Office of Inspector General | United States Postal Service

Audit Report

National Security Clearance Program

Report Number OV-AR-19-001 | June 18, 2019

Table of Contents

Highlights

Objective

Our objective was to determine whether controls are in place to effectively manage the U.S. Postal Inspection Service's national security clearance processes and safeguard personally identifiable information (PII).

The Postal Inspection Service processed 1,253 national security clearances between fiscal years (FY) 2016 and 2018. The Postal Inspection Service primarily grants Top Secret national security clearances; it only granted four Secret clearances during that time. The cost is dependent on the type of investigation, initial or reinvestigation, with a minimum cost of almost $2,000 to no more than $4,100 per clearance. Postal Service policy states that certain positions always require national security clearances, such as executive positions and certain manager positions. In addition, the Postal Inspection Service is responsible for conducting risk assessments to determine if other positions require national security clearances.

The Postal Inspection Service works with the Office of Personnel Management (OPM) to conduct a comprehensive search of an applicant's past involvement in criminal investigations. The Postal Inspection Service uses database searches to determine prior clearance status and criminal record history. It also collects and retains PII, such as an applicant's prior employment and financial history and family members' social security numbers.

In addition, the Postal Inspection Service uses two contractors to compile background investigation reports. The Postal Inspection Service is responsible for overseeing its contractors' performance. Specifically, contractors are required to complete initial investigation reports in 30 days and periodic reinvestigations in 60 days, per the contracts. These deadlines can be extended if a contractor submits an extension request to the Postal Inspection Service and it is approved. In addition, the Postal Inspection Service is responsible for coordinating with the Postal Service's Corporate Information Security Office (CISO) to certify all contractors' data security.

What the OIG Found

Overall, the Postal Inspection Service adequately reviewed, collected, and retained the documents required to grant national security clearances. However, improvements are needed for managing security clearance position designations, overseeing contractors' performance, reviewing contractors' data security, and physically safeguarding PII.

We found the Postal Inspection Service did not complete required Position Designation Surveys (PDS) to determine whether national security clearances are necessary for postal positions not specified by policy. Specifically, it did not have the required clearance assessments for 107 of 1,253 employees (9 percent) who had national security clearances processed between FYs 2016 and 2018. This occurred because management did not have a process in place for tracking the completion of PDS. Accordingly, management spent over $318,000 on clearances without the required PDS. Without clearance assessments, the Postal Inspection Service may have granted national security clearances that were unnecessary.

The Postal Inspection Service did not ensure its contractors completed background investigations per contract requirements. The two contractors provided late reports in 21 of 179, or 12 percent, of the randomly selected cases we reviewed. This occurred because management did not have a method for tracking contractor performance. Management also did not retain or document extension requests from the contractors. As a result, the Postal Inspection Service paid contractors over $87,000 annually for reports that did not meet timeliness requirements.

Postal Inspection Service management did not ensure the Postal Service's CISO conducted adequate data security reviews of the contractors' systems. The initial data security review should have occurred when the contracts began and the systems should have been subsequently assessed every two years. The review was not initiated for one contractor and was initiated, but not completed, for the other contractor. The contractors commenced work in 2007 and 2017, respectively. This occurred because the Postal Inspection Service manager was unaware of his responsibility to coordinate security reviews with the CISO and did not provide oversight to ensure reviews were completed. The contractors maintain PII records of all employees who have applied for a clearance, and the Postal Inspection Service does not currently have assurance that the information is adequately protected.

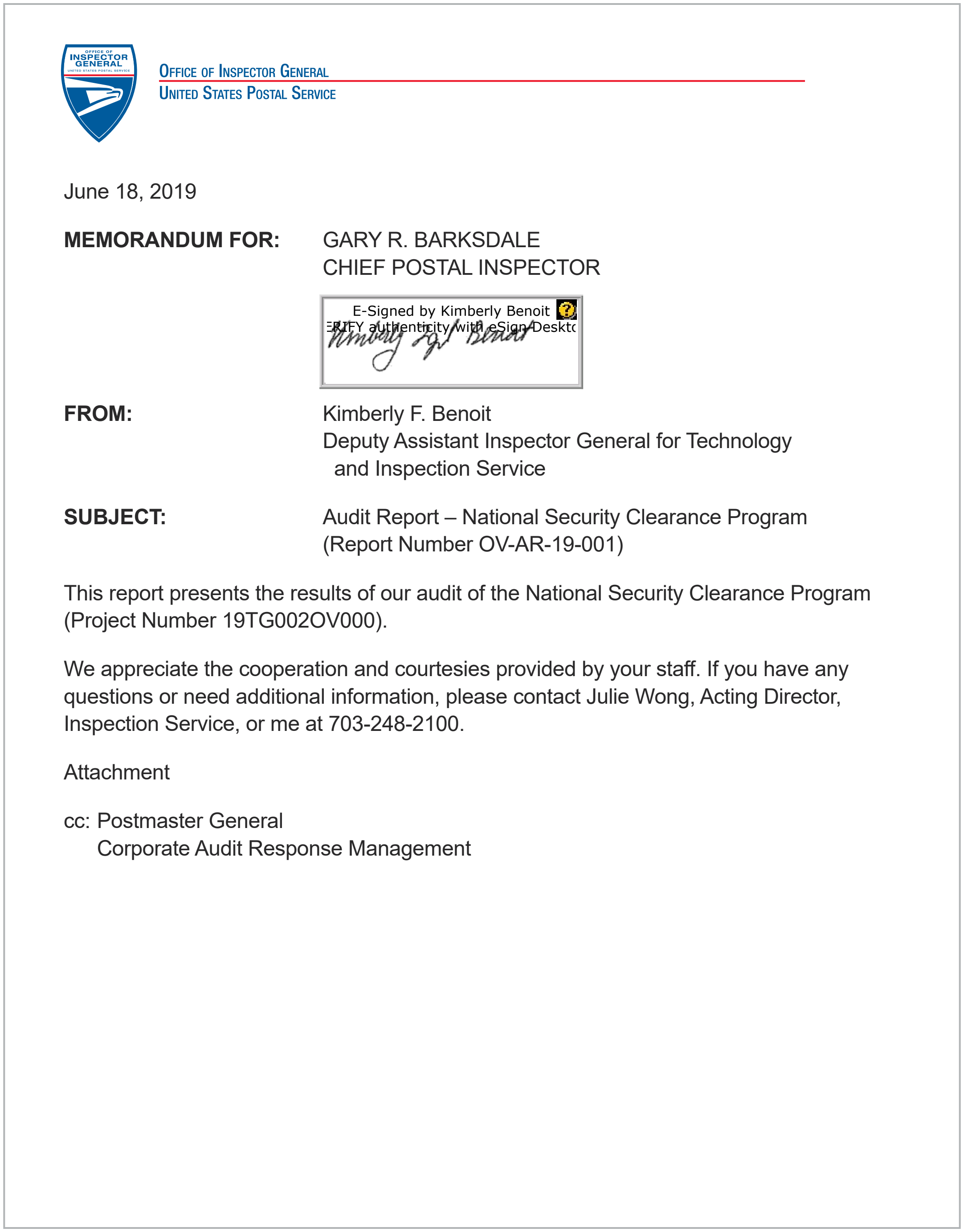
Additionally, Postal Inspection Service management did not always update or restrict access to areas where security clearances are processed. We found that management did not revoke building access for 15 of 23, or 65 percent, of former employees between 2014 and 2018. This occurred because management did not update access control lists as employees left, and management was unaware of the requirement for a semiannual access control review. There is an increased risk of unauthorized individuals, such as terminated employees, gaining access to secure areas containing PII. During the audit, management took corrective action to revoke access for the 15 former employees.

