



April 20, 2006

LEE R. HEATH
CHIEF POSTAL INSPECTOR

SUBJECT: Audit Report – Postal Inspection Service’s Security Investigations Service Center (Report Number SA-AR-06-002)



This report presents the results of our self-initiated audit of the Postal Inspection Service Security Investigations Service Center (SISC) (Project Number 03BN013SA002). Our overall objective was to determine whether the SISC effectively and efficiently supports the Postal Inspection Service’s mission.

The SISC generally followed policies and procedures to manage and safeguard closed cases and process Freedom of Information Act (FOIA) requests. However, opportunities exist to improve the overall management of the Background Security Clearance Program, personnel security training, and the 1510 Mail Loss/Rifling Program to more effectively and efficiently support the Postal Inspection Service’s mission.

We recommended the Chief Postal Inspector: (1) establish a comprehensive management plan to address erroneous data included in the Security Clearance Tracking System and reduce its carryovers of background investigations, (2) ensure SISC security personnel are provided formal annual and refresher training to more effectively manage and implement the personnel security program, and (3) ensure Postal Inspection Service inspectors review all U.S. Postal Service (PS) Forms 1510, Mail Loss/Rifling, complaints prior to complaints being destroyed. During the audit, SISC staff initiated corrective actions to address carryovers for background security clearances, personnel security training, and the 1510 Mail Loss/Rifling Program.

Management disagreed with establishing a comprehensive management plan to address erroneous data in the Security Clearance Tracking System and reduce its carryovers of background investigations. We do not plan to pursue this recommendation through the formal audit resolution process. Management agreed to ensure that Security Investigation Service Center personnel are provided formal annual and refresher training. Management also agreed to ensure Postal Inspection Service inspectors review all PS Forms 1510, complaints before the complaints are destroyed. Management’s comments and our evaluation of these comments are included in the report.

We appreciate the cooperation and courtesies provided by your staff during the audit. If you have any questions or need additional information, please contact Sandra Bruce, director, Oversight of Investigative Activities, or me at (703) 248-2300.

E-Signed by Mary Demory 
VERIFY authenticity with Approve!


Mary W. Demory
Deputy Assistant Inspector General
for Headquarters Operations

Attachments

cc: Lawrence E. Maxwell
Zane M. Hill
Mary Anne Gibbons
Steven R. Phelps

TABLE OF CONTENTS

Executive Summary	i
Part I	
Introduction	1
Background	1
Objective, Scope, and Methodology	2
Prior Audit Coverage	4
Part II	
Audit Results	7
Security Investigations Service Center Generally Supports the Postal Inspection Service's Mission	7
Background Security Clearance Program	7
Recommendation	11
Management's Comments	11
Evaluation of Management's Comments	12
Personnel Security Training	12
Recommendation	13
Management's Comments	14
Evaluation of Management's Comments	14
1510 Mail Loss/Rifling Program	14
Recommendation	15
Management's Comments	15
Evaluation of Management's Comments	15
Appendix A. Fiscal Years 2004 and 2005 Schedule of Security Investigations Service Center Open Cases	16
Appendix B. Fiscal Year 2004 Average Number of Days to Process and Grant Final and Interim Security Clearances	17
Appendix C. Management's Comments	19

EXECUTIVE SUMMARY

Introduction

This report represents the results of our self-initiated audit of the Postal Inspection Service Security Investigations Service Center (SISC). Our overall objective was to determine whether the SISC effectively and efficiently supports the Postal Inspection Service's mission.

Results in Brief

The SISC generally followed policies and procedures to effectively and efficiently support the Postal Inspection Service's mission. However, Postal Inspection Service officials could improve the overall management of the Background Security Clearance Program, personnel security training, and the 1510 Mail Loss/Rifling Program.

Specifically, background investigation data SISC staff provided showed the Postal Inspection Service had a carryover of about 9,700 open security clearance cases at the beginning of fiscal year (FY) 2004, and 18,300 open security clearance cases at the beginning of FY 2005. We discussed our results with SISC staff during the audit and based on the results, SISC staff conducted further analyses and stated they identified an unexplainable glitch in the Security Clearance Tracking System (SCTS).¹ According to SISC staff, this glitch resulted in SISC staff providing the U.S. Postal Service Office of Inspector General (OIG) with inaccurate information on background security clearances.

Therefore, SISC staff requested the OIG disregard the data we analyzed starting with the beginning of FY 2004, but instead analyze the data starting with the beginning of FY 2005. Additionally, in November 2005, SISC staff provided the OIG with a FY 2005 status report, which showed there were approximately 5,700 sensitive and nonsensitive open clearances as of October 21, 2005. Appendix A provides a schedule of background investigation requests.

