UNITED STATES GOVERNMENT
National Labor Relations Board
Office of Inspector General

Personnel Security

Report No. OIG-AMR-73-15-01

February 3, 2015

CONTENTS

National Labor Relations Board
Office of Inspector General

EXECUTIVE SUMMARY

Agencies are required to establish and maintain an effective personnel security program. At the National Labor Relations Board, the Security Branch Chief, as the Agency's Chief Security Officer, is responsible for planning, directing, and coordinating the personnel security program. We conducted this audit to determine whether the Security Branch's internal controls for suitability investigations are followed and whether the appropriate suitability investigations are conducted.

We generally found that the Security Branch does not have sufficient internal controls. We determined that the system of records notice for the Security Branch's personnel security records is not accurate and our inventory of personnel security files found that there were missing and incomplete files. We also determined that the data in the Security Branch's database was unreliable. Our testing of the Security Branch's compliance with its own procedures generally found that the Security Branch is not functioning as intended. We found that a significant number of employees did not have appropriate documentation of a pre-employment check, initial suitability investigations, or suitability investigations at the time of reassignments or promotions. We also determined that, as of April 30, 2014, 912 suitability investigations needed to be completed, at an expense of $1,399,070, to bring the Agency's personnel security function into compliance with OPM's reinvestigation requirements.

The Director of Administration reviewed the draft audit report and provided comments dated January 28, 2015. After the Inspector General questioned the information provided in those comments and provided the Director of Administration with a response, the Director submitted revised comments dated January 30, 2015. The revised comments state that management generally agreed with the report's assessment of the Security Branch, that recommendations 2a through 2l would be implemented, and described the particular corrective actions to be taken. The revised comments are included as an Appendix.

BACKGROUND

Executive Order 10450, Security Requirements for Government Employment, dated April 27, 1953, requires that agencies establish and maintain an effective personnel security program to insure that the employment and retention in employment of any civilian officer or employee within the agency is clearly consistent with the interests of the national security. It also establishes that the appointment of each employee shall be made subject to a investigation, the scope of which shall be determined according to the degree of adverse effect the employee in the position could bring about on the national security, but in no event shall the investigation be less than a national agency check and written inquiries to appropriate local law-enforcement agencies, former employers and supervisors, references, and schools attended by the person under investigation. The investigations are used for making determinations of suitability and for taking suitability actions and are collectively referred to in this report as "suitability investigations."

If an employee is selected for or reassigned to a position within the Agency that is at a higher risk level than that previously occupied, the employee must meet the suitability investigative requirements of the new position. Additionally, employees in positions designated Special-Sensitive or Critical-Sensitive shall be subject to periodic reinvestigation every 5 years. Employees in public trust positions are also required to be reinvestigated at least once every 5 years.

The personnel security function is performed by the Security Branch, a component of the Division of Administration. The Security Branch Chief, as the Agency's Chief Security Officer, is responsible for planning, directing, and coordinating the personnel security program. This includes pre-employment checks, sensitive and non-sensitive suitability investigations, and the issuance of security clearances and official identification cards.

OBJECTIVE, SCOPE, AND METHODOLOGY

The audit's objectives were to review the Security Branch's internal controls used in the processing of suitability investigations and to determine whether those controls are

being followed. We also determined whether the appropriate suitability investigations were being done for Agency employees.

For determining whether the Security Branch maintained appropriate suitability investigative files (files), whether the files were in proper order, and whether the database was accurate, our scope was the files and data for employees as of September 30, 2013. Our scope for reviewing the Security Branch's processes was transactions that occurred in Fiscal Year (FY) 2009 through FY 2013. For testing the current status of an employee's suitability investigation and the impact of reinvestigations on future years' budgets, our scope was the investigative status as of April 30, 2014. Except for the inventory of files, we excluded activities related to the Office of Inspector General (OIG) and Presidential appointees. We conducted this audit at National Labor Relations Board (NLRB or Agency) Headquarters in Washington, D.C.

We reviewed the Code of Federal Regulations and Governmentwide guidance on personnel security issued by the Office of Personnel Management (OPM); the Office of Management and Budget (OMB); the Government Accountability Office (GAO); the National Archives and Records Administration; and the National Institute of Standards and Technology. We interviewed Agency officials to identify the internal procedures and controls maintained by the Security Branch. We obtained and reviewed the Agency's policies and procedures and the Security Branch's internal procedural documents used as guidance.

We obtained from the Federal Personnel Payroll System (FPPS) a listing of all employees employed by the Agency; a listing of new hires, including students; a listing of employees who were transferred from another Federal agency; a listing of separated employees; and a listing of promoted and reassigned employees for the period of October 2008 to February 2014. We also obtained the Security Branch's database, Position Designation List, and mail log.

We inventoried the files to determine whether the Security Branch maintains a security file for the Agency's current employees as of September 30, 2013. We evaluated whether the Security Branch had sufficient internal controls in place to conduct suitability investigations. We tested whether the

personnel security execution process complies with Governmentwide regulations and guidance. We analyzed the potential impact that reinvestigations could have on the Agency's future budgetary resources.

We tested a statistical sample of Agency employees to determine whether the Security database was accurate, whether the investigative files contained documentation for the four basic elements of the security process, and whether employees underwent the appropriate suitability investigation. A statistical sample was used because of the large number of Agency employees. The Agency had 1,594 employees as of September 30, 2013. A 90 percent confidence rate resulted in a sample size of 77 items. We also tested a statistical sample of Agency positions to determine the accuracy of the Position Designation List. A statistical sample was used because of the large number of Agency positions on the Position Designation List. The Position Designation List had 860 positions. A 90 percent confidence rate resulted in a sample size of 76 items. The 90 percent confidence level is consistent with GAO guidance and our expected deviation rate. The results of our tests can be projected to the population.