What the OIG Recommended

We recommended management:

- Develop a process to ensure PDS are completed and maintained before initiating a national security clearance investigation.
- Complete PDS for personnel possessing national security clearances without a Position Designation Survey on file to determine if the position warrants a clearance.
- Track contractors' performance by consistently reviewing monthly reports and extension requests for investigations.
- Coordinate with the CISO to complete security reviews for contractors and ensure updated reviews are conducted every two years.
- Disable badges when employees separate and review and update the badge access list semiannually.

Transmittal Letter



OFFICE OF INSPECTOR GENERAL
UNITED STATES POSTAL SERVICE

June 18, 2019

MEMORANDUM FOR: GARY R. BARKSDALE
CHIEF POSTAL INSPECTOR

E-Signed by Kimberly Benoit
ERIFY authenticity with eSign Desktc

FROM: Kimberly F. Benoit
Deputy Assistant Inspector General for Technology
and Inspection Service

SUBJECT: Audit Report – National Security Clearance Program
(Report Number OV-AR-19-001)

This report presents the results of our audit of the National Security Clearance Program (Project Number 19TG002OV000).

We appreciate the cooperation and courtesies provided by your staff. If you have any questions or need additional information, please contact Julie Wong, Acting Director, Inspection Service, or me at 703-248-2100.

Attachment

cc: Postmaster General
Corporate Audit Response Management

Results

Introduction/Objective

This report presents the results of our self-initiated audit of the National Security Clearance Program (Project Number 19TG002OV000). Our objective was to determine whether controls are in place to effectively manage the U.S. Postal Inspection Service's national security clearance processes and safeguard personally identifiable information (PII).

Background

Between fiscal years (FY) 2016 and 2018, the Postal Inspection Service processed 1,253 national security clearances. The Postal Inspection Service primarily grants Top Secret national security clearances; it only granted four Secret clearances during that time.[1] The cost is dependent on the type of investigation, initial or reinvestigation, with a minimum cost of almost $2,000 to no more than $4,100 per clearance. Employees with Top Secret clearances could have access to classified material that, if disclosed, has the potential to cause damage to national security. Therefore, it is vital that the Postal Service selects and retains qualified individuals who meet Postal Service security interests and U.S. national security interests. While Postal Service policy details specific positions that always require a national security clearance, the Postal Inspection Service is responsible for conducting risk assessments to determine if a national security clearance is necessary for positions.

Postal Service employees who hold positions with access to classified material undergo an extensive background investigation facilitated by the Postal Inspection Service and are reinvestigated every five years thereafter. Specifically, the Postal Inspection Service's Security Investigations Service Center (SISC) has the authority to grant security clearances. They conduct checks of existing national security databases to determine whether an applicant has an existing security clearance or a security clearance investigation underway. They also collect fingerprints, process the Standard Form 86 (SF-86): Questionnaire for National Security Positions, and use the National Crime Information Center to obtain criminal record history information. These files contain PII such as an applicant's prior employment and financial history and family members' social security numbers.

The SISC works with the Office of Personnel Management (OPM) to conduct the National Agency Check. An integral part of all background investigations, the National Agency Check consists of a comprehensive search of an applicant's past involvement in criminal investigations.

