United States Government Accountability Office

GAO

Report to Congressional Requesters

November 2004

U.S. POSTAL SERVICE

Physical Security Measures Have Increased at Some Core Facilities, but Security Problems Continue

GAO-05-48

November 2004

U.S. POSTAL SERVICE

Physical Security Measures Have Increased at Some Core Facilities, but Security Problems Continue

GAO Accountability • Integrity • Reliability

Highlights

Highlights of GAO-05-48, a report to congressional requesters

Why GAO Did This Study

Mail and postal facilities are tempting targets for theft and other criminal acts. Approximately 800,000 U.S. Postal Service (USPS) employees process about 700 million pieces of mail daily at almost 38,000 facilities nationwide. Criminals attack letter carriers to get mail containing valuables and burglarize postal facilities to get cash and money orders. These activities at USPS facilities can put at risk the integrity of the mail and the safety of employees, customers, and assets. We looked at physical security measures at large facilities that perform automated mail-sorting functions, which on the basis of discussions with USPS, we defined as "core" facilities. Specifically, our objectives were to provide information on (1) what USPS has determined to be the physical security requirements at core facilities, (2) what security measures have been implemented and what security problems exist at USPS core facilities, and (3) what are USPS's plans to respond to identified security problems.

What GAO Recommends

GAO recommends that the Postmaster General develop a plan, with objectives, time frames, and resources needed, for correcting and updating USPS's security database so USPS can accurately assess the status of physical security at core facilities, identify needed improvements, and assess progress made. USPS agreed with our recommendation and committed to develop such a plan.

www.gao.gov/cgi-bin/getrpt?GAO-05-48.

To view the full product, including the scope and methodology, click on the link above. For more information, contact Peter Guerrero at (202) 512-2834.

What GAO Found

USPS has determined physical security requirements, such as access control and exterior lighting, for its facilities and specified them in a handbook and a manual. The security requirements are mandatory for new facilities and any renovations made to existing facilities. Further guidance outlines how physical security requirements are to be implemented at all facilities. Additionally, USPS uses policy memorandums to increase managers' awareness of specific security issues and reinforce physical security requirements, such as locking doors and wearing identification badges.

Available information showed that implementation of security measures had increased at some core facilities, although security problems still existed at some facilities. However, incomplete and inaccurate USPS data precluded us from making an assessment of changes in the implementation of security measures at all core facilities. Specifically, the USPS Facility Security Database, which records security conditions, has a number of problems, such as missing and incomplete data, duplicate responses, and miscoded facilities. Nevertheless, available information on one-third of the 373 core facilities showed some additional security measures have been implemented at each of these facilities since fiscal year 2001. However, our analysis of Inspection Service reports and our site visits to 13 core facilities revealed a number of security problems, such as facility and vehicle keys unaccounted for, doors and gates left unlocked or alarms deactivated, mail and stamp inventory left unsecured, and employees not wearing identification badges as required.

According to USPS officials, a number of plans and processes to improve physical security are being developed. For example, through a formal review and follow-up process, the Inspection Service is working with local and headquarters management officials to improve facility security. The Inspection Service has filled almost all of its 47 new Physical Security Specialist positions. USPS has also created an Emergency Preparedness group to ensure consistent application of and increased compliance with security standards and is in the process of updating and improving its Facility Security Database. This database has the potential for identifying and tracking facility security issues nationwide.

Source: GAO.

USPS guidelines state that site security is intended to prevent unauthorized entry or exit by employees and/or others. This unattended guardhouse indicates an unsecured access point at a core facility.