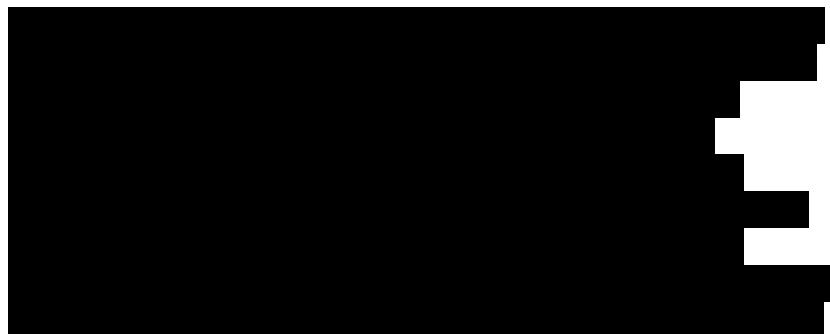
After receiving the updated information from the SISC staff, the OIG determined the background security data provided by SISC staff starting with the beginning of FY 2004 was the same data they initially provided the OIG. To further validate the data, the OIG analyzed background security

¹ SCTS is an automated system that monitors and tracks background security clearances and processes real time information that can not be recaptured.

clearance information² the SISC submitted to the Office of Personnel Management (OPM), and determined the information was comparable to the number of requests the SISC staff initially provided the OIG starting with the beginning of FY 2004. Unless the number of requests the OPM processed for the SISC staff was inaccurate, we cannot agree with management's assertion that the information SISC staff provided the OIG was inaccurate. However, we do acknowledge that as a result of our audit and based on the updated information SISC staff provided the OIG, it appears that management has initiated corrective actions to begin addressing the carryovers.

The background investigation process is essential to managing the inherent risk of allowing U.S. Postal Service employees and other personnel access to sensitive or proprietary information. To ensure effective management of the security clearance process, security clearance data must be consistent, accurate, and complete to assist management with making decisions regarding current workload requirements, and the overall management of the Background Security Clearance Program.

Further, 12 of the 15 SISC personnel responsible for reviewing and adjudicating security clearance requests had not received personnel security training within the past 5 fiscal years. This occurred because the Postal Inspection Service did not have a requirement to provide annual and refresher training to staff processing security clearance requests. As a result of our audit, Postal Inspection Service officials initiated corrective actions during the audit to obtain supplemental personnel security training for SISC employees.



² "Workload Average Timelines for U.S. Postal Inspection Service in Memphis, FY 04 and up to July 2, 2005."

³ According to SISC personnel, attractive targets for theft include things like [REDACTED]. While unattractive mail consists of items that are not considered attractive as targets for theft.

[REDACTED]

As a result of our audit, Postal Inspection Service officials initiated corrective actions during the audit and advised that all PS Forms 1510 will be forwarded to [REDACTED]

[REDACTED] We will further assess the 1510 Mail Loss/Rifling Program during our ongoing audit of the CISC.

**Summary of
Recommendations**

We recommended the Chief Postal Inspector: (1) establish a comprehensive management plan to address erroneous data included in the SCTS and reduce the number of carryovers for background security clearances, (2) ensure SISC security personnel are provided formal annual and refresher training to more effectively manage and implement the personnel security program, and [REDACTED]

[REDACTED]

During the audit, SISC staff initiated corrective actions to address excess background security clearances and erroneous data included in the SCTS, additional personnel security training, and [REDACTED]

**Summary of
Management's
Comments**

For recommendation 1, management did not agree to establish a comprehensive management plan to address erroneous data in the SCTS and reduce its carryovers of background investigations. Management stated that the OIG had data manipulation problems when analyzing security clearance data they provided the OIG on compact disc (CD). Management also stated that carryovers in background security clearances will always exist from one day to the next and from one year to the next. Additionally, management stated that the recommendation implied that the average processing time was excessive, but nothing in the report supports that assertion.

For recommendation 2, management agreed to ensure that SISC personnel receive formal annual and refresher training to supplement personnel security training. [REDACTED]

[REDACTED]

Management's comments, in their entirety, are included in Appendix C.

**Overall Evaluation of
Management's
Comments**

For recommendation 1, we disagree with management's assertion that the OIG experienced data manipulation problems when analyzing security clearance data, resulting in blank dates, future dates, and negative elapsed days for processing. SISC officials provided data to the OIG on a CD that could not be modified (read-only); therefore, the OIG could not manipulate the data. Further, SISC personnel provided the OIG with a written summary of interim and final clearances that we used to validate the data on the CD. Additionally, during our review of security clearance data, we notified SISC personnel of the erroneous data we identified and excluded it from our analysis.

Additionally, the OIG did not conclude or report that processing times were excessive. The OIG concluded there were carryovers in FYs 2004 and 2005, and these carryovers did not result from delays in processing background security clearances by the OPM. However, based on further OIG analyses, SISC staff did not process requests in FY 2005 as quickly as they received them; therefore, there appeared to be a growing backlog in FY 2006. For example, in FY 2005, the average number of requests was about 6,940 and the average number completed was about 5,280, resulting in an average carryover of about 1,660 per month. Although management disagreed with this recommendation, we do not plan to pursue this recommendation through the formal audit resolution process.