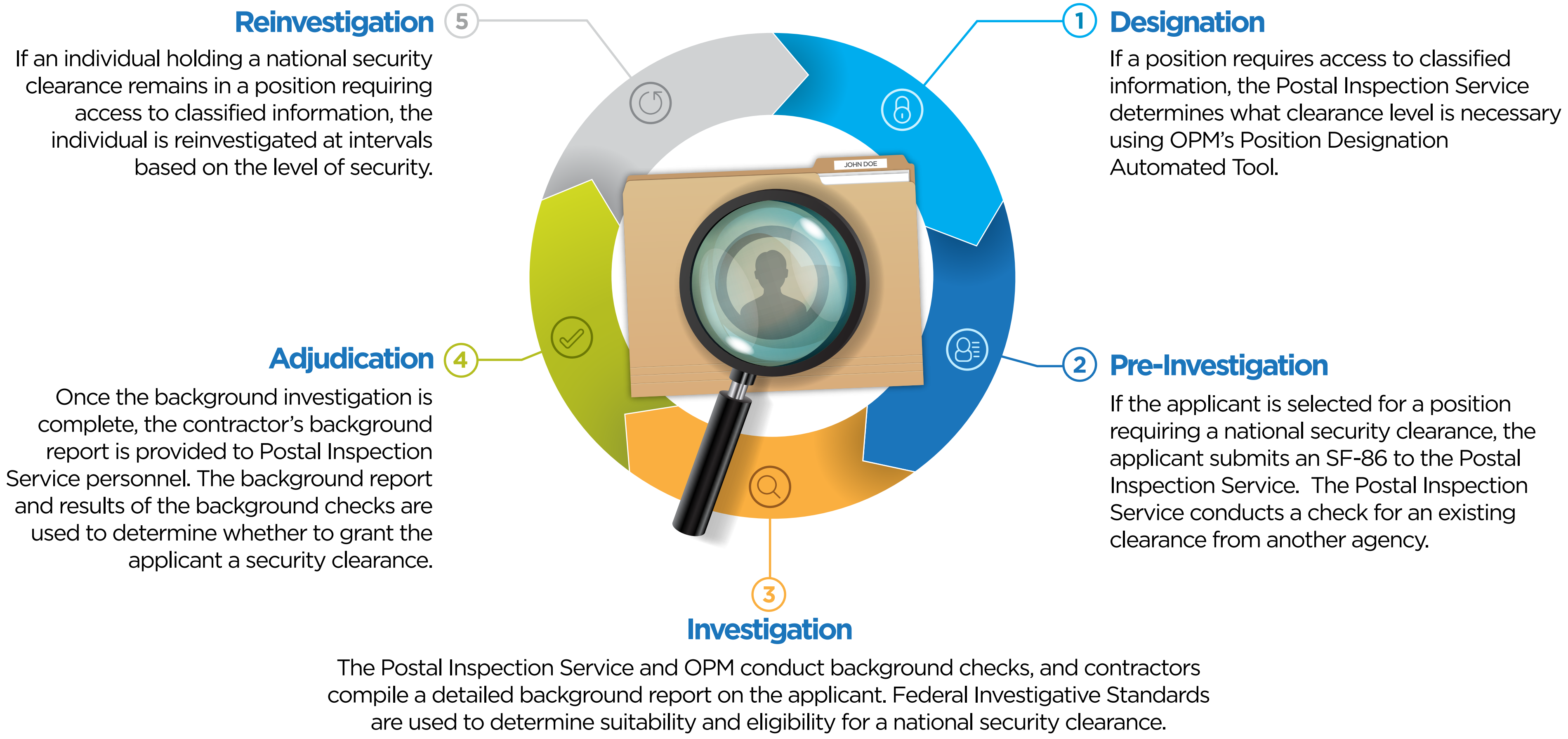
The SISC uses two contractors to generate extensive written background reports of investigation (background reports) that include previous background checks and interviews with the applicant, their coworkers, neighbors, and other contacts. This report helps develop information about a person's character, reputation, and U.S. allegiance to determine eligibility for appointment to, or suitability for retention in, a Postal Service position that has access to sensitive or classified information. The contractor's report is a key component the Postal Inspection Service uses to adjudicate a security clearance. The SISC is responsible for overseeing its contractors' performance and is responsible for coordinating with the Postal Service's Corporate Information Security Office (CISO) to certify all contractors' data security.

Overall, the Postal Inspection Service reviewed, collected, and retained required documents to grant national security clearances. However, improvements are needed for managing security clearance position designation, overseeing contractors' performance, reviewing contractors' data security, and physically safeguarding PII.

[1] One Secret clearance was processed by the SISC, while three were granted based on reciprocity.

Contractors are required to complete reports for initial investigations in 30 days and periodic reinvestigations in 60 days, in accordance with their contracts. These deadlines can be extended if a contractor submits an extension request to the Postal Inspection Service, and it is approved. The contractor timelines are a subset of the overall time it takes to complete a background investigation, per the Office of the Director of National Intelligence (ODNI) standards. ODNI timeliness standards are 114 days for initial investigations and 195 days for reinvestigations for 90 percent of processed clearances. This is the time from the date of an applicant's submission to the date of the adjudicative decision. Figure 1 shows the Postal Inspection Service's national security clearance process.

Figure 1. Postal Inspection Service's National Security Clearance Process



1 Designation

If a position requires access to classified information, the Postal Inspection Service determines what clearance level is necessary using OPM's Position Designation Automated Tool.

2 Pre-Investigation

If the applicant is selected for a position requiring a national security clearance, the applicant submits an SF-86 to the Postal Inspection Service. The Postal Inspection Service conducts a check for an existing clearance from another agency.

3 Investigation

The Postal Inspection Service and OPM conduct background checks, and contractors compile a detailed background report on the applicant. Federal Investigative Standards are used to determine suitability and eligibility for a national security clearance.

4 Adjudication

Once the background investigation is complete, the contractor's background report is provided to Postal Inspection Service personnel. The background report and results of the background checks are used to determine whether to grant the applicant a security clearance.

5 Reinvestigation

If an individual holding a national security clearance remains in a position requiring access to classified information, the individual is reinvestigated at intervals based on the level of security.

Source: U.S. Postal Service Office of Inspector General (OIG) analysis.

Finding #1: Positions Requiring National Security Clearance

We found that the Postal Inspection Service did not complete required Position Designation Surveys[2] (PDS) to determine whether a national security clearance was necessary for postal positions. The Postal Inspection Service did not have PDS for 107 of 1,253 employees (9 percent) who had national security clearances processed between FYs 2016 and 2018. Specifically, 66 Postal Service employees and 41 Postal Inspection Service employees did not have PDS for their positions.