Contents

Letter 1

Background 2
Summary 3
Conclusions 5
Recommendations 5
Agency Comments and Our Evaluation 5
Scope and Methodology 6

Appendixes

Appendix I: Physical Security of USPS Core Facilities 8

Appendix II: Comments from the U.S. Postal Service 42

Abbreviations

ID	identification
OMC	Observation of Mail Condition
USPS	U. S. Postal Service

GAO
Accountability * Integrity * Reliability

United States Government Accountability Office
Washington, D.C. 20548

November 16, 2004

The Honorable Tom Davis
Chairman, Committee on Government Reform
House of Representatives

The Honorable Joseph I. Lieberman
Ranking Minority Member
Committee on Governmental Affairs
United States Senate

The U.S. Postal Service (USPS) has a long-standing and continuing responsibility for the safety and security of USPS employees, facilities, assets, and the U.S. mail itself. Each year, USPS must deal with activities at its facilities that can put at risk the integrity of the mail and the safety of employees, customers, or assets. Criminals attack letter carriers—seeking mail containing valuables, such as jewelry or checks—and burglarize postal facilities, seeking cash and money orders. For example, in fiscal year 2001, USPS reported that it lost about $6.3 million in cash and checks to robberies, internal theft, and mishandling.[1] As agreed with your offices, we built on our previous work regarding cash security by examining physical security measures for USPS's "core"[2] mail-processing facilities. Specifically, our objectives were to provide information on (1) what USPS has determined to be the physical security requirements at core facilities, (2) what security measures have been implemented and what security problems exist at USPS core facilities, and (3) what are USPS's plans to respond to identified security problems. To provide information on the physical security requirements at core facilities, we examined USPS handbooks, manuals, policy memorandums, and other documentation. To determine what security measures have been implemented, we obtained and analyzed data about core facilities from the USPS Facility Security Database, examined data from USPS Inspection Service Observation of Mail Conditions, and visited 13 core facilities. To obtain information on

[1]See *U.S. Postal Service: More Consistent Implementation of Policies and Procedures for Cash Security Needed*, GAO-03-267 (Washington, D.C.: Nov. 15, 2002).

[2]For the purposes of this review, "core" is defined as 373 USPS mail processing facilities, which are designated as Processing & Distribution Centers (P&DC), Processing & Distribution Facilities (P&DF), Air Mail Centers (AMC), Air Mail Facilities (AMF), Bulk Mail Centers (BMC), and other facilities, such as Priority Mail Processing Centers. These facilities were defined as "core," based on discussions with USPS officials.

USPS plans to respond to identified security problems, we interviewed USPS officials and analyzed documentation they supplied. Additional details on our scope and methodology are provided at the end of this report. Information contained in this report on security measures implemented at core facilities was obtained from a USPS Facility Security Database. We asked USPS to provide us with complete data for 373 core facilities. We determined that the data USPS provided had many problems, including missing and incomplete information, miscoded facilities, and duplicate responses. Data that would have allowed us to compare changes in security measures over time were complete for only about one-third of the 373 core facilities. We used these data to ascertain what new security measures have been implemented since fiscal year 2001. We conducted our work from March 2003 through October 2004, in accordance with generally accepted government auditing standards. This report summarizes the information we provided to your staff during our September 29, 2004, briefing. The briefing slides, which provide more details about our analysis, are included as appendix I.

Background

USPS is required to provide mail delivery and postal services to every community, business, and residence in the United States; its territories; and its servicemen and women stationed overseas. In 2003, USPS collected, processed, and delivered over 202 billion pieces of mail. Over 800,000 full-time and part-time employees work in approximately 38,000 facilities, owned or leased by USPS and located throughout the United States, to provide mail services. Most of the facilities are the familiar post office type of facilities that provide retail postal services and products to businesses and the public. Others are large-core mail processing facilities that perform automated mail-sorting functions; these facilities can exceed 1 million square feet in size and employ thousands of workers.

The Postal Inspection Service, one of the nation's oldest law enforcement agencies, is USPS's law enforcement and security arm. The Inspection Service is responsible for ensuring the safety and security of postal employees, facilities, and assets. Its 1,900 postal inspectors perform periodic facility security reviews, which are referred to as the Observation of Mail Condition (OMC) Program. OMC reviews are conducted during the fall and early winter.[3] Of the 38,000 postal facilities nationwide, the

[3]According to USPS officials, OMC reviews occur between September and the first week in January because of the high volume of mail processed during this period.

