February 12, 2008

ALEXANDER E. LAZAROFF
CHIEF POSTAL INSPECTOR

DEBORAH M. GIANNONI-JACKSON
VICE PRESIDENT, EMPLOYEE RESOURCE MANAGEMENT

SUBJECT: Management Advisory – Review of the Postal Service's Personnel Security Process (Report Number SA-MA-08-001)

This report presents the results of our self-initiated review of the Postal Service's personnel security process (Project Number 07YG055SA000). We conducted this review to examine the Postal Service's personnel security processes and compare them with processes of other federal and selected private sector entities. This is one in a series of reviews we plan to conduct in this area. See Appendix A for additional information about this review.

Background

The Postal Service must maintain public trust and security of the mail as well as assure confidence in the reliability and integrity of its employees. Employees have the right to expect a safe work environment, and the public has a right to expect the Postal Service to maintain the privacy of the mail. Federal law makes it clear that protection of mail, Postal Service funds, and property is the responsibility of every Postal Service employee.

The Postal Service must ensure that individuals selected for employment have been carefully screened, evaluated, and determined suitable for Postal Service employment so the conduct of these individuals will reflect favorably on the organization.[1] The Postal Service's personnel security process encompasses screening for suitability and granting security clearances. All Postal Service employees undergo a suitability screening; in addition, depending on their positions, some employees may need security clearances, which require a more extensive background investigation.

A suitability screening determines whether applicants possess the necessary skills, abilities, and qualifications to perform various jobs in the Postal Service. The suitability screening process is designed to disqualify ineligible or unsuitable applicants. The Postal Service's Human Resources Selection Evaluation and Recognition Office

[1] Postal Handbook EL-312, *Employment & Placement,* Section 511.11, Rights to Workplace Safety & Mail Security, September 2001. Postal Service Handbook AS-805, *Information Security*, Chapter 5, Personnel Security, Policy & General Requirements, March 2002 (updated with *Postal Bulletin* revisions through November 23, 2006).

provides suitability guidance to area and district human resources (HR) personnel throughout the country. When evaluating and determining an applicant's suitability, HR personnel conduct, at a minimum, the following checks: age, employment, criminal and military service history, a National Agency Check with Inquiries (NACI)[2] for career applicants, and a Special Agency Check with Inquiries (SACI)[3] for noncareer applicants. The Office of Personnel Management (OPM) conducts the NACI and SACI, which include a Federal Bureau of Investigation (FBI) fingerprint check, for the Postal Service.

The Chief Postal Inspector or designee is responsible for issuing security clearances. If an employee needs a security clearance, the type of clearance granted depends on the sensitivity of the position held. A sensitive clearance is considered for employees who have access to sensitive information restricted to the highest levels of the federal government, U.S. Postal Service Office of Inspector General (OIG) files, U.S. Postal Inspection Service (USPIS) files, national security (classified) information, or sensitive information essential to executive decision making. The sensitive level of clearance within the Postal Service encompasses both national security[4] and public trust[5] positions.

Postal Service employees who require a security clearance undergo a more extensive background investigation. A background investigation is conducted to help develop information about the person's character, reputation, and allegiance to the United States to determine eligibility for appointment to, or suitability for retention in, a Postal Service position. OPM guidance for conducting background investigations establishes specific personnel security criteria and procedures for the federal government. Although the Postal Service is not subject to Title 5 of the Code of Federal Regulations (CFR),[6] it generally follows OPM guidance when conducting background investigations and also utilizes OPM to conduct portions of the investigation. Background investigations and the issuance of proper security clearances are key elements in protecting national security, ensuring the integrity of the mail, and protecting Postal Service employees, customers, and assets.