Federal law[3] requires agencies to abide by ODNI and OPM standards for proper designation of covered positions by using the OPM tool that generates PDS. A PDS, completed by the appropriate manager, determines the level of risk and type of clearance required for a position. According to Postal Service policy,[4] the Chief Postal Inspector or his designee makes risk assessments for national security postal positions by using PDS.[5]

This occurred because the Postal Inspection Service did not have a process to track completion of a PDS before processing clearances and did not retain all of the surveys in one centralized place. Postal Inspection Service management was not aware that PDS had not been conducted for all positions that had national security clearances. In addition, SISC management believed it was the purview of Postal Service management to make their own clearance determinations, therefore, they processed clearances for Postal Service employees as they were requested, without ensuring a PDS had been completed.[6]

Agencies must be able to demonstrate that they are adhering to the standards for proper designation of positions or they could lose their delegated authority to make position designation decisions. Without PDS, the Postal Inspection Service may have granted security clearances that were unnecessary. Between FYs 2016 and 2018, management spent $318,031.82 on 107 clearances without completed PDS.[7]

During the audit, management stated they are updating Postal Service policy to ensure all Postal Service positions are evaluated using the OPM tool to determine the type of background screening each position requires. In addition, management stated they will establish a cyclical review to ensure positions are re-evaluated and updated.

Recommendation #1

The **Chief Postal Inspector** develop a process to ensure Position Designation Surveys are completed and maintained before initiating a national security clearance investigation.

Recommendation #2

The **Chief Postal Inspector** complete Position Designation Surveys (PDS) for personnel possessing national security clearances without a PDS on file to determine if the position warrants a clearance.

[2] PDS are a required part of the Postal Inspection Service's clearance assessment process. They are generated through the OPM's Position Designation Automated Tool to ensure agencies have a systematic, dependable, and uniform way of making position designations.
[3] Code of Federal Regulations, Title 5, Part 1400.201(b), updated July 6, 2015.
[4] *Administrative Support Manual* (ASM), Issue 13, Chapter 2, Section 272, Personnel Security Clearances, updated through October 30, 2018.
[5] This applies to all postal positions except executives and managerial attorney positions, which are specifically listed in the ASM as always requiring a Top Secret clearance.
[6] Postal Service Form 2013, Request for Background Investigation, is required after a PDS is completed.
[7] The cost of each initial background investigation includes an OPM national agency check, costing $154-$179, and a cost for the contractor background report. The lower of the two contractors' costs for an initial investigation is $2,818.26. The conservative cost of each initial investigation is $2,972.26. The team multiplied this cost by the 107 employees given clearances without a PDS.

Finding #2: Oversight of Contractor Performance

The Postal Inspection Service did not ensure its contractors completed background investigation reports timely, according to contractual requirements. We found the contractors provided late reports in 21 of 179 randomly selected cases (12 percent) we reviewed, as shown in Table 1.[8]

Table 1. Contractor Timeliness Analysis

Case Type	Sample Size	Contract Requirement	Number of Late Cases
Initial	50	>30 days	6
Reinvestigations	129	>60 days	15
Total	**179**		**21**

Source: OIG analysis of SISC data.

Contractors' statements of work (SOW) require that reports for initial investigations be completed in 30 days and reinvestigations be completed in 60 days. According to the SOWs, contractors can request an extension from the SISC manager[9] on a case-by-case basis, but they must do so before the scheduled completion date for each case.[10] This occurred because management did not track contractors' performance. Management did not require or use monthly reports created by the contractors to monitor the timeliness of background reports. In addition, management did not retain contractors' requests for extensions on delayed cases.

When national security clearances are not completed timely, there is a risk that the Postal Service may not be able to recruit and retain skilled employees, which could impact the Postal Service and the Postal Inspection Service's mission. In addition, new employees may not be able to fulfill all aspects of their positions if their security clearances are delayed. As a result, the Postal Inspection Service paid contractors $263,130[11] for reports that did not meet timeliness requirements.

Recommendation #3

The **Chief Postal Inspector** ensure the Security Investigations Security Center manager tracks contractors' performance by consistently reviewing monthly timeliness reports and extension requests for investigations.

Finding #3: Data Security

SISC management did not ensure the Postal Service's CISO conducted adequate data security reviews of the systems used by contractors responsible for providing background reports. The manager should have initiated the CISO's Certification and Accreditation process for the first contractor (who began work in 2007) in 2009, when new information security policies were implemented. For the second contractor, who began work in 2017,[12] CISO began the certification process timely, but the final results were not approved by the appropriate officials. Periodic reviews of the contractors' systems also did not occur.[13]

Postal Service policy[14] states the Certification and Accreditation process is required for all information resources maintained or operated on behalf of the Postal Service. The process, which management should request when a contract begins, validates that contractors have adequate system controls in place to protect PII and other sensitive data they collect. A periodic review of the systems is required every two years after the initial process is completed.

[8] The Postal Inspection Service did not meet the ODNI standards of 114-day initial investigations and 195-day reinvestigations in 62 of 179 cases (35 percent). However, this was primarily due to an OPM backlog outside of the Postal Inspection Service's control.
[9] The SISC manager is the designated Contracting Officer's Representative (COR). The COR is responsible for day-to-day management of the contract.
[10] Cases with a documented and approved extension request would not be considered late, however, there were no documented extension requests in our sample.
[11] We projected our FY 2016-2018 sample to determine monetary impact for a 24-month period. We calculated monetary impact based on $1,790, the most conservative estimate of unit cost per investigation. Therefore, a monetary impact of $155,730.00 was calculated for FYs 2017 and 2018.
[12] Management stated a second contractor was hired for continuity-of-operations purposes.
[13] Had the certification process of the second contractor occurred, the periodic review would commence in August 2019.
[14] Handbook AS-805-A, *Information Resource Certification and Accreditation Process*, dated June 2015.

This occurred because the manager was unaware of his responsibility to coordinate security reviews with the CISO and ensure reviews were properly completed.

Contractors maintain records containing PII for thousands of employees, and the Postal Inspection Service does not have assurances that the information is adequately protected. Information in the SF-86 contains PII such as prior employment and financial history and an applicant's and family members' social security numbers. A security breach resulting in losing PII could damage the Postal Service brand, as well as current and prospective employees' trust.

During the course of the audit, management informed us the Certification and Accreditation process had been initiated for both contractors.

Recommendation #4

The **Chief Postal Inspector** ensure the Security Investigations Service Center manager coordinates with the Corporate Information Security Office, to complete security reviews for the contractors and ensure updated reviews are conducted every two years.