We conducted this performance audit in accordance with generally accepted government auditing standards during the period January 2014 through December 2014. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

INTERNAL CONTROLS

Internal control is a significant part of managing an organization. It comprises the plans, methods, and procedures used to meet missions, goals, and objectives. Internal control also serves as the first line of defense in safeguarding assets and preventing and detecting errors and fraud. Control activities occur at all levels and functions of the entity. They include a wide range of diverse activities such as approvals, authorizations, verifications, maintenance of security, and the creation and maintenance

of related records which provide evidence of execution of these activities as well as appropriate documentation.

We used the Internal Control Management Evaluation Tool, issued by GAO, to evaluate the internal controls of the Security Branch. The results are as follows:

GAO Evaluation Tool	OIG Determination	OIG Observation
The control activities identified as necessary are in place and being applied. Consider the following:		
Control activities described in policy and procedures manuals are actually applied and applied properly.	No	There was a lack of documentation of significant events in employees' file. The Security Branch was missing employee files. Additional issues are detailed in remainder of the report.
Supervisory personnel review the functioning of established control activities and remain alert for instances in which excessive control activities should be streamlined.	No	One Personnel Security Specialist was not filing the documents reflecting the significant events appropriately. The documents contained Personally Identifiable Information and were not properly safeguarded. The Security Branch lacked a uniform method to track work assigned to the Personnel Security Specialists. There was no supervisory review of investigations, unless an issue was brought to the attention of the Security Branch Chief.
Timely action is taken on exceptions, implementation problems, or information that requires follow-up.	No	We observed a lack of a process that would detect exceptions to the Internal Control procedures.

GAO Evaluation Tool	OIG Determination	OIG Observation
Control activities are regularly evaluated to ensure that they are still appropriate and working as intended.	No	The Security Branch did not have a review process. A process was established after the audit was initiated.
Information Processing – The agency employs a variety of control activities suited to information processing systems to ensure accuracy and completeness. Consider the following:		
Edit checks are used in controlling data entry.	No	No edit checks were implemented as part of the Security Branch database. Data fields in the Security Branch database had error rates that exceeded the tolerable error rate of 10 percent.
Access to data, files, and programs is appropriately controlled.	Yes	The programs are password-protected. Access to paper files is limited to Security Branch personnel.
Physical Control Over Vulnerable Assets – The agency employs physical control to secure and safeguard vulnerable assets. Consider the following:		
Physical safeguarding policies and procedures have been developed, implemented, and communicated to all employees.	Yes	The Security Branch has a method to restrict access to Security Branch personnel.
The agency has developed a disaster recovery plan, which is regularly updated and communicated to employees.	Yes	Safeguarding vital documents is under the Continuity of Operations Plan for the Agency.
Segregation of Duties – Key duties and responsibilities are divided or segregated among different people to reduce the risk of error, waste, or fraud. Consider the following:		
No one individual is allowed to control all key aspects of a transaction or event.	No	A Personnel Security Specialist is able to designate a position risk/sensitivity

GAO Evaluation Tool	OIG Determination	OIG Observation
Responsibilities and duties involving transactions and events are separated among different employees with respect to authorization, approval, processing and recording, making payments or receiving funds, review and auditing, and the custodial functions and handling of related assets.	No	level for a position. The Personnel Security Specialist then controls the investigation from initiating the Electronic Questionnaire for Investigations Processing request to making the suitability decision. The Security Branch Chief is consulted only for negative suitability issues. The entire process can be controlled by one employee within one branch.
Duties are assigned systematically to a number of individuals to ensure that effective checks and balances exist.	No	
Recording of Transactions and Events – Transactions and other significant events are properly classified and promptly recorded. Consider the following:		
Transactions and events are appropriately classified and promptly recorded so that they maintain their relevance, value, and usefulness to management in controlling operations and making decisions.	No	The Access database did not contain reliable information. Employee files are missing. A significant amount of files lacked a complete record. Additional issues are detailed below.
Proper classification and recording take place throughout the entire life cycle of each transaction or event, including authorization, initiation, processing, and final classification in summary records.	No	

GAO Evaluation Tool	OIG Determination	OIG Observation
Proper classification of transactions and events includes appropriate organization and format of information on original documents (hardcopy paper or electronic) and summary records from which reports and statements are prepared.	No	
Access Restrictions to and Accountability for Resources and Records – Access to resources and records is limited and accountability for their custody is assigned. Consider the following:		
The risk of unauthorized use or loss is controlled by restricting access to resources and records only to authorized personnel	No	Although the files were protected from unauthorized access, there were no controls in place to provide accountability for the files among the Security Branch personnel, and there were no controls in place to detect the unauthorized hoarding of 599 documents by a Personnel Security Specialist.
Accountability for resources and records custody and use is assigned to specific individuals.	No	
Periodic comparison of resources with the recorded accountability is made to determine if the two agree, and differences are examined.	No	The Security Branch does not have a process to compare the data with source documents or any reports generated to check the validity of electronic data.
How frequently actual resources are compared to records and the degree of access restrictions are functions of the vulnerability of the resource to the risk of errors, fraud, waste, misuse, theft, or unauthorized alteration.	No	

GAO Evaluation Tool	OIG Determination	OIG Observation
Documentation – Internal Control and all transactions and other significant events are clearly documented. Consider the following:		
Written documentation exists covering the agency's internal control structure and for all significant transactions and events.	Yes	The Agency has revised policies, dated May 15, 2013, and an internal procedural document for pre-employment screening, requesting investigations, adjudicating investigations, adjudicating Personal Identity Verification (PIV) card credentials, and processing separations.
The documentation is readily available for examination.	Yes	
The documentation for internal control includes identification of the agency's activity-level functions and related objectives and control activities and appears in management directives, administrative policies, accounting manuals, and other such manuals.	No	The internal control documentation does not include supervisory control activities and does not create segregation of duties.
Documentation for internal control includes documentation describing and covering automated information systems, data collection and handling, and the specifics of general and application control related to such systems.	No	The Security Branch does not have any written documentation on the use of its database.