[2] The NACI is a background investigation inquiry that includes FBI name check, fingerprint check of the FBI's criminal arrest database, Defense Clearance Investigation Index check, OPM Security/Suitability Investigations Index check, and a local law enforcement check of an applicant's residence, employment, and education for the last 5 years.
[3] The SACI includes the same checks as the NACI with the exception of a FBI name check, education verification, reference checks, and residence checks.
[4] National security clearances include Confidential, Secret, Top Secret, and Sensitive Compartmented Information.
[5] *Administrative Support Manual 13*, Section 272, Personnel Security Clearance, July 1999 (updated with *Postal Bulletin* revisions through December 2006) states that public trust positions are responsible for managing programs or operations that require a high degree of public trust because of their ability to affect the accomplishment of the activity's mission to a significant degree.
[6] Title 5 CFR establishes federal government guidelines, criteria, and procedures for hiring practices. Specifically, 5 CFR 731 addresses suitability requirements; 5 CFR 732 pertains to national security positions; and 5 CFR 736 pertains to personnel investigations.

Results

The Postal Service's personnel security processes and procedures for conducting background checks and granting security clearances were comparable to those used by other federal agencies and private sector entities. For example, an applicants' age, prior employment, fingerprints, criminal record, military service, and selective service status are checked to determine whether an applicant is suitable for employment. See Appendices B and C for detailed benchmarking results.

However, in our benchmarking, we noted differences in the following two areas: background checks of contract employees, and policies requiring employees to report arrests and convictions. The Postal Service could potentially reduce its security risk to employees, customers, the mail, and critical assets if it adopted policies and procedures in these areas similar to those used by some of the benchmarked agencies.

Background Checks of Contract Employees

Contractors are defined as individuals who provide services to the Postal Service and have access to occupied Postal Service facilities, information and resources, including computer systems. These individuals must obtain clearance from the Postal Service before being provided that access. Postal Service procedures require contractors to certify that contract employees have met suitability and security requirements. In addition, for a basic clearance, the Postal Service contracting officer, contracting officer's representative (COR), or designee verifies the data submitted by contractors, with no involvement from HR.

The Postal Service issues four levels of clearances for contractors: basic, non-sensitive, sensitive, and interim-sensitive. See Table 1 for contractor clearance levels.

Table 1: Levels of Clearances Granted to Postal Service Contract Employees

Level of Clearance	Definition
Basic	Clearance required for individuals who have access to Postal Service facilities, but do not require a higher level of clearance.
Non-sensitive	Clearance required for individuals who have access to Postal Service information that, if compromised, would have limited impact on the mission of the Postal Service; or who have restricted access to Postal Service computer systems such as word processing or data entry.
Sensitive	Clearance required for individuals who have access to information that, if compromised, would cause significant financial loss, inconvenience, or delay in the performance of the mission of the Postal Service; or who have physical access to restricted areas in Postal Service facilities, such as computer rooms and tape libraries; or who have access to computer systems such as on-site or remote terminals for systems development or accessing sensitive systems or data.
Interim-sensitive	Preliminary clearance granted for individuals for whom there is a priority need to begin work before completion of a sensitive clearance.

The level of clearance issued is determined by the scope and the nature of the work the individual will perform. At the time of the contract award, the Postal Service contracting officer, COR, or designee provides the contractor with the required clearance forms and receives the forms back from the contractor upon completion. The contracting officer, COR, or designee reviews these forms for completeness and adequacy. For a basic clearance, if the information provided by the contractor is satisfactory, the contracting officer, COR, or designee authorizes issuance of an identification badge to the contract employee.[7] For a higher clearance (non-sensitive, sensitive, or interim-sensitive), the contracting officer, COR, or designee reviews the forms submitted by the contractor and forwards them to the Security Investigations Service Center (SISC) for review and issuance of a security clearance. Individuals may begin work when they receive notification that the security clearance has been granted.

Benchmarking Results

The Social Security Administration (SSA), Internal Revenue Service (IRS), and Tennessee Valley Authority (TVA) do not rely on contractor certifications to ensure that contract employees meet personnel security requirements. These agencies' HR or personnel security departments, rather than the contracting officers, make suitability determinations for contract employees.