Management agreed with recommendation 2 and stated supervisors and managers will obtain annual background clearance training offered by the OPM. Management also agreed with recommendation 3 and stated inspectors use the [REDACTED]

Management comments and planned corrective actions for recommendations 2 and 3 are responsive, satisfy the intent of our recommendations, and should correct the issues identified in the finding.

INTRODUCTION

Background

The Postal Inspection Service is responsible for ensuring the integrity of the mail and safeguarding the U.S. Postal Service by: (1) performing investigative, security and preventive services, and (2) enforcing approximately 200 federal laws that protect the mail, postal employees, customers, and critical assets.

The Chief Postal Inspector is designated as the security officer for the Postal Service and issues instructions and regulations on security requirements. Postal Service installation heads are responsible for ensuring the safety of postal employees, as well as the security and integrity of the mail and of all postal property entrusted to them. Further, Security Control Officers (SCOs) at Postal Service facilities are primarily responsible for ensuring the general security of facilities as required by policies and procedures.

The Security Investigation Service Center (SISC) is one of the four service centers supporting the Postal Inspection Service's mission. The SISC primarily oversees the Background Security Clearance Program for all regular and contract Postal Service employees. The SISC also manages the 1510 Mail Loss/Rifling Program, maintains closed case files, and processes Freedom of Information Act (FOIA) requests.⁴

Background Security Clearance Program. All background security clearance information is electronically maintained in the SISC's Security Clearance Tracking System (SCTS).⁵ According to SISC personnel, the SCTS is the official Postal Inspection Service database for managing the background security clearance program. Further, security clearance documentation is maintained as follows:

- The SISC maintains documentation for career Postal Service employees.
- The administrative official for the contract maintains documentation for highway transportation contract employees.

⁴ Based on information provided by Criminal Investigation Service Center (CISC) staff, the Postal Inspection Service now requires all Postal Service (PS) Forms 1510, Mail Loss/Rifling Program, to be sent to the CISC and then disseminated to the respective division for inspectors to review.

⁵ The SCTS is designed to monitor and track security clearances requested and issued, and also actions taken by SISC, Office of Personnel Management, and contractors performing work on behalf of the SISC.

- Airline, FedEx, and Terminal Handling Service (THS) contractors maintain documentation for their employees.

The documentation maintained by contractors is available for review by the Postal Inspection Service or the contracting officer upon request.

Additionally, the Office of Personnel Management (OPM) provides investigative results to the Postal Inspection Service's SISC staff based on search results from the Federal Bureau of Investigation (FBI) and Department of Defense databases and investigative files. In fiscal years (FY) 2003 and 2004, the SISC granted 48,778 and 41,789 final clearances, respectively. In addition, in FY 2004, the SISC granted 5,211 interim sensitive security clearances.

1510 Mail Loss/Rifling Program. Postal Service customers file complaints for mail loss or tampering using PS Form 1510. Depending on the customers' geographic location, their complaints are sent to the respective Postal Inspection Service division for investigative follow up.

Closed Case Files. The SISC maintains closed investigative case files for divisions within the geographic area for 2 years. After 2 years, the SISC transfers files to the Federal Records Center, which are retained for 15 years.

Freedom of Information Act Program. The SISC processes FOIA requests. When the SISC receives a FOIA request, SISC staff research, copy, track, and report the time it takes to assemble and forward the requests to Postal Inspection Service headquarters for processing.

Objective, Scope, and Methodology

Our objective was to determine whether the Postal Inspection Service's SISC effectively and efficiently supports the Postal Inspection Service's mission.

To accomplish our objective, we interviewed Postal Service and Postal Inspection Service officials, including the inspector in charge, Group 1, and SISC's security managers, supervisors, and technicians. Additionally, we reviewed policies and procedures for personnel security clearances, including Postal Service *Administrative Support Manual* 13⁶, Handbook AS-805, *Inspection Service Manual* (ISM), Management Instructions and applicable federal regulations.

Further, we reviewed and analyzed background security clearance information. We obtained this information from SISC personnel who stated this information was extracted from the SCTS.⁷ We assessed the reliability of the computer-processed data contained in the SCTS and noted several data integrity errors. Specifically, the SCTS had illogical date sequences, blank or unreasonable data fields, and missing records. However, we did not include the erroneous data in our analyses of background security clearances.

Also, we performed comparative analyses between the OPM's workload data and the SISC workload data to assess whether the SISC information on background security clearances was comparable to that of the OPM. Based on the analyses, the data was sufficiently reliable to support the findings and conclusions in this report.

We also reviewed statistical and management reports of security clearance requests received and processed for FYs 2004 and 2005. Specifically, we obtained the OPM workload and average timelines to compare the number of background security requests the SISC submitted to the OPM to the background security information the SISC staff provided to the U.S. Postal Service Office of Inspector General (OIG).

Further, we analyzed the average number of days⁸ for processing and granting interim and final security clearances and the average number of days it takes the

⁶ Updated with *Postal Bulletin* revisions through October 28, 2004.