Inspection Service reviewed security at approximately 1,500 in fiscal year 2004. Inspection Service officials told us that most core facilities are reviewed each year.

To address physical security concerns, each postal facility has a Security Control Officer, and each postal region has an Area Security Coordinator. The Security Control Officer is usually the installation head or designated manager or supervisor. This official serves as the focal point to help implement security policies and coordinate with the Inspection Service as needed on security matters. Annually, the Security Control Officer is required to complete the Facility Security Survey. The Facility Security Survey is a checklist of 273 yes/no questions regarding the facility's compliance with physical security requirements, such as whether the lighting system is in working order.

USPS management uses data from the Facility Security Survey to collect information on facilities' implementation of security measures, and the survey results are maintained in the Facility Security Database.

Summary

In summary, we found the following:

- USPS has determined physical security requirements for its core facilities, such as access control and exterior lighting, and specifies these requirements in a handbook, a manual, and policy memorandums. Physical security requirements are contained in *USPS Handbook RE-5* (Building and Site Security Requirements, March 2001).[4] These security requirements are mandatory for new facilities and any renovations made to existing facilities. For example, RE-5 specifies that perimeter fencing and gates must be 8 feet high. In addition, *USPS Administrative Support Manual 13* outlines how physical security requirements are to be implemented at facilities. For example, this manual requires that all facilities ensure that personnel wear identification (ID) badges in full view during official duty hours. In addition to the handbook and manuals, USPS officials use policy memorandums to increase facility managers' awareness of specific security issues and reinforce the requirements, such as locking doors, wearing ID badges, and challenging those without IDs.

[4]Postal officials told us that RE-5 is under revision.

- Available information showed that implementation of security measures had increased since 2001 at some core facilities, although security problems still existed at some facilities. However, incomplete and inaccurate USPS data precluded us from making an overall assessment of the implementation of security measures at all 373 core facilities. USPS security data for core facilities had a number of problems, including miscoded facilities, duplicate responses, and incomplete information. Complete and accurate comparison data were available for only 119 of 373 core facilities. These data showed that some additional security measures were implemented at each of the 119 core facilities between fiscal years 2001, and the most recent year security survey data were available—either fiscal year 2003 or 2004. For example, 15 core facilities had installed electronic access control systems since 2001. In addition, our analysis of Inspection Service reports and our visits to 13 core facilities identified security problems. During its 2004 reviews, the Inspection Service found a variety of problems at core facilities, including required annual security surveys not being completed, facility and vehicle keys unaccounted for, doors and gates being left unlocked or alarms deactivated, unattended vehicles left unlocked, registered mail and stamp inventory left unsecured, and employees not wearing ID badges as required. During our visits to 13 core facilities we observed some similar security problems. At two locations, entry gates were left opened and unguarded, and we were able to enter restricted areas unescorted at three other facilities.

- According to USPS officials, a number of plans and processes to improve physical security are being developed. The Inspection Service is responsible for leading several of these efforts. For example, through a formal review and follow-up process, the Inspection Service is working with local and headquarters management officials to improve facility security. In an effort to address security concerns, the Inspection Service has filled almost all of 47 new Physical Security Specialist positions. In addition, at the end of fiscal year 2004, the Inspection Service completed training for 500 to 600 Security Control Officers, including those at the 373 core facilities. USPS officials also told us that an Emergency Preparedness group has been created to develop and implement measures to protect critical infrastructure, in collaboration with the Inspection Service. Although some management positions have been filled for this group, the unit is not yet fully operational. According to USPS officials, efforts are also under way to update and improve the Facility Security Database. For example, officials are in the process of refining a facility risk assessment, correcting data problems with the

Facility Security Database, and integrating the two into a single physical security evaluation and tracking tool. We are recommending that the Postmaster General develop a plan, with objectives, time frames, and needed resources, for correcting problems with the Facility Security Database. USPS concurred with this recommendation.