Finding #4: Physical Security of Background Investigation Files

SISC management did not always update or restrict access to secure areas of its office that house PII. Management did not revoke building access[15] for 15 of 23 (65 percent) former employees who transferred offices or left the Postal Inspection Service between 2014 and 2018, as shown in Table 2.

Table 2. Former Employees with Access to the SISC Office

Reason for Employee Separation from SISC, 2014 - 2018	Number of Employees	Badge Access Not Revoked	Badge Access Revoked
Retirement and disability/other	9	8	1
Promotion	2	0	2
Separation - transfer to another agency	3	2	1
Resignation	2	2	0
Reassignment	4	2	2
Change of Position	1	0	1
Non-Career Termination	1	1	0
Detail Assignment	1	0	1
Total	**23**	**15**	**8**
Percentage	**100%**	**65%**	**35%**

Source: OIG analysis of Postal Service data pulled from ePACS.

According to Postal Service policy,[16] management must update access control lists when assigning new personnel to the controlled area or when someone leaves and review and update access control lists semiannually.

This occurred because management did not update access control lists as employees left the agency and were unaware of the requirement for a semiannual access control review. When the badge access list is not accurate, there is an increased risk of unauthorized individuals, such as terminated employees, entering the building and gaining access to secure areas containing PII. During our site visit, we observed that SISC employees left completed background investigation files containing PII unsecured in the office. Employees keep background investigation files they are working on locked in their desk file

[15] The Postal Inspection Service uses the ePhysical Access Control System (ePACS) to grant or remove badge access to the SISC office.
[16] Handbook AS-805, Chapter 7, Physical and Environmental Security, dated December 2018.

cabinets; however, after a background investigation has been adjudicated, the paper files that include PII – such as the applicant's SF-86, fingerprint cards, the contractor's background report, and OPM background checks – are left in open containers for transfer to another department. The last pick-up each workday is at 2 p.m., and any documents placed in the containers after that time are not picked up until the next workday.

During the audit, management took corrective action to revoke access for the 15 former employees.

Recommendation #5

The **Chief Postal Inspector** require the Security Investigations Service Center manager to disable badges in a timely manner when employees separate and review and update the badge access list semiannually.

Management's Comments

Management agreed, in part, with recommendations 1 and 2; and agreed with recommendations 3, 4, and 5. Management disagreed with the monetary impact associated with recommendations 2 and 3.

Regarding recommendation 1, management agreed to complete and maintain PDS for all existing positions occupied by employees with a national security clearance. However, management plans to use PS Form 2013 as a replacement for PDS when business needs require initiation of a clearance investigation before completion of the PDS. The target implementation date is March 31, 2020.

Regarding recommendation 2, management agreed to complete PDS for employees who possess a national security clearance. Management stated that they use PS Form 2013 to initialize clearance investigations, as outlined in the ASM when the Postal Inspection Service determines an individual in the position requires a clearance, but the OPM Position Designation Automated Tool indicates otherwise. Management stated that they had either a PDS or PS Form 2013 on file for 106 of 107 employees identified by the OIG. Management stated the monetary impact should be decreased from $318,031.82 to $2,972.26. The target implementation date is March 31, 2020.

Regarding recommendation 3, management stated they have established a process to track contractors' performance to ensure they meet timeliness goals. Management stated that although prior investigations have been late, it has not affected clearance determinations. Management stated that the Postal Service realized the value of the investigations and did not sustain a monetary impact. Management stated that they implemented the tracking process on May 15, 2019.

Regarding recommendation 4, management stated that they have begun the Certification and Accreditation process for both contractors and will ensure reviews are conducted every two years. That target implementation date is September 30, 2019.

Regarding recommendation 5, management stated that they have established procedures for conducting semiannual reviews and ensuring that separated employees are removed from ePACS promptly. Management stated that they implemented this process on May 16, 2019.

See Appendix B for management's comments in their entirety.

Evaluation of Management's Comments

The OIG considers management's comments partially responsive to recommendations 1 and 2. The OIG considers management's comments responsive to recommendations 3, 4, and 5, and corrective actions should resolve the issues identified in the report.

Regarding recommendations 1 and 2, management stated that a PS Form 2013 could be used in place of a PDS in either of two scenarios: if a clearance is necessary before a PDS can be completed or if the Position Designation Automated Tool indicates there is no need for a clearance but the Postal Inspection Service deems a clearance is necessary. The Code of Federal Regulations and the ASM require a PDS for each position to determine the level of risk and the type of clearance required.[17] Management should adhere to the Code of Federal Regulations and ASM and complete PDS in all instances.

[17] ASM, Issue 13, Chapter 2, Section 272.281, updated through October 30, 2018; Code of Federal Regulations, Title 5, Part 1400.201(b), updated July 6, 2015.

After a PDS is completed, the ASM also requires a PS Form 2013 before the file can be submitted for clearance processing.[18] Management did not provide a PDS for 107 employees. As a result, the monetary impact of $318,031.82 is accurate. We will not pursue audit resolution for recommendations 1 and 2 because management provided implementation dates for the recommendations in their response. Management should take appropriate corrective action to complete and maintain PDS for all clearances.

Regarding recommendation 3, the OIG agrees that the Postal Service realized the value of the investigations performed by contractors; however, it paid $155,730 to contractors who failed to adhere to contractual requirements. When national security clearances are not completed timely there is a risk that the Postal Service may not be able to recruit and retain skilled employees, which could impact the Postal Service and the Postal Inspection Service's mission.

Regarding recommendations 3 and 5, management stated they have already taken corrective action to address the recommendations; however the OIG has not received supporting documentation. For the recommendations to officially close, management should provide support demonstrating that they have taken corrective action.

All recommendations require OIG concurrence before closure. Consequently, the OIG requests written confirmation when corrective actions are completed. Recommendations should not be closed in the Postal Service's follow-up tracking system until the OIG provides written confirmation that the recommendations can be closed.

[18] ASM Chapter 2, Section 272.284.

Appendices

Click on the appendix title below to navigate to the section content.

Appendix A: Additional Information

Scope and Methodology

The scope of our audit included an evaluation of the processing of national security clearances and controls at the SISC between FYs 2016 and 2018. We excluded from our sample the clearances for OIG personnel that are processed by the Postal Inspection Service.