⁷ SCTS is an automated system that monitors and tracks background security clearances and processes real-time information that cannot be recaptured.

⁸ Our analysis of interim and final clearances excluded computations resulting in a negative elapsed number of days and number of days appearing to be unreasonable (for example, year 2020).

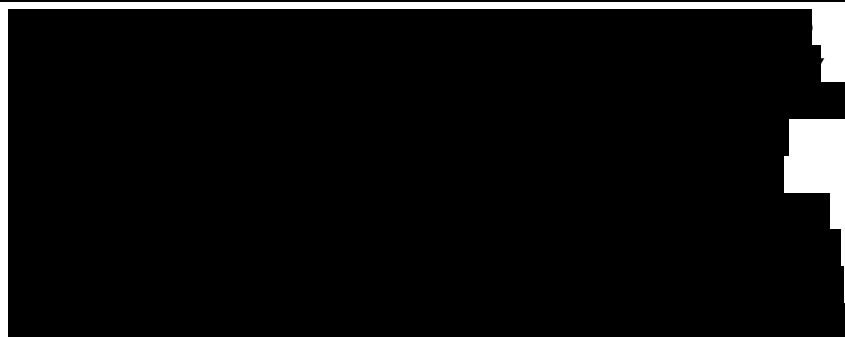
SISC to receive investigative results⁹ from the OPM. We did not assess the reliability of the data provided by the OPM. However, our comparison of the information provided by the SISC and that of the OPM determined that the investigative results were comparable. Therefore, we believe the data was sufficiently reliable to support the findings and conclusions in this report.

In addition, we reviewed training records for employees responsible for processing and adjudicating personnel security clearances to determine whether employees receive periodic training. We also reviewed the SISC's management of closed cases to determine whether files are adequately safeguarded and the SISC has an effective method of monitoring and tracking case files prior to transferring them to the Federal Records Center.

Further, we benchmarked with the Department of Homeland Security, Transportation Security Administration (TSA) to determine processes and procedures for managing and issuing background security clearances. However, we did not independently verify information received from the TSA.

We conducted this audit from October 2004 through April 2006,¹⁰ in accordance with generally accepted government auditing standards and included such tests of internal controls as we considered necessary under the circumstances. We discussed our observations and conclusions with management officials and included their comments where appropriate.

Prior Audit Coverage



⁹ Investigative results consist of: (1) Fingerprint-based national criminal history search of the FBI database, (2) FBI name check search of FBI's investigative files, (3) Defense Clearance Investigative Index (DCII) search of Department of Defense investigations, (4) OPM Security/Suitability Investigations Index (SII) search, and (5) Special Agreement Checks with Inquiries, which are inquiries to obtain employment and law enforcement history and as needed. Also, Military Personnel Records (MILR) are reviewed, as needed.

¹⁰ This was partially due to waiting for the Postal Inspection Service to provide additional information on the erroneous data in the SCTS, which we received in November 2005.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]



AUDIT RESULTS

**Security
Investigations
Service Center
Generally Supports
the Postal Inspection
Service's Mission**

The SISC generally followed policies and procedures to effectively and efficiently support the Postal Inspection Service's mission. Specifically, SISC staff safeguarded closed investigative case files against loss or theft and maintained these files for divisions within their geographic area for 2 years. After 2 years, these files are retained for 15 years at the Federal Records Center. Also, SISC staff processed FOIA requests as required.¹¹ All requests for information under FOIA should be sent to the Office of Counsel at Postal Inspection Service headquarters. SISC staff receives, researches, copies, tracks, and reports the time it takes to assemble and forward FOIA requests, and reports this information to Postal Inspection Service headquarters, Office of Counsel for processing.

However, opportunities exist to improve the overall management of the Background Security Clearance Program, personnel security training, and the 1510 Mail Loss/Rifling Program to more effectively and efficiently support the Postal Inspection Service's mission. During the audit, SISC staff initiated corrective actions to begin to address carryovers of background security clearance cases, personnel security training, and the 1510 Mail Loss/Rifling Program.

**Background Security
Clearance Program**

Postal Inspection Service officials could improve the overall management of the Background Security Clearance Program. Specifically, background investigation data provided by SISC staff showed the Postal Inspection Service had a carryover of approximately 9,700 open security clearance cases at the beginning of FY 2004, and 18,300 open security clearance cases at the beginning of FY 2005. We discussed our results with SISC staff during the audit. Based on our results, SISC staff conducted further analyses and stated they identified an unexplainable glitch in the SCTS. According to SISC staff, this glitch resulted in the SISC staff providing the OIG with inaccurate information on background security clearances.

Therefore, SISC staff requested that the OIG disregard the data we analyzed starting with the beginning of FY 2004, but instead analyze the data starting with the beginning of FY 2005. Additionally, in November 2005, SISC staff

¹¹ *Postal Bulletin 21929*¹¹ dated September 26, 1996, ISM, Section 165.212.

provided the OIG with a FY 2005 status report, including background security data, which showed there were approximately 5,700 sensitive and nonsensitive open clearances as of October 21, 2005.