Potential Gap

Postal Service HR personnel do not certify or verify whether contract employees who require basic clearances have met Postal Service security requirements. Allowing contractors to certify that their employees meet Postal Service security requirements and relying on the contracting officer, COR, or designee to verify the data provided by the contractor could expose Postal Service employees, customers, the mail, and critical assets to unnecessary risk. Alternatively, certification or verification by HR or security personnel could help ensure all contract employees meet security requirements and potentially reduce the risk.

Policy Requiring Employees to Report Arrests and Convictions

Except for a policy covering sex offenders, Postal Service policy does not specifically require Postal Service employees to inform management if they are arrested or convicted. According to the principles of ethical conduct set forth in the Postal Service's *Employment and Labor Relations Manual*, employees must not engage in criminal, dishonest, notoriously disgraceful, immoral, or other conduct prejudicial to the Postal Service. Conviction for a violation of any criminal statute may be grounds for disciplinary action against an employee, including removal of the employee, in addition to any other penalty imposed by law. However, Postal Service policy does not

[7] The contracting officer, COR, or designee may allow individuals who are needed immediately by Postal Service management to have limited access to the Postal Service facility for up to 2 weeks, under the supervision of a Postal Service employee, pending the receipt of the completed certifications for the basic clearance.

specifically state that employees must report violations of federal and state laws resulting in arrests and convictions to management or the OIG.

Benchmarking Results

We benchmarked with two entities that require all or segments of their employees to report arrests and convictions. TVA, which is an excepted service agency like the Postal Service, has adopted a policy that specifically requires regular and contract employees to notify their supervisor if they are arrested or charged with any criminal act. Similarly, employees at one of the private sector entities we benchmarked with have unescorted airport access privileges and are subject to the Transportation Security Administration's (TSA) mandated self-disclosure policy. This policy requires employees with unescorted airport access to report convictions and criminal offenses to management within 24 hours.[8]

Potential Gap

The Postal Service does not condone employee criminal behavior. By regulation, Postal Service employees who are convicted of a violation of a criminal statute can be subject to disciplinary action up to and including dismissal.[9] Current Postal Service policy conveys the sense that Postal Service employees are expected to obey the law and can be dismissed if they do not. However, the policy does not require Postal Service employees to report their criminal arrests and convictions to anyone in the Postal Service, except for convicted sex offenders. A policy requiring employees to report arrests and convictions could reduce the risk of exposure for Postal Service employees, customers, the mail, and critical assets.

We did not make any recommendations concerning these two issues in this report, however we may address them further in future audits of the Postal Service's personnel security processes and procedures. Although the OIG did not make recommendations, we did provide Postal Service management with the opportunity to comment on any issues identified in the report. The Vice President, Employee Resource Management, provided comments which are included in their entirety in Appendix D.

[8] TSA requires employees to report criminal offenses such as importation or manufacture of a controlled substance, extortion, bribery, rape, or aggravated sexual abuse and murder. The policy lists approximately 30 offenses that should be reported.

[9] Postal Service *Employment and Labor Relations Manual* (ELM 18), Section 665.16 Behavior and Personal Habits, June 2007 gives the Postal Service standards of conduct.

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

E-Signed by Darrell E. Benjamin,
VERIFY authenticity with ApproveIt

Darrell E. Benjamin, Jr.
Deputy Assistant Inspector General
for Support Operations

Attachments

cc: Michele L. Culp
Juliana Nedd
Mangala P. Gandhi
Katherine S. Banks

APPENDIX A: ADDITIONAL INFORMATION

Objective, Scope, and Methodology

Our objective was to assess the Postal Service's personnel security processes and procedures to determine whether they were comparable to other federal agencies and selected private sector entities. The scope of our review entailed a review of the Postal Service's personnel security processes for regular and contract employees, including suitability screening, background investigations, and security clearances.