Conclusions

Although the Inspection Service is responsible for improving USPS physical security, it may lack information critical to these efforts. USPS officials acknowledge that there is no integrated system for tracking the status of physical security efforts. On the basis of our examination of the limited data available, we believe that the Facility Security Database has the potential to be an effective management tool for identifying, tracking, and correcting security issues. However, its current problems, such as incomplete and duplicative data, prevent USPS management from using the database to assess the implementation of required security requirements and determining progress in correcting deficiencies. USPS is taking steps to address deficiencies in the Facility Security Database. However, USPS currently lacks an overall plan—with objectives, time frames, and resources needed—that would help ensure that these deficiencies will be addressed.

Recommendations

In order to support the Inspection Service's efforts to improve physical security at USPS core facilities, we recommend that the Postmaster General develop a plan, with objectives, time frames, and resources needed, for correcting and updating USPS' security database so that USPS can accurately assess the status of physical security at core facilities, identify needed improvements, and assess progress that facilities have made.

Agency Comments and Our Evaluation

We provided a draft of this report to USPS for its review and comment. In a letter from the Chief Operating Officer dated October 29, 2004, USPS agreed with our report's information and recommendation and committed to developing a plan that will identify the resources and time frames needed to complete work on the project to upgrade and expand its facility security information system. See appendix II for the full text of USPS's comments.

Scope and Methodology

To provide information on the physical security requirements at core facilities, we reviewed USPS handbooks, manuals, policy memorandums, and other documents. We reviewed this documentation to gain an understanding of how the requirements are specifically implemented at core postal facilities. We also interviewed USPS Operations and Inspection Service officials regarding these requirements and the extent of their application at core facilities. We used the written documentation and interviews to define the specific roles of various officials in identifying security concerns, assessing priorities, and implementing improvements to facilities.

To determine what changes in security measures have been implemented at 373 core facilities since 2001, we obtained and analyzed data extracted from USPS's Facility Security Database, including answers to 28 specific questions, out of 273, that reflected USPS's emphasis on prevention of unauthorized entry and exit. We compared the data extracted from the Facility Security Database with the defined list of 373 core facilities and determined that due to incomplete data, duplicate entries, and miscodes, we were unable to accurately determine the implementation status for 254 of the 373 core facilities. However, for 119 core facilities, we had complete data that, although not projectible to the universe of 373 core facilities, were sufficiently reliable for determining the changes in security measures at these facilities from one reporting period (2001) to another (2003/2004).

We analyzed Postal Inspection Service OMC reports for fiscal year 2004 to identify security problems at core facilities. To observe security measures, we visited 13 core mail-processing facilities, selected on the basis of a mix of age, size, and geographic diversity.

We are sending copies of this report to the Postmaster General, the Chairman of the Senate Committee on Governmental Affairs, and the Ranking Minority Member of the House Committee on Government Reform, and other interested parties. We will provide copies to others on request. In addition, the report will be available at no charge on the GAO Web site at http://www.gao.gov.

If you have any questions about this report, please contact me on (202) 512-2834 or Carol Anderson-Guthrie, Assistant Director, on (214) 777-5739. Other key contributors to this assignment were Dwayne Curry, Eric Fielding, Reid Jones, Donna Leiss, and Walter Vance.