GAO Evaluation Tool	OIG Determination	OIG Observation
Documentation of transactions and other significant events is complete and accurate and facilitates tracing the transaction or event and related information from authorization and initiation, through its processing, to after it is completed.	No	The employee files lacked documentation of the pre-employment check, investigation reports, fingerprint check results, and adjudication dates. We observed that each Personnel Security Specialist has their own style of documenting events. Data fields in the Security Branch database had error rates that exceeded the tolerable error rate of 10 percent.
All documentation and records are properly managed, maintained, and periodically updated	No	
Documentation, whether in paper or electronic form, is useful to managers in controlling their operations and to any others involved in evaluating or analyzing operations.	No	
Authorization Control		
Source documents are controlled and require authorization. Consider the following:		
Key source documents require authorizing signatures.	No	The Security Branch Chief reviews files only when they are brought to his attention due to information that may result in an adverse suitability determination. We observed that the decisional documents used to enter data were not reviewed and signed by a supervisor.
Supervisory or independent review of data occurs before it is entered into application system	No	
Completeness Control		
All authorized transactions are entered into and processed by the computer.	No	Data fields in the Security Branch database had error rates that exceeded the tolerable error rate of 10 percent.

GAO Evaluation Tool	OIG Determination	OIG Observation
Reconciliations are performed to verify data completeness.	No	The Security Branch has no procedure for data reconciliations.
Accuracy Control		
The agency's data entry design features contribute to data accuracy.	No	Data fields in the Security Branch database had error rates that exceeded the tolerable error rate of 10 percent.
Data validation and editing are performed to identify erroneous data.	No	
Erroneous data are captured, reported, investigated, and promptly corrected.	No	
Output reports are reviewed to help maintain data accuracy and validity.	No	
Management has a strategy to ensure that ongoing monitoring is effective and will trigger separate evaluations where problems are identified or systems are critical and testing is periodically desirable. Consider the following:		
The monitoring strategy includes methods to emphasize to program managers their responsibility for internal control and their duties to regularly monitor the effectiveness of control activities.	No	Due to our determination that there is no segregation of duties and that the Security Branch Chief is not actively reviewing the work of subordinates, we found that there was no monitoring strategy in place.
The strategy includes a plan for periodic evaluation of control activities for critical operational and mission support systems.	No	Agency Policy and internal procedural documents do not include a plan for periodic evaluation.

The Director of Administration is responsible for an effective internal control system. As part of that responsibility, the Director of Administration sets the Security Branch's objectives, implements controls, and evaluates the internal control system. Internal control, however, does not guarantee the success of any program or the absence of

waste, fraud, and mismanagement, but it is a means of managing risk.

Because of the extent of the lack of internal controls that we identified, this report provides a series of targeted recommendations that are intended to remediate the internal control deficiencies. Those recommendations are listed throughout the report as 2a through 2l. Our audit and the recommendations, however, are not a substitute for the Director of Administration's responsibility for an effective internal control system. We therefore are making an alternate overarching recommendation that can be implemented in lieu of the specific targeted recommendations 2a through 2l.

Recommendation

1. We recommend that the Director of Administration reorganize the Security Branch to ensure the following:

   A set of internal control activities that ensure that the Security Branch fulfills the personnel security function in compliance with Governmentwide regulations and policies;

   A method to monitor the Security Branch's compliance with and the effectiveness of the internal control activities; and

   The Security Branch is appropriately staffed and funded to fulfill its mission.

Management Comment

The Director of Administration elected to implement recommendations 2a through 21 and take steps to address recommendation 1.

COMPLIANCE WITH POLICIES AND PROCEDURES

Files

File Maintenance

The Security Branch is responsible for maintaining the personnel security records for the current and former employees, applicants, contractor personnel, and student

volunteers. The Security Branch's records include both paper files and an electronic database.

The Security Branch's records are identified as a Privacy Act system of records. Each Privacy Act system of records is required to have a system of records notice that has been published in the Federal Register. A system of records notice is also required to be published in the Federal Register any time that there is a revision to the system. Our review of the system of records notice for the Security Branch's personnel security records determined that the notice is not accurate. The notice does not list all of the categories of individuals covered by the system, it does not provide notice that the system of records includes an electronic database, and it does not accurately describe the storage of the files or the access controls.

The Security Branch stored most of the files in a large filing cabinet system with rotating shelves. The files were generally kept in alphabetical order and grouped by employees, students, contractors, and separated employees. Because the filing system could not accommodate all of the files, a second grouping of files was stored in cardboard boxes and identified as employees who separated in FY 2011. Individual employees within the Security Branch also kept files in his or her office. It was explained to the OIG that the files in the individual offices were generally for active suitability investigations that were assigned to the Security Branch employee. We observed that access to the Security Branch and its file room was controlled. We also observed, however, that there were no controls in place to track the files within the Security Branch.

To determine if the Security Branch's controls over the files were operating in a satisfactory manner, we conducted an inventory of the files. Using information from FPPS, we determined that the Security Branch should have had 1,604 files for current employees as of September 30, 2013. During our initial inventory, we located 1,445 files. Following that inventory, on April 30, 2014, we provided the Security Branch with a list of 159 employee names for whom we could not locate a file. Between June 6, 2014 and July 3, 2014, an additional 38 files were located. As a result of our inventory, we determined that the Security Branch was missing files for 121 employees.

For the employees with missing files, we looked at the year the employee was hired to determine if there was a pattern. The table below shows that most of the missing files were for employees who were hired prior to 1990:

Year of Accession	Number of Missing Files
on/after the Year 2010	4
2005-2009	1
2000-2004	5
1995-1999	0
1990-1994	3
1985-1989	45
1980-1984	30
1975-1979	22
1970-1974	10
Before 1970	1

Recommendations

2a. We recommend that the Security Branch update the system of record notice for the personnel security files.