To accomplish our objective, we obtained and reviewed applicable criteria, laws, regulations, Postal Service policies and procedures, and other documentation pertaining to our objective. We conducted interviews with Postal Service and USPIS personnel at headquarters and at the SISC in Memphis, Tennessee. We also conducted interviews with OPM personnel and other personnel deemed pertinent to this review. We benchmarked with the following federal and private sector entities to obtain an understanding of their personnel security processes: IRS, SSA, TVA, United Parcel Service (UPS), and Dalsey, Hillblom, and Lynn (DHL). We selected these entities because of their: exposure to the public, excepted service status,[10] or business in the mailing industry. We assured the private sector entities that any information they provided would be used strictly for comparative purposes and would not be directly attributed to their organization in our report. As a result, the report does not identify the private sector entities regarding specific practices, policies, or procedures.

We conducted this review from July 2007 through February 2008 in accordance with the President's Council on Integrity and Efficiency, *Quality Standards for Inspections*. We discussed our observations and conclusions with management officials on November 28, 2007 and included their comments where appropriate.

Prior Audit Coverage

The OIG issued three audit reports related to the personnel security process within the past 3 years:

- *Separation of Duties at the Eagan, Minnesota; San Mateo, California; and St. Louis, Missouri Information Technology and Accounting Service Center* (Report Number IS-AR-07-017, dated August 29, 2007) – This report stated that, generally, policies, procedures, and internal controls were adequate to separate duties for personnel with access to critical information system resources at the data centers. However, controls to determine which career employees required sensitive security clearances needed strengthening. We recommended and management agreed to: assess the risk of the duties of all Information Technology (IT) and Accounting Service Center (ASC) positions; establish

[10] Excepted service agencies are not subject to the appointment, pay, and classification rules in Title 5, United States Code. However, they are subject to veterans' preference.

periodic reassessment of such risks; establish a central location to maintain a list of sensitive positions; notify the USPIS when new IT and ASC positions are created or a new employee is hired; and appropriately amend the *Administrative Support Manual*, Issue 13, Chapter 2, Section 272.

- *Inspection Service Security Investigations Service Center* (Report Number SA-AR-06-002, dated April 20, 2006) – This report stated that the SISC generally followed policies and procedures for managing and safeguarding closed cases and processing Freedom of Information Act requests. However, opportunities existed to improve the overall management of the background security clearance program, personnel security training, and the 1510 Mail Loss/Rifling Program to better support the USPIS mission. During the audit, SISC staff took corrective actions to address carryovers for background security clearances, personnel security training, and the 1510 Mail Loss/Rifling Program. Management agreed to ensure that SISC personnel receive formal annual and refresher training; and that postal inspectors review all Postal Service Form 1510, Mail Loss/Rifling, complaints before the complaints are destroyed. Management disagreed with establishing a comprehensive management plan to address erroneous data in the Security Clearance Tracking System and reduce its carryover of background investigations.

- *Audit of Personnel Security Controls at the Eagan, San Mateo, and St. Louis Information Technology and Accounting Service Centers* (Report Number IS-AR-04-011, dated September 8, 2004) – This report identified no exceptions in the review of initial security clearances and updates for contractors. However, the report concluded that the Postal Service did not consistently obtain security clearance updates for career employees. We recommended that the Vice President, Chief Technology Officer, direct the Security Control Officers in St. Louis and San Mateo to process security clearance updates as required for all Postal Service employees assigned to sensitive positions at the IT and ASCs. Management agreed with the recommendation.

APPENDIX B: SUITABILITY RESULTS

Employee and Contractor Suitability Results						
	Postal Service	TVA	SSA	IRS	Private Sector Entity A	Private Sector Entity B
Background Checks	District or area HR office conducts investigation for regular employees; contractor or vendor conducts investigation for contract employees.	Personnel security office conducts investigation in accordance with risk level for employees and contractors.	Suitability security office conducts investigation in accordance with risk level for employees and contractors.	Personnel security office conducts investigation in accordance with risk level for employees and contractors.	HR office conducts investigation in accordance with risk level for employees and contractors.	HR office conducts investigation in accordance with risk level for employees and contractors.
Adjudication	District HR manager or designee for Postal Service employees; contractor or vendor for contract employees.	Personnel security and suitability office for employees and contractors.	Suitability security office for employees and contractors.	Labor relations office for employees; personnel security office for contractors.	HR office for employees and contractors.	HR office for employees and contractors.
Reinvestigations	No system in place for regular or contract employees.	No system in place for regular employees. Fingerprint check upon contract renewal for contract employees.	No system in place for regular employees. Fingerprint check every 5 years for contract employees.	Every 5 years for employees in high-risk positions, such as criminal investigators and executives. Every 5 years for all contractors.	No system in place.	No system in place.
Arrest and Conviction Policy	No policy.	Policy requiring employees and contractors to report arrests and convictions to management.	No policy.	No policy.	No policy.	Employees and contract employees with unescorted airport access are subject to TSA policies, which require them to report convictions within 24 hours.