To accomplish our objective, we:

- Identified systems the Postal Inspection Service uses to process national security clearances.
- Reviewed a statistical sample of 179 security clearance investigation files processed between FYs 2016 and 2018 for timeliness and completeness.
- Conducted interviews with Postal Inspection Service personnel at the SISC in Memphis, TN, to obtain and validate information about the security clearance process. We also conducted a physical security review.
- Analyzed contracts for the companies responsible for conducting background investigation reports on behalf of the Postal Inspection Service to determine timeliness requirements and other contractual obligations.
- Analyzed the physical and system access control lists to confirm only appropriate personnel have access to the SISC facility and the systems used for security clearance processes, respectively.
- Analyzed the process the Postal Inspection Service uses to determine whether a job position requires a national security clearance.
- Identified the required training for conducting security clearance investigations to determine whether the SISC personnel received adequate training.

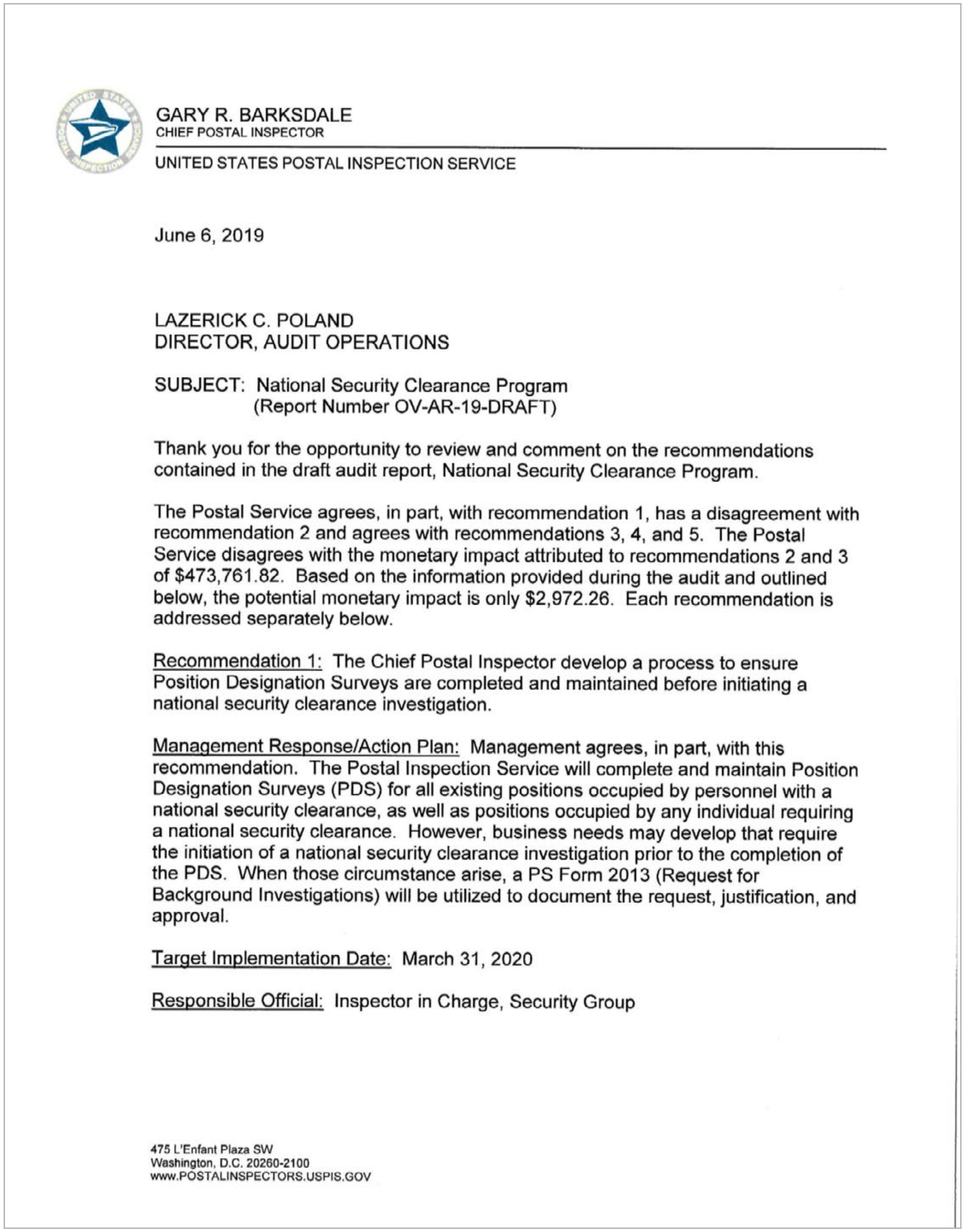
We conducted this performance audit from October 2018 through June 2019, in accordance with generally accepted government auditing standards and included such tests of internal controls as we considered necessary under the circumstances. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective. We discussed our observations and conclusions with management on May 10, 2019, and included their comments where appropriate.

We assessed the reliability of National Security Clearance program data by evaluating the Security Clearance Tracking System and ePACS. We determined that the data were sufficiently reliable for the purposes of this report.

Prior Audit Coverage

The OIG did not identify any prior audits or reviews directly related to the objective of this audit within the last five years.

Appendix B: Management's Comments



GARY R. BARKSDALE
CHIEF POSTAL INSPECTOR

UNITED STATES POSTAL INSPECTION SERVICE

June 6, 2019

LAZERICK C. POLAND
DIRECTOR, AUDIT OPERATIONS

SUBJECT: National Security Clearance Program
(Report Number OV-AR-19-DRAFT)

Thank you for the opportunity to review and comment on the recommendations contained in the draft audit report, National Security Clearance Program.

The Postal Service agrees, in part, with recommendation 1, has a disagreement with recommendation 2 and agrees with recommendations 3, 4, and 5. The Postal Service disagrees with the monetary impact attributed to recommendations 2 and 3 of $473,761.82. Based on the information provided during the audit and outlined below, the potential monetary impact is only $2,972.26. Each recommendation is addressed separately below.