After receiving the updated information from the SISC staff, the OIG determined the background security data provided beginning with FY 2004 was the same data that SISC had initially provided the OIG. Therefore, to further assess the data, the OIG analyzed the number of background investigation requests the SISC submitted to the OPM¹² and determined the number of requests was comparable (by at least 90 percent) to those the SISC staff initially provided the OIG. The results follow:

Table 1. Background Clearance Requests/Investigations (SISC Versus OPM)

FY	SISC Submitted to OPM ¹³	OPM Submitted to SISC ¹⁴
2004	58,435	53,431
2005	65,484	59,548

Unless the number of requests the OPM processed for the SISC staff was inaccurate, we cannot agree with management's assertion that SISC staff provided the OIG with information beginning in FY 2004 that was inaccurate. However, based on the November 2005 information the SISC staff provided, we acknowledge they have initiated corrective actions to address the number of carryovers. Thus, as of October 21, 2005, the SISC had about 5,700 open background investigation requests. Appendix A provides a schedule of open background investigation requests.

Detailed Analyses of Background Security Clearances. As requested by the Postal Inspection Service, we modified our analyses to use background security data beginning with FY 2005. Based on information from the SISC staff and the SCTS, as of the beginning of FY 2005, the SISC had a

¹² Represents data provided by the OPM, "Workload Average Timelines for U.S. Postal Inspection Service in Memphis, FY 2004 and up to July 2, 2005." Therefore, we extrapolated the number of requests for the remaining 3 months of the fiscal year.

¹³ Represents data provided by the OPM on background investigation requests the SISC submits to the OPM.

¹⁴ Represents data provided by the OPM on completed background investigations the OPM sent to the SISC.

carryover of about 18,300 open background investigation cases, and about 5,700 open background investigation cases as of October 21, 2005. In addition, the SISC experienced a 10.8 percent increase in its workload from FYs 2004 to 2005. Appendix A gives a schedule of background investigation requests.

Further, in FY 2004, the SISC granted 43,261¹⁵ final clearances, of which 41,789¹⁶ or 95 percent averaged 78 calendar days to process and grant final clearances to contract employees. Additionally, the SISC granted 5,211¹⁷ interim security clearances in FY 2004, which averaged 11 calendar days to process and grant interim clearances. This process was generally consistent with the SISC internal standard operating guidelines of 10 calendar days to process and grant clearances. Appendix B summarizes the average number of days to process and grant final and interim clearances in FY 2004.

SISC management stated that projections of security clearance workloads are based on historical information and the knowledge of any new programs or changes to be implemented. However, SISC personnel stated that the Postal Service and Postal Inspection Service do not provide any reports, projections of new hires, or workload requirements to assist SISC management with more effectively assessing workload.

Furthermore, SISC personnel stated any delays in processing background security clearance requests were primarily due to delays in receiving investigative results¹⁸ from the OPM. We analyzed statistics for background security clearance requests received from the OPM to estimate the average number of days to receive investigative results from the OPM.

Based on our analyses of the 32,341¹⁹ security clearance requests the OPM processed for SISC in FY 2004, 28,365,

¹⁵ The 43,261 final clearances granted excluded 43 final clearances granted based on reciprocity.

¹⁶ The 41,789 excludes the 1,472 clearances with negative elapsed days.

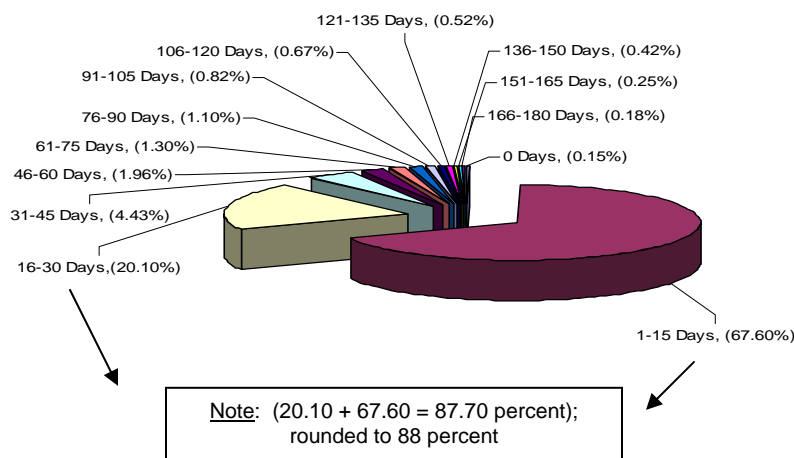
¹⁷ The 5,211 excludes the 164 clearances with negative elapsed days.

¹⁸ Investigative results consist of fingerprint-based national criminal history searches of the FBI database; FBI name check searches of the FBI's investigative files; the DCII search of Department of Defense Department investigations; searches of the OPM Security/Suitability Investigations Index (SII); Special Agreement Checks with Inquiries, in which inquiries are sent to obtain employment and law enforcement history; and as needed, reviews of MILR.