2b. We recommend that the Security Branch develop an internal control to systematically inventory its files, including a method to track files within the Security Branch.

The corrective action related to the missing files is addressed as part of the recommendations related to the reinvestigation process that is discussed below.

Hard Copy File Errors

Correct Name

When an employee requests to change his or her name in the official personnel records, the Security Branch receives a notification of the resulting personnel action that effectuates the change. The records in FPPS begin in September 2002. From that date through September 30, 2013, 117 current employees had his or her name changed. For those employees, we found that 50 files were incorrectly labeled with the employee's former name. We also observed that

there were 24 files that were identified by a name that did not match the official personnel records.

Misfiled

During our inventory of files, we observed that 60 current employee files were misfiled either with student or separated employees. Among those 60 files, were 28 of the files that did not have the correct name.

We also observed that there were 71 files among the current employee files that did not belong to a current employee as of September 30, 2013. After the initial inventory, we returned to the Security Branch to obtain additional information regarding the 71 files. At that time, the Security Branch could not locate two of the files. The descriptions of the remaining 69 files are detailed in the table below:

Status of Individual	**Number of Files**
Separated employees	49
Students	6
Contractors	10
Applicants	1
Insufficient information in the file to make a determination	3

In addition to the misplaced files, there were two groups of two employees that had identical first and last names. Although there were two employees in each group, there was only one file for each name, and it contained documentation for both employees. There were also four employees who had multiple files.

Recommendation

2c. We recommend that the Security Branch develop a logical filing system. As part of this recommendation, the Security Branch should take corrective action to address the finding regarding the misidentified files discussed above.

Records Retention and Destruction

The retention and destruction of files are governed by General Records Schedule 18, Security and Protective Service Records. That schedule requires the destruction of a

file when an individual dies or not later than 5 years after the employee's separation or transfer. The Security Branch's practice is to maintain the files for 5 years in accordance with the maximum time allowed by the records retention schedule.

When we began the audit, Security Branch personnel were in the process of destroying the FY 2009 files. For the purpose of testing compliance with the records retention schedule and the Security Branch's practice, we reviewed files for employees separated beginning in FY 2010 through FY 2013. Using data from FPPS, we identified 600 employees who separated during that period.

We found the following:

- The Security Branch improperly maintained files for four deceased employees;
- We were unable to locate 106 files; and
- There were 124 files for individuals that were not listed as an employee who separated during the last 5 fiscal years or listed as a current employee.

Recommendation

2d. We recommend that the Director of Administration review the records retention schedule for Personnel Security Records and develop a written records retention policy for the Security Branch.

Record Maintenance

The GAO standards require that all transactions and other significant events need to be clearly documented, and the documentation should be readily available for examination.

Documents

The Agency's Personnel Security Files, System of Records (NLRB-17) states that the Security Branch maintains Federal agency name checks, police checks, investigative summaries reflecting the reasoning behind suitability recommendations, and other relevant inquiries for current employees, former employees, and applicants.

We obtained a statistical random sample of 77 employees and reviewed the security files for those employees to determine if the file contained documentation of four basic elements of the security process. The table below shows the results of the review:

Category	Found	Not Found
Pre-employment check decision	65	12
Finger print/Name check results	36	41
Suitability investigation	69	8
Suitability decision (Adjudication results)	58	19

For the 58 employees who had a suitability decision documented in the file, 6 did not have a completed suitability investigation report. We also observed that for one of the employees without a suitability investigation, there was no documentation that the Security Branch responded to OPM's request for additional information.

Database Reliability

The Security Branch maintains a database to record information related to suitability investigations. To determine the reliability of the database, we selected a random sample of 77 individual records in the database and determined whether the database information matched the information in the file. The table below shows the results of the testing.

Database Field	Data Matches	Data Does Not Match
Pre-employment check date	39.0%	61.0%
Employee position sensitive category	64.9%	35.1%
Fingerprint /Name check completion date	18.2%	81.8%
Suitability investigation initiation date	49.4%	50.6%
Suitability investigation completion date	48.1%	51.9%
Suitability investigation adjudication date	35.1%	64.9%

Based on our testing, we determined that the security database is unreliable. In reaching this determination, we used a tolerable error rate of 10 percent, which is consistent with GAO guidance.
The types of errors are shown in the table below.

Database Field	Does not Match	Data Only in the File	Data only in the Database	No Data in either	Total
Pre-employment check date	19.5%	26.0%	6.5%	9.1%	61.0%
Employee position sensitivity category	24.7%	6.5%	1.3%	2.6%	35.1%
Name/Fingerprint check completion date	3.9%	27.3%	1.3%	49.4%	81.8%
Suitability investigation initiation date	18.2%	16.9%	2.6%	13.0%	50.6%
Suitability investigation completion date	27.3%	16.9%	5.2%	2.6%	51.9%
Suitability investigation adjudication date	7.8%	16.9%	20.8%	19.5%	64.9%

Recommendation

2e. We recommend that the Security Branch develop a process to accurately input data into its database that includes a quality control process.

Personnel Security Process

The Agency's personnel security process includes the following steps: risk designation; pre-employment check; suitability investigation; reporting suitability decision to OPM; issuance of PIV card; separation; and promotions and reassignments.

Risk Designation

The Agency's Security Branch procedures state that the proper position designation is the foundation of an effective and consistent suitability and personnel security program. Governmentwide regulations require that every "covered position" should be designated at a high, moderate, or low risk level. Covered positions include competitive service positions, excepted service positions that allow the incumbent employee to be converted to a competitive service

position without competition, and career Senior Executive Service positions. High and moderate risk level positions are considered "public trust" positions. All positions subject to investigation must also receive a sensitivity designation of Special-Sensitive, Critical-Sensitive, or Noncritical-Sensitive, when appropriate.

