Security is adhering to their policies and to determine if the financial process used is efficient;
- Reviewed training records to ensure that training requirements were met for all Adjudicators and Security Assistants; and
- Reviewed and analyzed information for the Personnel Security financial process.

In planning our work and gaining an understanding of the internal controls over the adjudications process, we considered, but did not rely on, Personnel Security's internal control structure to the extent necessary to develop our audit procedures. These procedures were analytical and substantive in nature. We gained an understanding of management procedures and controls to the extent necessary to achieve our audit objectives. The purpose of our audit was not to provide an opinion on internal controls but merely to evaluate controls over the processes included in the scope of our audit.

Our audit included such tests and analysis of Personnel Security's background investigations cases received and reviewed for the adjudications and clearance process, including timeliness standards to conduct these reviews; training for staff; and other procedures, as we considered necessary under the circumstances. The results of our tests indicate that OPM needs to strengthen controls over its personnel security adjudications processes. In addition, we identified one area for improvement that, when addressed, could have a positive impact on OPM's PIV process.

In conducting the audit, we relied to varying degrees on computer-generated data. Due to the nature of the audit, we did not verify the reliability of the data generated by the systems involved. However, while utilizing the computer-generated data during our audit, nothing came to our attention to cause us to doubt its reliability. We believe that the data was sufficient to achieve our audit objectives. We did not evaluate the effectiveness of the general application controls over computer-processed performance data.

We judgmentally selected a sample of 107 out of 38,562 Tier 1, 2, and 4 cases from October 1, 2016, through September 30, 2017, using IDEA²¹. Our sampling methodology consisted of selecting:

²¹ IDEA Case Ware Analytics is a data analysis software.

- 38 out of 2,545 cases that were adjudicated for Federal employees and OPM contractors;
- 23 out of 16,455 cases that were adjudicated for GSA and EPA;
- 23 out of 18,022 cases that were submitted from GSA and EPA; and
- 23 out of 1,540 scheduled cases for review.

In addition, we judgmentally selected a sample of 23 out of 1,289 position descriptions from the position designation automated tool from October 1, 2016, through September 30, 2017, to determine if proper clearances were assigned. Lastly, we selected all of the Personnel Security Staff to determine if they were trained properly.

The samples selected during our review were not statistically based. Consequently, the results from our samples were not projected to the populations.

III. AUDIT FINDINGS AND RECOMMENDATIONS

The sections below detail the results of our audit on OPM’s personnel security adjudications process. We determined that the Personnel Security office met the Intelligence Reform and Terrorism Prevention Act timeliness standards, properly adjudicated cases, and their financial process is effective. Issues related to standard operating procedures, training, retention policy, and adjudicated cases are outlined below.

1. **General Observation**

During our audit we identified one area of improvement, standard operating procedures, that when addressed, could have a positive impact on the PIV process.

Security Services is not ensuring that its standard operating procedures are updated, approved, and disseminated timely. During our audit, Security Services originally provided us with unsigned copies of their procedures for the completion of *New Hire Initiation for Contractors and Detailees*, Form 1715, dated August 21, 2014, and *Black Box Policy*, dated July 10, 2014. After a second request, we received the procedures for *New Hire Initiation for Contractors and Detailees*, Form 1715, dated September 20, 2017, which was not signed and disseminated to Security Services staff until December 12, 2017.

The U.S. Government Accountability Office’s (GAO) *Standards for Internal Control in the Federal Government, Principle 14*, states that “Management communicates quality information down and across reporting lines to enable personnel to perform key roles in achieving objectives, addressing risks, and supporting the internal control system.”

Recommendation 1

We recommend that Security Services implement work instructions/procedures for reviewing, approving, and disseminating policies in a timely manner.

FSEM’s Response

Security Services concurs with the recommendation and has “implemented signed instructions for reviewing, approving, and disseminating procedural changes.”

2. Training

We selected all 14 Adjudicators and 12 Security Assistants employed by Personnel Security to determine if training requirements were met. We determined that Personnel Security lacks the proper documentation to verify that all of their Adjudicators and Security assistants received the appropriate training to perform their job functions. Details of our review were provided to FSEM separate from this report. However, we found that the training files for all Adjudicators and Security Assistants did not contain one or more of the following:

Table 1: Adjudicator Training Results ²²						
Training Course	Suitability Basic Skill Standards	Suitability Core Competencies	Suitability Training Gap Analysis Worksheet	On the Job Training Checklist	Refresher	COOP Awareness
Incomplete Training Support Provided	4	4	14	14		
Missing Training Certificates					3	1

In addition, on-the-job training, which was required for the 12 Security Assistants, was either incomplete or no support was provided for the training.