¹⁹ SISC records indicate 38,987 Case Closing Transmittals were received from the OPM in FY 2004. The OIG excluded records in which the date submitted to the OPM preceded the date sent to the OPM, elapsed days were negative, date fields were blank, and date fields were questionable.

or 88 percent, were processed and returned to the SISC between 1 and 30 days, with an average of 19 calendar days. Therefore, we did not find major instances in which the OPM caused delays in issuing investigative results to the SISC. The following chart shows the average timeframes for the OPM to process the requests.

Table 2. Percentages and Average Timeframes for OPM Clearances Processed



Further, the Postal Inspection Service's FY 2004 Annual Performance Plan²⁰ identified an initiative for the Postal Inspection Service to continue an ongoing collaborative effort with the OPM to minimize delays in receiving National Agency Checks and ensure timely receipt of OPM reports. Therefore, any delays or carryovers would result in untimely requests and would not be consistent with the performance plan.

Benchmarking Results. Our benchmarking results for similar searches and inquiries performed by the OPM determined that the average number of days to provide investigative results for the TSA was between 2 and 65 days. Therefore, the amount of time it took for the OPM to provide investigative results to SISC was consistent with the timeframes for the TSA.

²⁰ The Annual Performance Plan is a guide for the Postal Inspection Service over a 12-month period that sets forth operational and transformational objectives and provides a linkage between its long-term goals and the work that is performed on a day-to-day basis.

Data Integrity Errors. The OIG further identified 6,646 records with data integrity errors for background investigation data in the SCTS database. Although Postal Inspection Service officials requested that we include all records in our analyses, we did not include those records with questionable or unreasonable dates because erroneous data would distort the overall results of our audit. An illustration of the errors follows:

Table 3. SCTS and Erroneous Data

Description of Database Errors	Records with Errors
Blank Dates for Date Received	1,141
Negative Elapsed Days for Processing Security Clearances	5,503
Final Clearances Issued Showing a Future Date	2
Total Records with Errors	6,646

The background investigation process is essential to managing the inherent risk of allowing Postal Service employees and other personnel access to sensitive or proprietary information. To ensure effective management of the security clearance process, security clearance data must be consistent, accurate, and complete. This assists management with making decisions regarding current workload requirements and the overall management of the Background Security Clearance Program.

Recommendation

We recommend the Chief Postal Inspector:

1. Establish a comprehensive management plan to address erroneous data in the Security Clearance Tracking System and reduce its carryovers of background investigations.

Management's Comments

Management disagreed with this recommendation, stating that the reason for blank dates, negative elapsed days for processing, and final clearances showing future dates, was data manipulation problems the OIG experienced when conducting analysis of data they supplied to OIG via

compact disc, not because the data in the SCTS was erroneous.

Management also stated that, "carryover" data is not the same as "backlogged" or "delayed" data and that carryovers will always exist from one day to the next, and thus from one year to the next. Further, they said the recommendation implied that average processing time was excessive, and that nothing in the report supports that assertion. The SISC security clearance processing time "from end-to-end" is within processing standards, similar to other government agencies.

**Evaluation of
Management's
Comments**

We disagree with management's assertion that the OIG experienced data manipulation problems when conducting analysis of security clearance data, resulting in blank dates, future dates, and negative elapsed days for processing. SISC officials provided the OIG with data on CD that could not be modified (read-only); therefore, the OIG could not manipulate the data. Further, SISC personnel provided the OIG with a written summary of interim and final clearances that we used to validate the data on the CD. Additionally, during our review of security clearance data, we notified SISC personnel of the erroneous data we identified and excluded it from our analysis.

Additionally, the OIG did not conclude or report that processing times were excessive. The OIG concluded that carryovers in FYs 2004 and 2005 did not result from delays in processing background security clearances by OPM. Further, based on additional analyses, SISC staff did not process requests in FY 2005 as quickly as they received them, and in FY 2006, the backlog appeared to grow. For example, in FY 2005, the average number of requests was about 6,940 and the average number completed was about 5,280, resulting in an average carryover of about 1,660 per month. Although management did not agree with this recommendation, we do not plan to pursue this recommendation through the formal audit resolution process.

**Personnel Security
Training**

SISC security personnel managing and implementing personnel security policies have not received formal personnel security training within the past 5 fiscal years. This occurred because the Postal Inspection Service is not required to provide annual and refresher training to staff who

process security clearance requests. The Postal Inspection Service follows the guidelines and procedures for training outlined by the Postal Service's Corporate Training and Development Department in the *Employee and Labor Relations Manual* (ELM) 710. The ELM requires that employees be provided with both formal and informal learning experiences that contribute to individual growth and improve performance in current and future jobs.

Our review of training records from FY 2000 to the third quarter of FY 2005 determined that 12 of the 15 employees who processed background security clearances had not received training in personnel security or the security clearance process in the past 5 fiscal years. The remaining three employees received internal on-the-job training from the SISC security staff.