The Security Branch maintains a Position Designation List that contains, among other things, the position title, grade, description number, risk level, the type of suitability investigation that is required for the position, and the suitability investigation form that is to be used to initiate the suitability investigation. There are 860 positions listed in the Position Designation List. Not every Agency employee occupies a unique position on the list.

We reviewed the Position Designation List and found the following issues:

- Eight positions did not specify the position's risk level, sensitivity level, or the type of investigation required;

- None of the 47 positions considered by the Security Branch to be a "national security position" and designated with a sensitivity level, including 19 career Senior Executive Service positions, were categorized at a high, medium, or low risk level; and

- None of the 527 covered positions designated as high, moderate, or low risk were also designated with a sensitivity level.

We also observed that excepted service positions for which the incumbent employee could not be converted to a competitive status position were treated as if they were a covered position and designated as a high, medium, or low risk position. These positions were generally not designated with a sensitivity level.

Prior to FY 2011, the Security Branch used a manual position designation form to determine the personnel security designation for a position. To determine the accuracy of the Position Designation List, we reviewed a statistical random sample of 76 positions from the list with a risk level that was determined using the position designation

form and compared the forms to the Position Designation List. The results are shown in the tables below:

	Yes	No
Position Sensitivity Designation Form Found	60	16

	Yes	No
Position Designation List Risk Level Matches with Position Sensitivity Designation Form Risk Level	59	1

In order to ensure a systematic, dependable, and uniform way of making a position designation, OPM created the Position Designation Automated Tool (PDT). The Security Branch began using the PDT in FY 2011. We also reviewed the 14 positions that had a risk level that was determined using the PDT. We found that for one position the Position Designation List stated a lower level of investigation than what was required by using the PDT.

Because the Position Designation List is the source document to determine which investigation is required for a new hire, promoted employee, and reassigned employee, we compared the risk level in the Position Designation List to the risk level assigned in FPPS for current employees as of the end of FY 2013. The chart below shows the results of the testing:

	Position Designation List Matches FPPS		Positions Listed in FPPS but not in Position Designation List
	Yes	No	
Number of employees	1,163	325	106

We also observed that, in FPPS, the employees in the same position type did not always have the same risk level.

Recommendations

2f. We recommend that the Security Branch create a new Position Designation List that corrects the identified errors.

2g. We recommend the Division of Administration ensures that the Position Designation List matches FPPS.

Pre-employment Check

Once a hiring decision is made, the Security Branch conducts a pre-employment check on the new appointee. The pre-employment check includes a review of the security questionnaires, relevant additional forms, and the Federal Bureau of Investigations (FBI) Fingerprint/Name Check results.

During FY 2012 and FY 2013, there were 199 appointments, consisting of 175 new hires and 24 transfers. We reviewed the files for the new hires and transferred employees to determine if a pre-employment check was completed before the employee entered on duty. The table below shows the results:

Category	Yes	No	No Documentation
New Hires	151	3	21
Transferred Employees	19	2	3

Recommendation

2h. We recommend that the Security Branch develop policies and procedures to ensure that a pre-employment check is conducted prior to an individual entering on duty.

Suitability Investigations

Newly Hired Employees

Except for Critical-Sensitive and Special-Sensitive positions, a suitability investigation must be initiated within 14 days for an employee placed in a permanent position or an appointment exceeding 180 days.

During FY 2012 and FY 2013, there were 144 new employees who were either placed in a permanent position or had an appointment exceeding 180 days. We first reviewed the employee's file to determine whether it contained documentation of a suitability investigation. Our results are shown in the table below:

	Yes	No
Suitability investigation in file	109	35

We observed that the files for five employees who did not have documentation of a suitability investigation were also among the employees who lacked documentation of a pre-employment check.

For the 109 newly hired employees that had documentation of a suitability investigation in the file, we then reviewed the documentation to determine if the suitability investigation was initiated within 14 days of placement. The results are shown in table below:

Suitability investigation initiated within 14 days of placement	**Yes**	**No**	**Initiation Date not Documented**
	77	3	29

Transferred Employees

Agencies making suitability determinations shall grant reciprocal recognition to a prior favorable fitness or suitability determination when (i) the gaining agency uses criteria for making fitness determinations equivalent to suitability standards established by OPM; (ii) the prior favorable fitness or suitability determination was based on criteria equivalent to suitability standards established by OPM; and (iii) the individual has had no break in employment since the favorable determination was made.

During FY 2012 and FY 2013, there were 24 employees who transferred from another Federal agency. Of those 24 employees:

- 10 were in a position at the same risk level as his or her prior position and had a current suitability investigation. For all 10 of those employees, the Security Branch granted reciprocal recognition to the prior favorable suitability determination. For 1 of the 10 employees, the Security Branch also initiated and completed a suitability investigation despite having already granted reciprocal recognition to the prior favorable suitability determination.

- The remaining 14 transferred employees required a new suitability investigation. We found that the Security Branch initiated 7 suitability investigations

and that there was no documentation for 7 transferred employees that a suitability investigation was initiated.

Appropriate Suitability Investigation Completed

Based upon the risk level assigned to a position, one of four levels of suitability investigation is completed. The lowest level suitability investigation is a National Agency Check and Inquiries (NACI); the next in-depth is a Moderate Risk Background Investigation (MBI); the third level is a Background Investigation (BI); and the fourth level and most in-depth is a Single Scope Background Investigation (SSBI).