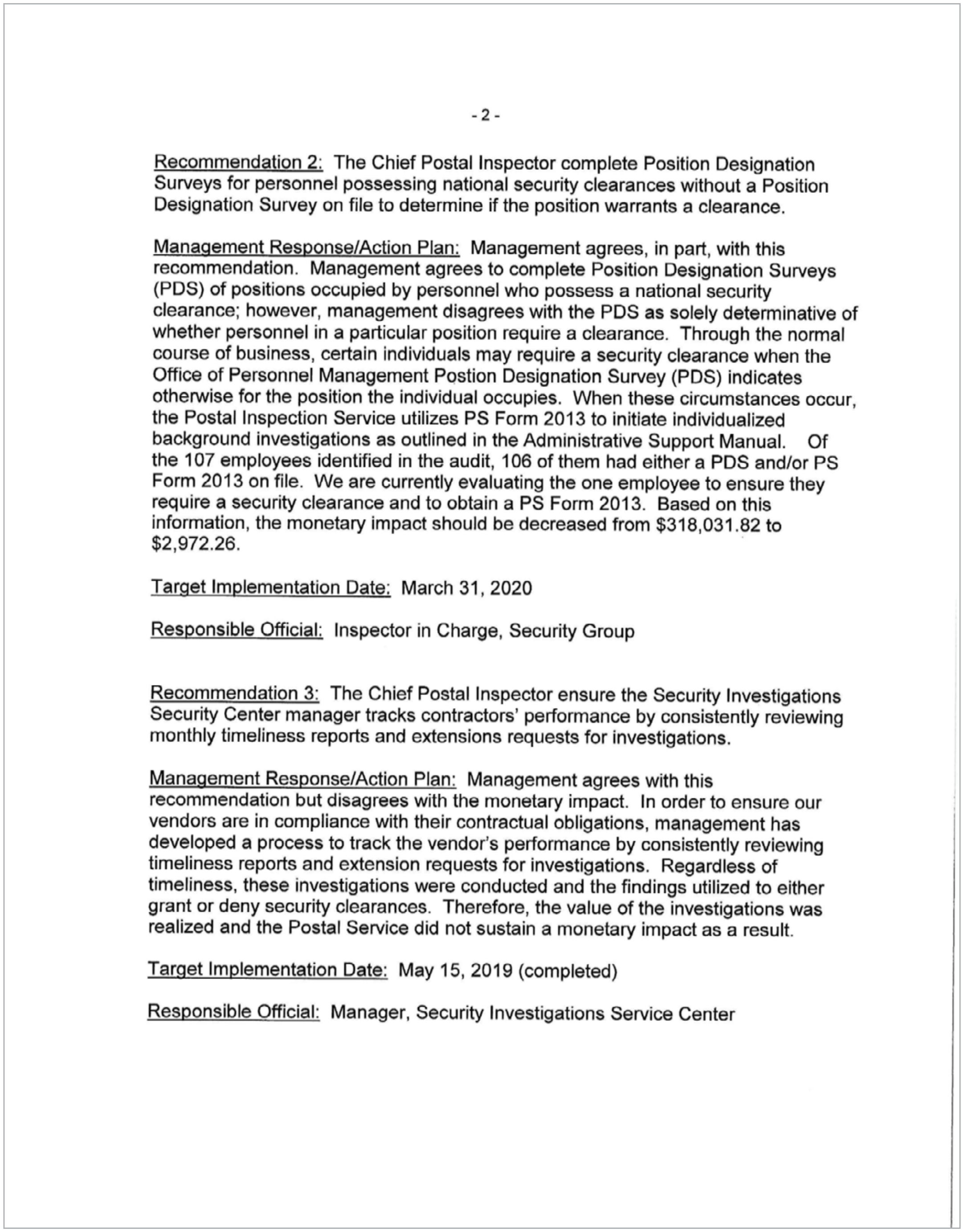
Recommendation 1: The Chief Postal Inspector develop a process to ensure Position Designation Surveys are completed and maintained before initiating a national security clearance investigation.

Management Response/Action Plan: Management agrees, in part, with this recommendation. The Postal Inspection Service will complete and maintain Position Designation Surveys (PDS) for all existing positions occupied by personnel with a national security clearance, as well as positions occupied by any individual requiring a national security clearance. However, business needs may develop that require the initiation of a national security clearance investigation prior to the completion of the PDS. When those circumstance arise, a PS Form 2013 (Request for Background Investigations) will be utilized to document the request, justification, and approval.

Target Implementation Date: March 31, 2020

Responsible Official: Inspector in Charge, Security Group

475 L'Enfant Plaza SW
Washington, D.C. 20260-2100
www.POSTALINSPECTORS.USPIS.GOV



Recommendation 2: The Chief Postal Inspector complete Position Designation Surveys for personnel possessing national security clearances without a Position Designation Survey on file to determine if the position warrants a clearance.

Management Response/Action Plan: Management agrees, in part, with this recommendation. Management agrees to complete Position Designation Surveys (PDS) of positions occupied by personnel who possess a national security clearance; however, management disagrees with the PDS as solely determinative of whether personnel in a particular position require a clearance. Through the normal course of business, certain individuals may require a security clearance when the Office of Personnel Management Postion Designation Survey (PDS) indicates otherwise for the position the individual occupies. When these circumstances occur, the Postal Inspection Service utilizes PS Form 2013 to initiate individualized background investigations as outlined in the Administrative Support Manual. Of the 107 employees identified in the audit, 106 of them had either a PDS and/or PS Form 2013 on file. We are currently evaluating the one employee to ensure they require a security clearance and to obtain a PS Form 2013. Based on this information, the monetary impact should be decreased from $318,031.82 to $2,972.26.