Postal Inspection Service management stated the SISC has a Process Management Review Team that reviews all current processes, including the background security clearance program. In addition to reviewing the process, the team interviews employees to determine whether they have the tools needed to perform their job responsibilities. The SISC has also adopted a quality assurance program, which requires a supervisor to review every case that involves a denial and every 20th case for all specialists.

Postal Inspection Service management acknowledged the importance of employees receiving annual and refresher training to maintain skills, applying consistent standards and processes, and identifying and discussing changes that affect security and the SISC's and Postal Inspection Service's mission. Without annual and refresher training, SISC security personnel could miss opportunities to identify emerging trends with personnel security, which could pose a risk to the Postal Service's security interests. During the audit, SISC staff initiated corrective actions to obtain supplemental personnel security training for SISC employees.

Recommendation

We recommend the Chief Postal Inspector:

2. Ensure Security Investigations Service Center security personnel are provided formal annual and refresher training to supplement personnel security training.

Management's Comments	Management agreed with this recommendation, stating supervisors and managers will obtain annual background clearance training through the OPM, U.S. Department of Agriculture, or other acceptable sources. Also, the SISC will continue to look for ways to improve and streamline the security clearance process.
Evaluation of Management's Comments	Management's comments and planned corrective actions are responsive and satisfy the intent of the recommendation and should correct the issues identified in the finding.
1510 Mail Loss/Rifling Program	<p>The Postal Inspection Service's 1510 Mail Loss/Rifling Program is being implemented as required.²¹ The Postal Inspection Service's Service Centers (formerly known as Postal Inspection Service Operations Support Groups) manage the 1510 Program. Postal Service customer complaints regarding mail loss, theft, and tampering are forwarded to the appropriate service center responsible for the geographical area in which the complaints were mailed.</p> <p>SISC personnel determine whether the alleged item reported as lost, stolen, or tampered with is attractive or unattractive and, depending upon the customer's address, distribute the complaint to the appropriate Postal Inspection Service division for investigative follow up. [REDACTED]</p> <p>[REDACTED]</p> <p>Specifically, in FY 2004, the SISC [REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p>

²¹ *Postal Bulletin 22013*, dated December 16, 1999.

[REDACTED]

After providing Postal Inspection Service officials our audit results, they initiated corrective actions to address the issues with the 1510 Mail Loss/Rifling Program. The officials advised all PS Forms 1510 will be forwarded to the Postal Inspection Service Criminal Investigative Service Center (CISC) and sent to the appropriate division for the inspectors to review. We will further assess the 1510 Mail Loss/Rifling Program during our future audit of the CISC.

Recommendation

We recommend the Chief Postal Inspector:

3. [REDACTED]

**Management's
Comments**

Management agreed with this recommendation and stated Postal Inspectors use the [REDACTED]

[REDACTED] Included in the database are mail loss reports received by Postal Service call centers, mail loss complaints entered online via the Internet, and paper PS Forms 1510 manually input into the database. Additionally, effective October 1, 2005, the CISC began consolidating and sending all paper PS Forms 1510 to the appropriate field divisions for input in the FCD and subsequent review by inspectors.

**Evaluation of
Management's
Comments**

Management's comments and planned corrective actions are responsive and satisfy the intent of the recommendation and should correct the issues identified in the finding.

APPENDIX A. FISCAL YEARS 2004 AND 2005 SCHEDULE OF SECURITY INVESTIGATIONS SERVICE CENTER OPEN CASES

Description	FY 2004	FY 2005
Beginning Balance for FY	9,731	18,389
Cases Added during FY	58,435	65,484 ²²
Total:	68,166	83,873
Less Cases Completed during FY	49,777	69,143 ²³
Total Open Cases: (As of Beginning of the FY)	<u>18,389</u>	<u>14,730</u>
Total Open Cases: (As of October 21, 2005)		<u>5,766</u>

²² Represents a 10.8 percent increase from FYs 2004 to 2005.

²³ This total does not include top secret clearances granted, top secret clearances updates, updates granted, denials, and disqualifications.

APPENDIX B. FISCAL YEAR 2004 AVERAGE NUMBER OF DAYS²⁴ TO PROCESS AND GRANT FINAL AND INTERIM SECURITY CLEARANCES

FY 2004 Final Clearances

Category ²⁵	Number of Clearances	Number of Days	Average Number of Days	Percentage of Total Clearances
CONTRACT EMPLOYEES:				
Ground Handlers	1,543	151,873	98	
HCR Drivers	12,173	1,087,189	89	
APS/Pinkerton	64	5,086	79	
THS	995	77,060	77	
Airline	19,337	1,468,621	76	
Contract USPIS	279	13,434	48	
Contract USPS	4,593	249,147	54	
Unarmed Security Guard	113	7,827	69	
Other ²⁶	439	17,360	39	
Subtotal:	39,536	3,077,597	78	95
CAREER EMPLOYEES:				
USPIS	155	7,460	48	
Casual USPS	625	21,761	35	
USPS	438	28,633	65	
Other ²⁷	1,035	23,887	23	
Subtotal:	2,253	81,741	36	5
TOTAL:	41,789	3,159,338	76	100

²⁴ Average number of days equals the total number of days divided by the total number of clearances.