To determine whether the appropriate suitability investigation was completed, we selected a statistical sample of 77 employees and reviewed documentation of the employee's suitability investigation. Because the positions for three employees were not listed on the Position Designation List, we were unable to determine whether the appropriate suitability investigation was completed. For the remaining 74 employees, the results are shown in the table below:

			No			
Appropriate suitability investigations completed	**Yes**		**Incorrect Investigation**	**Lack of Proper Documentation**	**Missing Files / Investigations**	**Total**
	51		11	2	10	23

Given the results of statistical sample above, we reviewed the appropriateness of the suitability investigations for the employees requiring reinvestigation as of April 30, 2014. The following table provides detailed information on our finding:

Type of Suitability Investigation	Number of Employees	Documentation of Correct Suitability Investigations	
		Number of Investigations	Percent
MBI	635	480	76%
BI	297	205	69%
SSBI	37	21	57%
Total	969	706	73%

The table below shows the type of errors found during our review of the file and the required suitability investigations:

Type of Error	Suitability Investigation Required			Total
	MBI	BI	SSBI	
Incorrect investigations	40	59	11	110
Lack of proper documentation	45	23	4	72
Missing files / investigations	70	10	1	81
Total	155	92	16	263

For employees with an incorrect suitability investigation, we also determined when the error occurred:

Year Investigation Completed	Number of Investigations
Prior to 1991	20
1991 - 2000	50
2001 - 2005	28
2006 - 2010	11
2011 to Present	1

Recommendation

2i. We recommend that the Security Branch develop policies and procedures to ensure that an employee undergoes the appropriate suitability investigation.

Reporting the Suitability Decision to OPM

Except for non-sensitive low risk positions in which no potential derogatory information exists, OPM requires that agencies make a suitability determination based upon the information in the investigation. The results of the suitability determination must be reported to OPM within 90 days of receiving the completed investigation.

There were 114 new employees who during FY 2012 and FY 2013 had a suitability investigation requiring that OPM be provided with a suitability determination. We calculated the number of days the Security Branch took to report the suitability determination to OPM. The results are shown in the table below:

Number of Days to Report to OPM	Number of Suitability Investigations
Less than or equal to 90 days	86
More than 90 days	18
Date not documented	10

Issuance of PIV Card

Homeland Security Presidential Directive 12 established the requirements for a common identification standard for identity credentials issued by Federal departments and agencies to Federal employees for gaining physical access to Federally controlled facilities and logical access to Federally controlled information systems. The credential is commonly referred to as a "PIV card." OPM's implementing guidance on the issuance of the PIV card requires that the Agency initiate a suitability investigation (NACI or at least equivalent) and ensure the FBI fingerprint check is completed before issuing the PIV card.

The Agency uses the USA Access Program to issue PIV cards. We attempted to obtain the issuance data generated by the USA Access Program for 149 PIV cards issued to newly hired employees during FY 2012 and 2013, including employees who had appointments of less than 180 days. Because of the manner in which the issuance data is maintained by the USA Access Program, we could only obtain accurate PIV card issuance dates for 113 PIV cards issued to newly hired employees.

We reviewed the files of the 113 newly hired employees who had accurate data in the USA Access Program to determine if the file contained documentation that the fingerprints check and the initiation of a suitability investigation were completed prior to the issuance of the PIV card. The results are shown in table below:

Found documentation of fingerprint check and initiation of suitability investigation prior to issuance of PIV card	**Yes**	**No**
	68	45

Recommendation

2j. We recommend that the Security Branch develop policies and procedures to ensure that it does not issue a PIV card until a fingerprint check is conducted and the suitability investigation is initiated.

Separation

Separations are actions that remove employees from the rolls of their agencies, including deaths, resignations, removals, and retirements. The Agency developed Form NLRB 4197, Certification to Release of Final Salary and Separation (Form 4197), which is used in the separation process.

The Security Branch is notified of a separation in two ways: a personnel action in FPPS and receipt of the Form 4197.

Notification through the Use of Form 4197

Agency guidance states that the Form 4197 should be received by the Security Branch prior to or no later than the day of the employee's separation. According to the Security Branch procedures, when the Form 4197 is received, Security Branch personnel should make an entry for the receipt of the form in the "mail log" and update the Personnel Security Database with a separation date. The Security Branch Chief then reviews and signs the Form 4197 and forwards it to the Office of Human Resources. A copy of the completed form is kept in the employee's security file.

We identified 152 employees who separated in FY 2013 and reviewed employee's security file to determine if the file contained a copy of the Form 4197. The table below shows the results of the review:

Employee Duty Station	Form 4197 in the File	
	Yes	No
Headquarters	41	8
Field Office	79	24

We also reviewed the mail log maintained by the Security Branch to determine whether an entry was made for the 152 Forms 4197 that should have been received:

Status of Form 4197	Form Logged	
	Yes	No
In the file	42	78
Not in the file	2	30

For the 120 Forms 4197 found during review, we identified five copies that were not signed and/or dated by the Security Branch Chief or a designee in his absence. For the remaining 115 forms, 40 of them were also entered into the mail log. For those 40 forms, we compared the date the Security Branch Chief signed the Form 4197 to the date it was entered into the mail log. The results are shown in the table below.

Period	Number of Forms
Signature date prior to mail log date	3
Signature and mail log date the same	26
Signature date after the mail log date	11

We observed that one of the forms had a signature that was 147 days prior to the mail log date. We also observed that one form had a signature date that was 92 days after the mail log date.

Notification through Personnel Action

For the 152 employees who separated in FY 2013, we did not find a separation action for one employee, and the separation actions for five employees were not routed through the Security Branch. We reviewed the separation actions for the remaining 146 employees to determine the number of days that the action was pending in the Security Branch before a

Security Personnel Specialist noted concurrence and forwarded the action to the Office of Human Resources:

Date of Concurrence	Separation Actions
On the day of receipt	63
1 Day	40
2 Days	14
3 Days	6
4 Days	6
5 or more days	17

We reviewed the Security Branch's policies and procedures and found that there was no guidance on what actions are to be taken by the Security Branch after receiving notification of a personnel action through FPPS. Those procedures state that the separation process starts when the Security Branch receives the Form 4197. Security Branch personnel confirmed our understanding that the Security Branch's concurrence does not have any particular meaning or trigger any process.