Target Implementation Date: March 31, 2020

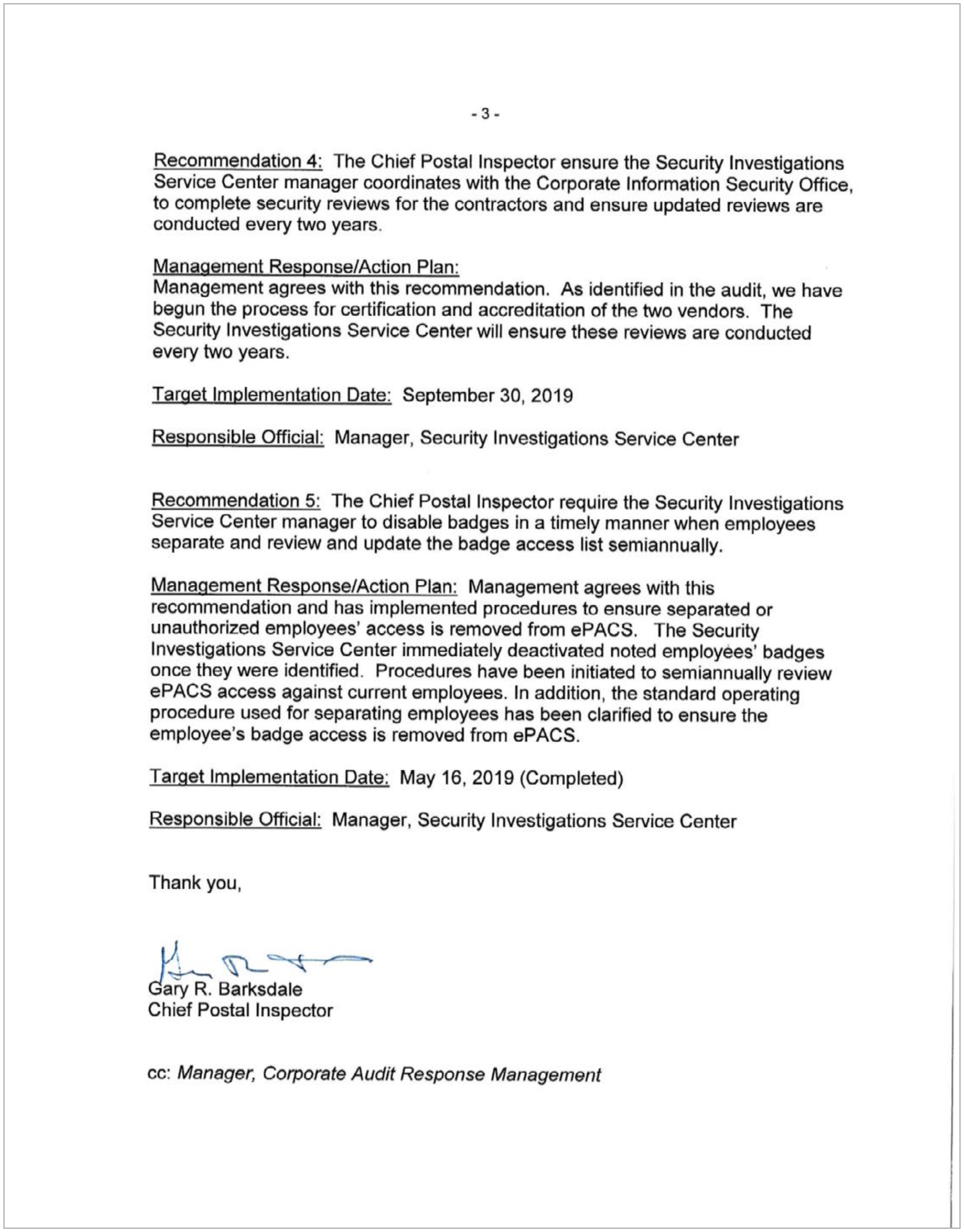
Responsible Official: Inspector in Charge, Security Group

Recommendation 3: The Chief Postal Inspector ensure the Security Investigations Security Center manager tracks contractors' performance by consistently reviewing monthly timeliness reports and extensions requests for investigations.

Management Response/Action Plan: Management agrees with this recommendation but disagrees with the monetary impact. In order to ensure our vendors are in compliance with their contractual obligations, management has developed a process to track the vendor's performance by consistently reviewing timeliness reports and extension requests for investigations. Regardless of timeliness, these investigations were conducted and the findings utilized to either grant or deny security clearances. Therefore, the value of the investigations was realized and the Postal Service did not sustain a monetary impact as a result.

Target Implementation Date: May 15, 2019 (completed)

Responsible Official: Manager, Security Investigations Service Center



Recommendation 4: The Chief Postal Inspector ensure the Security Investigations Service Center manager coordinates with the Corporate Information Security Office, to complete security reviews for the contractors and ensure updated reviews are conducted every two years.

Management Response/Action Plan:
Management agrees with this recommendation. As identified in the audit, we have begun the process for certification and accreditation of the two vendors. The Security Investigations Service Center will ensure these reviews are conducted every two years.

Target Implementation Date: September 30, 2019

Responsible Official: Manager, Security Investigations Service Center

Recommendation 5: The Chief Postal Inspector require the Security Investigations Service Center manager to disable badges in a timely manner when employees separate and review and update the badge access list semiannually.

Management Response/Action Plan: Management agrees with this recommendation and has implemented procedures to ensure separated or unauthorized employees' access is removed from ePACS. The Security Investigations Service Center immediately deactivated noted employees' badges once they were identified. Procedures have been initiated to semiannually review ePACS access against current employees. In addition, the standard operating procedure used for separating employees has been clarified to ensure the employee's badge access is removed from ePACS.

Target Implementation Date: May 16, 2019 (Completed)

Responsible Official: Manager, Security Investigations Service Center

Thank you,

Gary R. Barksdale
Chief Postal Inspector

cc: *Manager, Corporate Audit Response Management*

BACK *to* COVER

◀◀ ◀ ▶ ▶▶

OFFICE OF
INSPECTOR
GENERAL
UNITED STATES POSTAL SERVICE

Contact us via our Hotline and FOIA forms.
Follow us on social networks.
Stay informed.

1735 North Lynn Street
Arlington, VA 22209-2020
(703) 248-2100

For media inquiries, contact Agapi Doulaveris
Telephone: 703-248-2286
adoulaveris@uspsoig.gov