The National Standard Training Requirements Parts 1 and 2, *Implementation Plan for Background Investigator and Adjudicator/Certifications of OPM's Compliance to Suitability Adjudicator National Training Standards and National Security Adjudicator Training Standards*, establishes on-the-job training standards to assist agencies in developing plans and implementing approved National Training Standards for all adjudicators responsible for determining eligibility for access to classified information or to hold a sensitive position. The training is provided to equip adjudicators, working for or on behalf of the Federal government, with the knowledge, skills, and ability to conduct national security adjudications.

²² The results in the table for each attribute tested are independent of each other.

GAO's *Standards for Internal Control in the Federal Government, Principle 4*, states that "Management establishes expectations of competence for key roles, and other roles at management's discretion, to help the entity achieve its objectives. Competence is the qualification to carry out assigned responsibilities. It requires relevant knowledge, skills, and abilities, which are gained largely from professional experience, training, and certifications."

In addition, the GAO's *Standards for Internal Control in the Federal Government, Principle 10 - Design Control Activities*, advises that "Management design control activities in response to the entity's objectives and risks to achieve an effective internal control system. Control activities are the policies, procedures, techniques, and mechanisms that enforce management's directives to achieve the entity's objectives and address related risks ... [and] clearly documents internal control ... in a manner that allows the documentation to be readily available for examination. The documentation may appear in management directives, administrative policies, or operating manuals, in either paper or electronic form. Documentation and records are properly managed and maintained."

Failing to ensure that all training completed by Adjudicators and Security Assistants is properly documented increases the potential risk that Personnel Security staff are not properly trained to handle and adjudicate personnel security cases for applicants receiving various levels of access to Federal government information, systems, and buildings.

Recommendation 2

We recommend that the Personnel Security office implement policies and procedures to ensure that all training completed by staff is properly documented and maintained.

FSEM's Response

Personnel Security concurs with the recommendation and the office's policy is to maintain forms accurately and to document training as it occurs. "FSEM-[Personnel Security] employees have been reminded of the requirements to submit copies of training certificates within 5 days of completion." Additionally, FSEM-Personnel Security will update forms identified and will be obtaining existing certificates that were identified as missing in FSEM-Personnel Security's master file of certificates.

Recommendation 3

We recommend that the Personnel Security office ensures that tracking tools used for documenting training for all Adjudicators and Security Assistants are fully completed, signed, and dated.

FSEM's Response (to Draft Recommendation)

Personnel Security concurs with the recommendation and “will continue to ensure tracking is in place going forward for all new adjudicative personnel entering into FSEM-[Personnel Security] and we will continue to track training as appropriate of established team members. FSEM-[Personnel Security] has taken the initiative of reaching out to the other entities within OPM that have similar processing requirements, for best practices. Additionally, FSEM-[Personnel Security] is in the process of developing training tracking tools that will assist with assessing training needs and better documenting completion of training milestones.”

OIG Comment:

We have revised our recommendation based on the FSEM's response to our draft report. The FSEM should respond to our revised recommendation during the audit resolution process.

3. Retention Policy

The Personnel Security office does not destroy Special Agreement²³ case files in accordance with their internal retention policy for Submitted²⁴ and Adjudicated²⁵ case files. We analyzed 23 out of 18,022 Special Agreement Submitted case files and 23 out of 16,455 Special Agreement Adjudicated case files, and relevant information documented from OPI to determine the destruction dates. Details of our review were provided to FSEM separate from this report; however, a summary of our findings are below:

²³ Special Agreement cases are received for Federal contractors from GSA, EPA, and seven other agencies who have an interagency agreement with OPM.

²⁴ Submitted cases are processed by Personnel Security for contractors, by receiving a completed *New Hires Initiation for Contractors and Detailee*, Form 1715, from the COR/COTR, and initiating e-Qip.

²⁵ Adjudicated cases are processed by Personnel Security for contractors to be cleared for duty or eligibility for employment.

Submitted and Adjudicated Case File Results					
GSA and EPA Cases	Total Universe	Total Case Files Sampled	Number of Sampled Case Files Eligible for Destruction ²⁶	Case Files Destroyed Untimely ²⁷	Case Files Not Destroyed
Submitted Cases	18,022	23	8	8	0
Adjudicated Cases	16,455	23	19	18	1

Personnel Security’s retention policy states that 120 days should be calculated from the date the case was adjudicated. After the 120th day, the case file should be destroyed and the date of destruction should be updated in OPI.