Requiring the Security Branch personnel to process personnel actions without any purpose is inefficient and delays the processing of the action by the Office of Human Resources. It is possible, however, that this step may have potential utility as a compensating control.

To illustrate that potential, we analyzed the timing of the receipt of the action by the Security Branch, as compared to the separation date of the employee:

Date Separation Action Received	Number of Employees
Before the separation date	106
On the day of separation	2
After the separation date	38

For the 106 employees where the Security Branch received the personnel action before the day of separation, many were received well in advance of the separation date:

Period	Number of Employees
More than 120 days before	2
91-120 days before	3
61-90 days before	12
31-60 days before	30
21-30 days before	16
11-20 days before	18
6-10 days before	9
2-5 days before	13
1 day before	3

We then reviewed the separation actions for 29 employees whose Forms 4197 were missing:

Separation Action Receipt by Security Branch	Before the Day of Separation	On or After the Day of Separation
More than 3 weeks (+/-) from separation date	8	4
Less than 3 weeks (+/-) from separation date	7	10

We also identified 13 out of 29 separated employee files that did not have a Form 4197 were either misfiled in the current employee drawer or the student drawer, or were found in a Personnel Security Specialist's office.

It would appear that, while not perfect, the receipt of a separation action could be used to establish a control to ensure that the Security Branch properly initiates its separation process. If not, there is no apparent reason to continue to route the separation actions through the Security Branch.

Recommendation

2k. We recommend that the Division of Administration review this process and establish an internal control to utilize the separation actions or remove the Security Branch from the routing of those actions.

Promotions and Reassignments

Except for Critical-Sensitive and Special-Sensitive positions, a reinvestigation must be initiated before or within 14 days after the promotion or reassignment is effective. For employees promoted to Critical-Sensitive positions, the reinvestigation must be initiated preplacement unless a waiver is granted, but must be initiated within 14 days after placement. For employees promoted to Special-Sensitive positions, the reinvestigation must be initiated preplacement.

The Security Branch is notified of a promotion or reassignment through a personnel action in FPPS. From the beginning of FY 2009 through FY 2013, we identified 177 promotions and reassignments to positions at a higher risk level. We then determined whether a suitability investigation was completed for those employees and, if so, whether it was initiated within 14 days of the promotion or reassignment or before for Critical-Sensitive and Special-Sensitive positions . The results are shown in the table below:

Fiscal Year	Number of Promotions and Reassignments Resulted in Higher Risk Level	Suitability Investigation Initiated			No Documentation of Investigation
		Within 14 Days	After 14 Days	Initiation Date not Documented	
2009	36	0	6	0	30
2010	27	6	7	2	12
2011	26	3	1	0	22
2012	43	6	1	6	30
2013	45	4	3	3	35
Total	177	19	18	11	129

In FY 2013, the three employees who had a suitability investigation initiated after 14 days of the promotion or reassignment include one employee who was promoted to a Critical-Sensitive position. From FY 2009 to FY 2013, there were no employees promoted or reassigned to Special Sensitive positions.

REINVESTIGATIONS BASED ON TIME

An employee who is in a position with a sensitivity level of Critical-Sensitive or Special-Sensitive, and any employee in a public trust position, regardless of the sensitivity level, must be reinvestigated at least once every 5 years. In general, moderate risk level employees require an MBI, high risk level employees require a BI, and national security sensitive level employees require either a BI or or an SSBI, depending on the position's sensitivity level. The initial suitability investigation is more detailed and more expensive than a reinvestigation.

According to the Security Branch personnel, due to budgetary constraints, the Security Branch had not begun initiating suitability reinvestigations for employees in Public Trust positions unless the employee was promoted or reassigned, or a request for a reinvestigation was received from higher officials. Our review of the files found that as of April 30, 2014, only 85 of the 969 employees in positions with a sensitivity level of Critical-Sensitive or Special-Sensitive or in a public trust position requiring reinvestigation had documentation of a current and correct suitability investigation.

Budgeting

We calculated that as of April 30, 2014, 912 suitability investigations needed to be completed, at an expense of $1,399,070, to bring the Agency's personnel security function into compliance with OPM's reinvestigation requirements.

As discussed above, 263 employees who required an MBI, BI, or SSBI either (1) did not undergo the proper initial suitability investigation; (2) the employee's file did not contain the proper documentation that a suitability investigation was completed; (3) or the employee's file was missing or did not have documentation of a proper initial suitability investigation. We also identified 28 non-sensitive / low risk employees whose files were either missing or did not have documentation of a proper suitability investigation. For these 291 employees, the Security Branch must initiate an appropriate initial suitability investigation. The table below details the number of intial suitability investigations

that are required by type and the associated cost as of April 30, 2014:

	Type and Cost of Suitability Investigations Required							
	NACI		MBI		BI		SSBI	
Status	Number	Cost	Number	Cost	Number	Cost	Number	Cost
Missing files/ investigations	28	$4,788	70	$73,080	10	$36,350	1	$4,568
Lack of proper documentation	0		45	$46,980	23	$83,605	4	$18,272
Incorrect investigations	0		40	$41,760	59	$214,465	11	$50,248
Total	28	$4,788	155	$161,820	92	$334,420	16	$73,088

There are also 621 employees who underwent the correct suitability investigation, but their investigation was more than 5 years old as of April 30, 2014. Those employees fall into two categories. The first category is employees whose suitability investigations are considered to be out of scope because they were completed more than 7 years ago. For this group of employees, the initial suitability investigation must be performed again. The table below details the number of suitability investigations required by type and the cost of the suitability investigations as of April 30, 2014:

	MBI		BI	
	Number	Cost	Number	Cost
Investigations more than 7 years old as of April 30, 2014	488	$509,472	80	$290,800

The second category includes employees whose current suitability investigation, as of April 30, 2014, is more than 5 years, but less than 7 years old. For this a group, a reinvestigation may be completed. The table below details the number of suitability investigations require by type and the cost of the suitability investigations as of April 30, 2014:

	National Agency Check with Law and Credit		Periodic Reinvestigation		SSBI Periodic Reinvestigation	
	Number	Cost	Number	Cost	Number	Cost
Reinvestigations for investigations less than 7 years as of April 30, 2014	47	$17,296	5	$4,190	1	$3,196

Workforce Capacity

Based upon our interviews with Security Branch personnel, it is not possible to accurately determine the amount of time required to complete the suitability investigative process for any particular suitability investigation type or employee. They did note, however, that if no issues arise during the suitability investigation, the least amount of time that the suitability investigation process would require by a Personnel Security Specialist is 3 hours.