Peter F. Guerrero
Director, Physical Infrastructure Issues

Physical Security of USPS Core Facilities

Physical Security of USPS Core Facilities

Briefing to Congressional Requesters
September 29, 2004

1

GAO
Accountability * Integrity * Reliability

Purpose

- The U.S. Postal Service (USPS) has over 800,000 employees and almost 38,000 facilities nationwide. These employees and facilities handle about 700 million pieces of mail every day and the vast majority arrives intact. But mail and postal facilities remain a compelling target for larceny and other criminal acts. Criminals attack letter carriers seeking mail containing valuables such as jewelry, checks, or financial information, and burglarize facilities seeking cash and money orders. In fiscal year 2001, the USPS reported that it lost $6.3 million[1] in remittances (cash and checks) to robberies, internal theft, and mishandling. These disruptive or criminal activities at USPS facilities can put at risk the integrity of the mail and the safety of employees, customers, and assets.

[1]See *U.S. Postal Service: More Consistent Implementation of Policies and Procedures for Cash Security Needed, GAO-03-267 (Washington, D.C.: Nov. 15, 2002).*

2

Objectives

- Our objectives were to provide information on the following:
  - What has USPS determined to be the physical security requirements at core facilities?[2]
  - What security measures have been implemented and what security problems exist at USPS core facilities?
  - What are USPS's plans to respond to identified security problems?

[2]For the purposes of this review, "core" is defined as USPS mail processing facilities that are designated as Processing & Distribution Centers (P&DC), Processing & Distribution Facilities (P&DF), Air Mail Centers (AMC), Air Mail Facilities (AMF), Bulk Mail Centers (BMC) and other facilities, such as Priority Mail Processing Centers (PMPC). These facilities were defined as "core" on the basis of discussions with USPS officials.

3

Scope and Methodology

- Identified 373 core postal facilities;
- Examined USPS handbooks, manuals, policy memorandums, and other documentation;
- Obtained, analyzed, and assessed reliability of data on facilities from USPS Facility Security Database;
- Analyzed USPS Inspection Service Observation of Mail Condition Data;
- Visited 13 postal facilities;
- Interviewed USPS officials; and
- Conducted our work in Washington, D.C., and at several core postal facilities, in accordance with generally accepted government auditing standards.

4

Summary

- USPS has determined the physical security requirements, such as access control and exterior lighting, for core facilities. These requirements are specified in a handbook, manual, and policy memorandums. According to the Inspection Service, physical security procedures at USPS facilities were established to address the threats of robberies, burglaries, theft, and vandalism. These security standards are mandatory for new and existing facilities, and they are used as guidance for implementing security improvements.

- USPS data preclude an overall assessment of changes in implementation of security measures at core facilities since fiscal year 2001. Data on core facilities contained a variety of problems, such as missing and duplicative data, and inclusion of some noncore facilities. Available information for core facilities shows additional security measures have been implemented, such as the installation of access control devices and closed circuit television cameras. USPS fiscal year 2004 inspection reports showed security problems at some core facilities, such as gates and vehicles left unlocked. Our site visits to 13 core facilities identified similar security problems.

5

Summary (cont'd)

- USPS is aware of security problems at its core facilities and is taking steps to address them. USPS has a number of plans and processes in place to address physical security problems at various levels of the organization. Principally, the Inspection Service takes the lead in correcting security deficiencies through a formal review and follow-up process, with the assistance of local and headquarters management officials. USPS has created an emergency preparedness group to ensure consistent application and increased compliance with security standards. USPS is also in the process of updating and improving its facility security databases.

- We are recommending that the Postmaster General develop a plan, with objectives, time frames, and resources needed for completing, correcting, and updating USPS' security database so that it can be used by the USPS to assess the current status of physical security at core facilities, identify needed improvements, and assess progress that facilities have made.

6

Background

- USPS is required to provide mail delivery and postal services to every community, business, and residence in the United States.
  - In 2003, USPS collected, processed, and delivered over 202 billion pieces of mail.
  - To provide mail services, USPS has 373 core mail processing facilities.[3] (See table 1.)

[3]The facilities are operated by either USPS or a contractor and are either owned or leased by USPS.