GAO’s *Standards for Internal Control in the Federal Government, Principle 12 – Implement Control Activities*, states that “Management documents in policies the internal control responsibilities of the organization. ... Management documents in policies for each unit its responsibility for an operational process’s objectives and related risks, and control activity design, implementation, and operating effectiveness.”

In addition, *Standards for Internal Control in the Federal Government, Principle 12*, also states that “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. Changes may occur in personnel, operational processes, or information technology.”

Recommendation 4

We recommend that Personnel Security ensure that staff input all relevant destruction information into OPI, including destruction dates, for all Special Agreement case files.

²⁶ Number of Sampled Case Files Eligible for Destruction is the sum of Case Files Destroyed after Retention Period plus Case Files Not Destroyed after Retention Period.

²⁷ Case File Destroyed Untimely represents a case that was destroyed after the 120th day of the retention period.

FSEM's Response

FSEM-Personnel Security does not concur with the recommendation and states “OPI is already updated with relevant destruction information to include a destruction field. Prior to the audit, FSEM-[Personnel Security] established fields in OPI that are updated with relevant destruction information to include a destruction field. Upon the entry of a destruction event in OPI, the date of action of the entry is recorded under the action summary.”

OIG Comment:

While Personnel Security provided documentation showing the destruction dates in the OPI destruction field, the fields were not updated until after we identified the issue during the audit.

Recommendation 5

We recommend that Personnel Security destroy all case files that are over the 120-day retention period, or document special circumstances in OPI.

FSEM's Response

Personnel Security concurs with the recommendation. The 120 day “goal was originally established to ensure that they had enough space availability to maintain retention files. FSEM-[Personnel Security] has modified the retention period to 180 days and has also expanded our space capacity for case in retention status ... FSEM-[Personnel Security] will continue to monitor our retention case status to meet our internal goal of 180 days. FSEM-[Personnel Security] is also reviewing current processing procedures to identify any potential improvements that may be made ultimately making the destruction process more efficient and less labor intensive.”

Recommendation 6

We recommend that Personnel Security complete monthly reviews to ensure that files are being destroyed and documented in OPI in a timely manner.

FSEM's Response

Personnel Security concurs with the recommendation and states the “Chief of the Special Agreements and Identity Processing (SAIP) Branch will conduct a designated monthly review of the Retention files space on the first of each month. Also, ongoing storage space monitoring will take place daily as SAIP personnel work with files in very close proximity to the Retention files, and they place adjudicated files in the Retention drawers daily.”

4. Adjudicated Cases

We judgmentally selected a sample of 23 out of 2,545 Adjudicated Cases for Federal employees and OPM Federal contractors from October 1, 2016, through September 30, 2017, in order to determine if Personnel Security properly followed their adjudications procedures. We determined that the information included in OPI was accurate; however, for all 23 case files reviewed, Personnel Security staff did not consistently follow procedures to complete the required information for the following forms: (1) *Issue Summary and Adjudication Recommendation*; (2) *Certification of Investigation*; (3) *INV Form 79A, Report of Agency Adjudication Action on OPM Personnel Investigations*; and (4) *U.S. Office of Personnel Management Notice of Personnel Suitability, Security, and Clearance Determinations Standard Form 06*.

Details of our review were provided to FSEM separate from this report.

Personnel Security's adjudication instructions for internal administrative handling of personnel security files provide guidance to Adjudicators on completing the necessary forms. Personnel Security created and updated some of its internal work forms, such as the *Issue Summary Adjudication and Recommendation* form, for adjudications instruction. The adjudication procedures also provide guidance to Personnel Security office staff on the case file data required to be input into OPI.

GAO's *Standards for Internal Control in the Federal Government, Principle 12 – Implement Control Activities*, states that “Management documents in policies the internal control responsibilities of the organization.” Also, “Management documents in policies for each unit its responsibility for an operational process's objectives and related risks, and control activity design, implementation, and operating effectiveness.”

GAO's *Standards for Internal Control in the Federal Government, Principle 12 – Implement Control Activities*, also states that “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. Changes may occur in personnel, operational processes, or information technology.”

The lack of current and accurate adjudication procedures creates inconsistencies in the way Personnel Security staff complete forms during the adjudications process.

Recommendation 7

We recommend that Personnel Security review and update their adjudications policies and procedures to ensure consistency with their day-to-day operations.

FSEM's Response

Personnel Security concurs with the recommendation and “strives to ensure all instructions and internal standard operating procedures are updated and note that this is an area that FSEM-[Personnel Security] was actively working to address at the time of the audit. ... Going forward, it is a goal of FSEM-[Personnel Security] to periodically review instructions and update as appropriate. We recently have hired several new staff members and as training is conducted, instructions that appear to require updates are being updated as appropriate.”