A better guide, however, might be the number of suitability investigations completed by the Security Branch during a period of time, such as a fiscal year. If the Security Branch was operating at full investigative capacity during FY 2013, on average, it could be expected to complete the same number of initial suitability investigations during any 12-month period. During FY 2013, a team of three Personnel Security Specialists completed 83 suitability investigations. At the FY 2013 rate, it would take approximately 11 years to complete the reinvestigations of the 912 employees requiring reinvestigation as of April 30, 2014.

We also note that there are groups of employees that will be added to the reinvestigation backlog each year.

Recommendation

21. We recommend that the Director of Administration develop a plan to bring the Agency into compliance with OPM's suitability reinvestigation requirements.

APPENDIX

UNITED STATES GOVERNMENT
National Labor Relations Board
Office of the Director of Administration
Memorandum

Date: January 30, 2015

To: David P. Berry
Inspector General

From: Caroline H. Krewson
Director of Administration

Subject: Response to Audit of the National Labor Relations Board Personnel Security
Report No. OIG-AMR-73-XX-XXX

I have reviewed the above referenced audit report and agree with your assessment. I appreciate the hard work of your auditors to provide recommendations to improve the operations of the Personnel Security Program and the services we provide the Agency. We will implement recommendations 2a through 2l. I am also taking steps to address recommendation #1, beginning with an assessment of the organizational structure within the Security Branch. I am receiving weekly status reports on the progress made to address the recommendations.

The Personnel Security Program within the Security Branch has undergone changes under the leadership of the Chief Security Officer (CSO). The Electronic Questionnaire Investigative Processing (e-QIP) system was initiated in 2011 and fully implemented by 2012. The transition was difficult because the Agency had over 50 submittal sites. The system helped reduce the errors on applicants' submissions and aided the Agency in meeting OPM submission timeliness goals.

Additionally, in 2011 the CSO identified a cost savings measure for the Agency when he discontinued a separate agreement with the FBI to conduct name checks as part of the preliminary clearance and moved the Agency to electronic fingerprint submittal with the acquisition of a live-scan fingerprinting machine. The new service eliminated dual National Agency Checks being conducted by the FBI under two separate agreements and reduced the costs from $56.00 to $21.00 per check. Further, the Agency transitioned towards the process of having the PIV Card GSA USAccess enrollment fingerprint capture be the delivery mechanism to OPM and the FBI at the same cost.

The CSO used two paid student interns to supplement the personnel security workload. The students helped dispose of records that had been stored more than ten years after employees had departed the NLRB.

Additionally, the CSO sent personnel security specialists through approved courses for recognized certification from OPM and Defense Security Service in 2011 and 2012.

In 2014 an acquisition was approved by the Acting Director of Administration and the Office of Chief Information Officer for e-Delivery of Background Investigation software that will move the Agency from paper delivery of cases to electronic delivery and digital storage of personnel security files.

Below is our response to the auditor's specific recommendations. Due to similarities in the recommendations we have grouped the response where appropriate. A management action plan will be developed and track the progress on the recommendations. We will provide you with updates and make any necessary adjustments.

Recommendations numbered 2a, 2d: The Security Branch will work with the Records Officer to update the system of record notice for the personnel security files. The Branch is developing a records retention policy that will be reviewed and approved by the Director of Administration.

Recommendation numbered 2b, 2c: The Security Branch will improve the current filing system by creating missing files, locating misidentified files, and eliminating any process that may not be clear to staff. The Branch has already separated the active and inactive storage locations. The Branch is now observing the file check-out procedures and will add annual audits of files to be performed by the CSO. The CSO is now reviewing all personnel security files that are created by the personnel security specialists.

Recommendation number 2e: The Security Branch is validating the data for all the active records in the database. The CSO will review all personnel security files created and maintained by his personnel security specialists, and verify the data contained within the database.

Recommendation number 2f, 2g: The Security Branch will team with Human Resources to create a new Position Designation List that corrects the identified errors. Human Resources will also ensure that the Position Designation List matches FPPS. All Position Designations will be reviewed and approved by the CSO to ensure they are accurate.

Recommendation number 2h, 2i, 2j: The Security Branch is developing a new Pre-employment Clearance form that will be reviewed by the CSO to ensure that all security processing steps have been completed. The PEC will provide a record to ensure the appropriate suitability investigation has been initiated and the fingerprint or name check has been received prior to the PIV Card issuance. The PEC will be verified by the CSO.

Recommendation number 2k: As a result of the audit findings, the Chief Security Officer will ensure the Security Branch utilizes the FPPS separation

actions to locate the file for the employee and conduct a screening for any unresolved security actions. The folder will be provided to the Security Assistant. Once the 4197 Certification of Final Salary Check is received the file will be moved from active to inactive status. The CSO will write an internal policy document to delineate clear procedures with sufficient internal controls.

Recommendation number 21: A plan is being developed to address the reinvestigations. The Agency will incrementally complete all of the mandatory reinvestigations. In FY15, $70,000.00 in funds has been added to the normal Security Branch budget to address background investigations. The CSO will keep senior management informed of additional funding requirements.

cc: Mark G. Pearce, Chairman
Richard F. Griffin, Jr. General Counsel
Jennifer Abruzzo, Deputy General Counsel