7

GAO
Accountability * Integrity * Reliability

Background (cont'd)

Table 1: Type, Description, and Number of the 373 USPS Identified Core Facilities, as of March 2004

Facility type	Description	Number
Processing & Distribution Center/Facility (P&DC/P&DF)	A key mail facility that processes and dispatches part or all of both incoming and outgoing mail for a designated service area.	268
Airport Mail Center/Airport Mail Facility (AMC/AMF)	A mail facility at an airport that receives, concentrates, transfers, dispatches, and distributes mail transported by air.	63
Bulk Mail Center (BMC)	A highly mechanized mail processing plant that distributes standard mail in piece and bulk form.	21
Other facilities	Other mail processing facilities that fit the criteria for core facility; for example, Priority Mail Processing Centers.	21

Source: GAO analysis of USPS data.

8

Background (cont'd)

- The Postal Inspection Service is the law enforcement and security arm of USPS and is responsible for ensuring the safety and security of postal employees, facilities, and assets. The Postal Inspection Service has over 1,900 postal inspectors.[4]
  - Postal Inspectors help safeguard both employees and facilities against criminals and other threats to security by enforcing the federal laws applicable to the U.S. mail and investigating crimes that affect the mail.
  - Postal Inspectors periodically perform security reviews at selected individual postal facilities or at a cross-section of facilities within a postal district. These security reviews are referred to as the Observation of Mail Condition program (OMC), and they are performed at the request of the Chief Operating Officer.
  - Reviews are conducted annually for an average of about 15 weeks during the fall and early winter.[5] The fiscal year 2004 reviews included approximately 1,500 of the almost 38,000 postal facilities nationwide. Generally, core facilities are reviewed every year.

[4]The Postal Inspection Service also has a force of about 1,400 uniformed Postal Police Officers to provide perimeter security; escort high-value mail shipments; and perform essential protective functions, such as access control at the facilities.

[5]According to USPS officials, OMC reviews are conducted between September and the first week in January.

Background (cont'd)

- USPS also uses other approaches to address physical security issues.
  - Each postal facility has a Security Control Officer (SCO). The SCO is a designated position held by the installation head or a designated manager or supervisor. SCO duties include
    - developing and directing a security program on an ongoing basis,
    - ensuring that appropriate attention is paid to security issues,
    - acting as a liaison to the Inspection Service, and
    - conducting an annual Facility Security Survey and taking corrective actions as needed.

10

Background (cont'd)

- Each postal area also has an Area Security Coordinator, a USPS management official responsible for
  - ensuring adequate funding for security,
  - soliciting and encouraging management support in enforcement of security polices and procedures,
  - providing guidance and direction to SCOs, and
  - monitoring and evaluating the effectiveness of security programs.

11

Background (cont'd)

- USPS management collects data on the status of its facilities' security using the Facility Security Survey. USPS management uses the Facility Security Survey to review, evaluate, and isolate security issues for a given facility. The Facility Security Survey is
  - a checklist of 273 yes/no questions,
  - completed yearly by SCOs, and
  - maintained in the Facility Security Database.

12

Objective 1: What Has USPS Determined To Be the Physical Security Requirements for Core Facilities?

- USPS has determined the physical security requirements, such as access control and exterior lighting, for core facilities. These requirements are specified in a handbook, manual, and policy memorandums. According to the Inspection Service, physical security procedures at USPS facilities were established to address the threats of robberies, burglaries, theft, and vandalism. These security standards are mandatory for new and existing facilities, and they are used as guidance for implementing security improvements.

13

Objective 1: What Has USPS Determined To Be the Physical Security Requirements for Core Facilities?

- Physical security standards are contained in USPS *Handbook RE-5* (Building and Site Security Requirements, March 2001).
  - Requirements apply to existing facilities and new construction, whether owned or leased.
  - Security Control Officers and Postal Inspectors use *Handbook RE-5* standards as a guide to assess physical security.
- *Handbook RE-5* standards are intended to prevent unauthorized entry or exit by employees and others. Table 2 provides examples of selected site security requirements and descriptions.