²⁵ HCR – Highway Contract Route, APS – No Definition for the Acronym, and THS – Terminal Handling Service.

²⁶ Includes contract employees for the Call Center, CAS Airline, contract fraud analysts, Hub and Spoke Program (HASP), Y2K (Year 2000), and Wackenhut.

²⁷ Includes blank fields (categories that were not identified).

FY 2004 Interim Clearances

Category	Number of Clearances	Number of Days	Average Number of Days	Percentage of Total Clearances
CONTRACT EMPLOYEES:				
Call Center	432	2,810	7	
Unarmed Security Guard	141	1,981	14	
Contract USPS	3,749	37,693	10	
Contract USPIS	199	3,225	16	
Other ²⁸	85	2,642	31	
Subtotal:	4,606	48,351	10	88
CAREER EMPLOYEES:				
USPS	339	5,822	17	
USPIS	72	1,233	9	
Other ²⁹	194	1,927	10	
Subtotal:	605	8,982	15	12
TOTAL:	5,211	57,333	11	100

²⁸ Includes contract employees for the APS/Pinkerton, CAS Airline, contract fraud analysts, Hub and Spoke Program (HASP), Y2K (Year 2000), Wackenhut, ground handlers, casual USPS, and HCR drivers.

²⁹ Includes blank fields (categories that were not identified) and a security control officer (SCO).

APPENDIX C. MANAGEMENT'S COMMENTS



UNITED STATES POSTAL INSPECTION SERVICE

Deputy Chief Inspector
Headquarters Operations

February 3, 2006

Kim H. Stroud
Director, Audit Reporting
USPS Office of Inspector General
1735 North Lynn Street
Arlington, VA 22209-2020

SUBJECT: Inspection Service response to the Qualitative Assessment Review
Postal Inspection Service's Security Investigations Service Center
(Report Number SA-AR-06-DRAFT)

The following represents the Postal Inspection Services' response to the USPS-OIG qualitative assessment review (QAR) of the Security Investigations Service Center (SISC).

Again, we appreciate the opportunity to provide comments in this report. Please contact Juliana Nedd, Inspector in Charge, Group 1-Security, at (202) 268-4547, if you have any questions.

A handwritten signature in black ink, appearing to read "L. E. Maxwell".

L. E. Maxwell
Deputy Chief Inspector

Attachment:

cc: L. R. Heath, Chief Postal Inspector
Z. Hill, Assistant Chief Inspector, Investigations and Security
J. Nedd, Inspector in Charge, Group 1 – Security

475 L'Enfant Plaza West SW, Room 3010
WASHINGTON DC 20260-2170
TELEPHONE: 202-268-5015
FAX: 202-268-4563

Response to USPS-OIG Audit of the Postal Inspection Service
Security Investigative Service Center (SISC)

Summary of Management Responses

We have reviewed the draft Qualitative Assessment Review – Postal Inspection Service's Security Investigations Service Center (SA-AR-06-DRAFT) dated January 6, 2005. This memorandum represents our formal response to the three recommendations addressed to the Chief Postal Inspector. In summary, we agree in part with the recommendations.

OIG Recommendation No. 1

Establish a comprehensive management plan to address erroneous data in the Security Clearance Tracking System and reduce its carryovers of background investigations.

Management Response

Management disagrees with this recommendation. As was explained to OIG audit personnel, the reason for blank dates, negative elapsed days for processing, and final clearances showing future dates, was because of data manipulation problems the OIG experienced when conducting analysis of data we supplied to them via CD; not because the data in the SCTS was erroneous. As was also explained to OIG audit personnel, "carryover" data is not the same as "backlogged" or "delayed" data. Carryover background security clearances will always exist from one day to the next; and thus from one year to the next. The implication in the recommendation is that average processing time was excessive. Nothing in the report supports that assertion. The SISC security clearance processing time "from end-to-end" is within processing standards; similar to other government agencies.

OIG Recommendation No. 2

Ensure SISC security personnel are provided formal annual and refresher training to provide supplemental personnel security training.

Management Response

Management agrees with this recommendation. Supervisors and managers will obtain annual background clearance training through programs offered by the Office of Personnel Management, U.S. Department of Agriculture, or other acceptable sources. The SISC will continue to look for ways to gain efficiencies, improve and streamline the security clearance process.

OIG Recommendation No. 3

[REDACTED]

Management Response

Management agrees with this recommendation. [REDACTED]
[REDACTED] for review and analysis of mail loss reports. Included in the database are mail loss reports received by USPS call centers, mail loss complaints entered online via the internet, and paper PS Forms 1510 manually input into the database. Effective October 1, 2005, the Inspection Service Criminal Investigative Service Center (CISC) began consolidating and sending all paper PS Forms 1510 to the appropriate field divisions for input into the FCD and subsequent review by inspectors.