APPENDIX C: SECURITY CLEARANCE RESULTS

Employee and Contractor Security Clearance Results						
	Postal Service	TVA	SSA	IRS	Private Sector Entity A	Private Sector Entity B
Background Checks	**FOLLOW OPM GUIDANCE** Applicants must undergo a background investigation. Minimum investigative requirements correlate to risk levels.	**FOLLOW OPM GUIDANCE** Applicants must undergo a background investigation. Minimum investigative requirements correlate to risk levels.	**FOLLOW OPM GUIDANCE** Applicants must undergo a background investigation. Minimum investigative requirements correlate to risk levels.	**FOLLOW OPM GUIDANCE** Applicants must undergo a background investigation. Minimum investigative requirements correlate to risk levels.	No federal security clearances.	No federal security clearances.
Adjudication	Security Investigations Service Center.	Personnel security office.	Suitability security office.	Labor relations office.	No federal security clearances.	No federal security clearances.
Reinvestigations	Follow OPM guidelines.	Follow OPM guidelines.	Follow OPM guidelines.	Follow OPM guidelines.	No federal security clearances.	No federal security clearances.
Arrest and Conviction Policy	No policy.	Policy requiring employees and contractors to report arrests and convictions to management.	No policy.	No policy.	No federal security clearances.	Employees and contract employees with unescorted airport access are subject to TSA policies, which require them to report convictions within 24 hours.

APPENDIX D: MANAGEMENT'S COMMENTS

DEBORAH GIANNONI-JACKSON
VICE PRESIDENT
EMPLOYEE RESOURCE MANAGEMENT

UNITED STATES
POSTAL SERVICE

January 18, 2008

DARRELL E. BENJAMIN, JR.

SUBJECT: Management Response to the Draft Management Advisory – Review of the Postal Service's Personnel Security Process (Report Number SA-MA-08-DRAFT)

We appreciate the opportunity to provide comments to the management advisory report of the review of the Postal Service's Personnel Security Process. The attached represents Employee Resource Management's response.

Upon review, we do not believe any portion of this report is exempt from disclosure under the Freedom of Information Act.

If you have any questions, please feel free to contact Mangala Gandhi, Manager, Selection, Evaluation, and Recognition, at 202-268-3793.

for Deborah Giannoni-Jackson

Attachment

475 L'ENFANT PLAZA SW, ROOM 9840
WASHINGTON, DC 20260-4200
FAX: 202-268-3800
WWW.USPS.COM

cc: A. Lazaroff, Chief Postal Inspector
J. Nedd, Inspector in Charge, Security Group
M. Gandhi, Manager, SER
Lucine M. Willis - Electronic Copy
Katherine Banks - Electronic Copy

Response to USPS Office of Inspector General Management Advisory: Review of Personnel Security Process

Potential Gap No. 1

Postal Service HR personnel do not certify or verify whether contract employees who require basic clearances have met Postal Service security requirements. Allowing contractors to certify that their employees meet Postal Service security requirements and relying on the contracting officer, COR, or designee to verify the data provided by the contractor could expose Postal Service employees, customers, the mail, and critical assets to unnecessary risk. Alternatively, certification or verification by HR or security personnel could help ensure all contract employees meet security requirements and potentially reduce the risk.

Management Response

The Headquarters (HQ) office of Selection, Evaluation, and Recognition (SER) develops policies and procedures for screening *employees*. Policies specifying security requirements for *contractors* are developed by the Postal Inspection Service and are found in the Administrative Support Manual (ASM).