Recommendation 8

We recommend that Personnel Security communicate policies and procedures to staff prior to the implementation of any new or updated management directives.

FSEM's Response

Personnel Security concurs with the recommendation and is working to develop new or updated materials. “FSEM-[Personnel Security] routinely distributes any new or updated policies and procedures to staff either via email along with discussion in group meetings or individual meetings depending on the topic.”

APPENDIX I

Boxes in Appendix I and II represent information deleted by OIG; Not Relevant to Final Report.

April 2, 2018

MEMORANDUM FOR:

[REDACTED]
CHIEF, INTERNAL AUDITS GROUP

FROM:

DEAN HUNTER
DIRECTOR, FACILITIES, SECURITY AND EMERGENCY MANAGEMENT

SUBJECT:

Audit of the U.S. Office of Personnel Management's Personnel Security Adjudications Process, Report No. 4A-CF-00-17-050

Thank you for providing OPM the opportunity to respond to the Office of the Inspector General (OIG) draft report, Audit of the U.S. Office of Personnel Management's Personnel Security Adjudications Process, Report No. 4A-CF-00-17-050.

Responses to your recommendations including planned corrective actions, as appropriate, are provided below.

Recommendation #1: We recommend that Security Services implement work instructions/procedures for reviewing, approving, and disseminating policies in a timely manner.

We Concur

We concur with the finding that the SOP was not signed; however, we did have an SOP that documented our processes, of which the staff were aware. Since that time, we have implemented signed instructions for reviewing, approving, and disseminating procedural changes in a timely manner. [REDACTED]

Recommendation #2: We recommend that the Personnel Security office implement policies and procedures to ensure that all training completed by staff is properly documented and maintained.

We Concur

FSEM-PS agrees with the importance of having policies and procedures in place to ensure training is properly documented and maintained. FSEM-PS does maintain a local file of our training certificates, however, this is not meant to be an official tracking mechanism.

To ensure that FSEM-PS's local training file is up to date, employees have been reminded of the requirement to submit copies of training certificates within 5 days of completion for inclusion in FSEM-PS's local file. [REDACTED] Additionally, FSEM-PS management has reviewed specific findings and has obtained available certificates that were identified as missing for inclusion in our local file. Based on OIG feedback and discussion, FSEM-PS has developed a skills/duties tracking form that will be utilized for new employees documenting training requirements. [REDACTED]

Recommendation #3: We recommend that the Personnel Security office ensure that all the Adjudicators and Security Assistants have taken the appropriate training to perform their job functions.

We concur

FSEM-PS agrees with and supports the importance of Adjudicators and Security Assistants to be appropriately trained to perform their job duties and we believe that FSEM-PS has met all established training requirements. It is important to note that the OIG's report reflected that it was found that the Personnel Security Office met the Intelligence Reform and Terrorism Prevention Act timeliness standards, providing evidence that we properly adjudicated cases, and that the financial process was found to be effective and efficient. We believe these findings illustrate the success of FSEM-PS's training efforts.

FSEM Management is committed to ensuring personnel are appropriately trained. It is the policy for all new personnel to attend the Essentials of Suitability Adjudication Program (ESAP) which became the certified standard across government in August 2012. All other staff on board prior to August 2012 have either taken the ESAP course or equivalent courses that were available over the last several decades. It is also our internal policy for adjudicative personnel processing National Security cases to complete numerous National Security training courses that address a wide range of knowledge and skills sets. Additionally, FSEM-PS management and senior staff work closely with trainees and experienced staff to ensure appropriate adjudicative reviews are made in accordance with applicable Executive Orders, Regulations, memorandums, internal processing requirements, etc.

FSEM-PS will continue to ensure tracking is in place going forward for all new adjudicative personnel entering into FSEM-PS and we will continue to track training as appropriate of established team members. FSEM-PS has taken the initiative of reaching out to the other entities within OPM that have similar processing requirements, for best practices. Additionally, FSEM-PS is in the process of developing training tracking tools that will assist with assessing training needs and better documenting completion of training milestones.

In order for FSEM-PS to appropriately address this recommendation, we would like further clarification as it appears to be broad in scope and not specific as to what action items would entail.

Recommendation #4: We recommend that Personnel Security ensure that staff input all relevant destruction information into OPI, including destruction dates, for all Special Agreement case files.

We do not concur

We disagree with this finding as OPI is already updated with relevant destruction information to include a destruction field. Prior to the audit, FSEM-PS established fields in OPI that are updated with relevant destruction information to include a destruction field. Upon the entry of a destruction event in OPI, the date of action of the entry is recorded under the action summary.