For highway transportation contractors, the policy is supplemented by a Management Instruction (updated in 2004) which requires non-sensitive security clearances and specifies clear roles and responsibilities for Inspection Service personnel, administrative officials, and network operations management. The ASM specifies that non-sensitive clearances are also required for individuals (including annuitants) providing contract services, including contractors' employees such as Manpower temporaries.

When contracts are awarded to external vendors for specific services requiring their employees or subcontractors to have access to postal information and/or resources, the statement of work contains standard but very specific security requirements including clearances for personnel and site security reviews jointly conducted by Inspection Service and Corporate Information Security personnel to protect the interests of the Postal Service and reduce risk.

Thus, non-sensitive clearances are required for the majority of contractors with access to facilities, postal information, and resources. Non-sensitive clearances are processed and tracked by the Inspection Service in Memphis, Tennessee, to ensure the individuals meet security requirements. Inspection Service facility security reviews include reviews of contractors to ensure compliance with security policy. Adding a layer of certification or verification by Human Resources would add very little control and needlessly and significantly increase the workload in Human Resources.

The remaining contractors are those who provide services under local buying authority (e.g., snow removal in parking lots). The ASM policy requires the contracting postal manager to take reasonable security precautions before allowing these individuals to enter a postal facility, such as examining their past job performances, local criminal histories, and knowledge of their respective companies. This has proven an effective process that eliminates delays and keeps the Postal Service from absorbing the significant costs of drug screening, criminal record checks, and motor vehicle record checks (where appropriate). It is unlikely that significant security gains would be achieved by expanding the scope of Human Resources' responsibilities to perform such screening or to verify that the contracting postal manager took adequate safety precautions.

Potential Gap No. 2

The Postal Service does not condone employee criminal behavior. By regulation, Postal Service employees who are convicted of a violation of a criminal statute can be subject to disciplinary action up to and including dismissal. Current Postal Service policy conveys the sense that Postal Service employees are expected to obey the law and can be dismissed if they do not. However, the policy does not require Postal Service employees to report their criminal arrests and convictions to anyone in the Postal Service, except for convicted sex offenders. A policy requiring employees to report arrests and convictions could reduce the risk of exposure for Postal Service employees, customers, the mail, and critical assets.

Management Response

It is not clear how self-disclosure of employee arrests and convictions could reduce the risk of exposure for employees, customers, the mail, and critical assets.

In fairness to applicants and in consideration of the Postal Service's obligations to the public and the workforce, the Postal Service considers only those records in which an arrest resulted in a criminal conviction or in which charges are pending at the time of the inquiry. Then it is postal policy to evaluate the employability of each applicant with a criminal conviction record individually. An applicant is rejected on the basis of a history of criminal conviction only after a specific finding that the history is directly related to the applicant's present capacity to perform as a Postal Service employee. Similarly, *employee* arrests do not necessarily result in conviction nor relate to the employee's capacity to perform his or her job. Requiring an employee to disclose the fact of an off-duty arrest and surrounding details can be problematic because the employee may suffer negative consequences despite final adjudication in the employee's favor. Requiring an employee to disclose a *conviction* is nearly impossible to enforce consistently without incurring the expense and administrative burden of periodic criminal record checks. In addition, discipline for the off-duty conduct is often difficult since it must be corrective, not punitive, and generally cannot be upheld unless there is a clear connection between the misconduct and service efficiency.

Nevertheless, postal managers and Postal Inspection Service personnel are often aware of employee off-duty arrests either because the employee voluntarily reports it, or the Office of Personnel Management alerts the Inspection Service when the FBI criminal arrest database is updated with new prints for a postal employee, or local law enforcement agencies alert Inspectors of an employee arrest. Further, the national agreements for the major unions contain provisions in Article 29 for dealing with an employee when their State driver's license has been revoked or suspended. We believe these formal and informal measures, and the recently-imposed sex offender policy, adequately mitigate risk to the Postal Service.