Recommendation #5: We recommend that Personnel Security destroy all case files that are over the 120-day retention period, or document special circumstances in OPI.

We Concur

FSEM-PS concurs that we have not met our internal goal of destroying cases within the 120 day timeframe. This goal was originally established to ensure that we had enough space availability to maintain retention files. Since establishing this goal, FSEM-PS has modified the retention period to 180

days and has also expanded our space capacity for cases in a retention status. It is the internal goal of FSEM-PS to destroy closed case files for our Special Agreement cases within our goal; however, it is not a documented requirement within our special agreements and is not considered a priority workload. It is subject to the availability of resources to complete the process and the need for additional space in the filing cabinets. Management daily reviews this workload and assigns personnel to the workload after assessing other priority processing requirements and the need for additional space for incoming workload. It does not expose subjects to any additional undue risk when files are not destroyed within the internal goal. Cases in a retention status are noted in OPI as such and the goal date for destruction is identifiable from the date of adjudication. Additionally, the retention cases stored in the filing room are marked with dates used to establish destruction.

FSEM-PS will continue to monitor our retention case status to meet our internal goal of 180 days. FSEM-PS is also reviewing current processing procedures to identify any potential improvements that may be made ultimately making the destruction process more efficient and less labor intensive.

Recommendation #6: We recommend that Personnel Security complete monthly reviews to ensure that files are being destroyed and documented in OPI in a timely manner.

We concur

FSEM-PS agrees that monthly reviews are appropriate. FSEM-PS Management reviews this process on a daily basis and assigns workload based on assigned workload priorities, available staffing and space considerations.

Recommendation #7: We recommend that personnel Security review and update their adjudications policies and procedures to ensure consistency with their day to day operations.

We concur

FSEM-PS agrees and strives to ensure all instructions and internal standard operating procedures are updated and note that this is an area that FSEM-PS was actively working to address at the time of the audit. It is noted, however, that the report reflected that the Personnel Security Office met the Intelligence Reform and Terrorism Prevention Act timeliness standards, properly adjudicated cases, and the financial process is effective and efficient and that it was also determined that the information included in FSEM-PS's database, OPI, was accurate. OPI is considered the "official" site for the internal tracking of security file processing.

Over the last several years, FSEM-PS has been moving to an electronic platform for the processing of case work. FSEM-PS utilizes OPI to track the various operations associated with investigative processing and security file maintenance.

Going forward, it is a goal of FSEM-PS to periodically review instructions and update as appropriate. We recently have hired several new staff members and as training is conducted, instructions that appear to require updates are being updated as appropriate.

Recommendation #8: We recommend that Personnel Security communicate policies and procedures to staff prior to the implementation of any new or updated management directives.

We concur

FSEM-PS fully supports the need to communicate policies and procedures to staff. FSEM-PS routinely distributes any new or updated policies and procedures to staff either via email along with discussion in group meetings or individual meetings depending on the topic at the time they become available. In most instances, management of FSEM-PS meet with staff and work hand in hand to develop any new or updated materials, with senior staff members frequently writing the updates or initiating the development of updates or procedures. Any updates are distributed via email and are entered into FSEM-PS's instruction files.

**Deleted by OIG
Not relevant to Final Report**

I appreciate the opportunity to respond to this draft report. If you have any questions regarding our response, please contact Dean Hunter, Director of Facilities, Security and Emergency Management at [REDACTED] or via email at [REDACTED]@OPM.Gov or [REDACTED], Director, Personnel Security, Facilities, Security and Emergency Management at [REDACTED] or via email at [REDACTED]@OPM.Gov.

APPENDIX II

From: [REDACTED]
Sent: Monday, April 30, 2018 9:01 AM
To: [REDACTED]
Cc: Hunter, Dean S.
Subject: RE: Draft Report
Attachments: Destruction of Adjudicated Files - REVISED 4-27-18.docx

**Deleted by OIG
Not Relevant to Final Report**

Retention Space Monitoring

The Chief of the Special Agreements and Identity Processing (SAIP) Branch will conduct a designated monthly review of the Retention files space on the first of each month. Also, ongoing storage space monitoring will take place daily as SAIP personnel work with files in very close proximity to the Retention files and they place adjudicated files in the Retention drawers daily. If it's noticed that the files seem to be approaching the maximum described limit within these instructions, the SAIP Chief will be notified so that attention can be given to resolve the storage concern and continue to meet our specified criteria.

Deleted by OIG – Not Relevant to Final Report

[REDACTED]
[Director, Personnel Security](#)
[Facilities, Security & Emergency Management](#)



Report Fraud, Waste, and Mismanagement

Fraud, waste, and mismanagement in 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