14

GAO
Accountability * Integrity * Reliability

Objective 1: What Has USPS Determined To Be the Physical Security Requirements for Core Facilities?

Table 2: Examples of Selected Handbook RE-5 Site Security Standards

Security standards	Description
Facility perimeter fencing	Perimeter fencing and gates must be 8 feet high; fencing must terminate at ground level on either a concrete, paved surface, or firm nonshifting soil. An 8-foot, nonscalable wall may be used where aesthetics is a factor. Fencing/gates must be protected from vehicular damage by using wheel stops, curbs, bollards, etc.
Landscaping of fencing & building	Trees must not be closer than 10 feet to the fence or building. Landscaping must not provide points of concealment or unauthorized entry into secure grounds.
Security lighting	This is the single "best security device" available to protect employees. Basic lighting includes lighting at entrance gates, employee entrances, vestibule entrances, areas around the building perimeter & perimeter security fencing, all areas not open to the general public, and customer entrances.
CCTV systems[a]	Where security CCTV systems are required, lighting must be sufficient throughout the site so that cameras can operate effectively and record required information. They are to provide a color picture, have an automatic iris and pan-tilt-zoom lens, and for exterior use, are installed in environmentally controlled domed housings. CCTV system must cover all pedestrian and vehicle entries into the site and all employee entries into the facility, all employee and customer parking areas, and the bulk mail entry unit (BMEU), and all entry points into and out of the facility's truck parking and maneuvering areas.
Locks	All exterior doors must have a lock with deadbolt or approved equal locking capability.
Access control system	This system must provide positive control over employees entering a facility. It must prevent piggybacking or tailgating of employees without human intervention. This is usually done via turnstiles, but may be done with a pair of doors or specialty sensors. The system must consist of stand-alone smart panels that make the access decision and must have a stand-alone storage database capability that is downloaded routinely to the central computer database.

Source: USPS.

[a]CCTV – closed-circuit television.

15

Objective 1: What Has USPS Determined to be the Physical Security Requirements for Core Facilities?

- Policies and procedures related to physical security are primarily contained in *Administrative Support Manual 13*, section 27. The manual outlines
  - general responsibilities for the various security positions, such as SCOs and
  - practices for providing physical security.

16

Objective 1: What has USPS Determined To Be the Physical Security Requirements for Core Facilities?

- Policy memorandums on security issues are used to increase USPS facilities' managers' awareness of specific security issues. These memorandums
  - reinforce the requirements from the *Administrative Support Manual*, such as informing facilities that locking doors, wearing identification (ID) badges, and challenging those without IDs are easy actions to ensure the security of their facilities; and
  - highlight areas of corrective action based on USPS Inspection Service reviews, such as ensuring that proper vehicle security procedures are followed.

17

Objective 2: What Security Measures Have Been Implemented and What Security Problems Exist at USPS Core Facilities?

- While incomplete and inaccurate USPS data preclude an overall assessment of changes in implementation of security measures at core facilities since fiscal year 2001, information for 119 core facilities shows additional security measures have been implemented.

- Our analysis of Postal Inspection Service Observation of Mail Condition reports for fiscal year 2004 showed security problems at some core facilities. Our site visits to 13 core facilities also identified security problems.

18

Objective 2: What Security Measures Have Been Implemented and What Security Problems Exist at USPS Core Facilities?

- We were unable to evaluate overall changes in the implementation of core facility security measures because of incomplete and inaccurate Facility Security Database information.
  - We requested facility security survey data for core facilities for fiscal year 2001 and the most recent survey in Facility Security Database— fiscal years 2003/2004.[6]
    - Between May 2003 and April 2004, we worked with USPS to obtain data necessary to perform our analysis.
    - In September 2003, USPS provided data files that did not contain complete survey responses for many core facilities.
    - In March 2004, USPS assured us that the Facility Security Database was improved and that USPS could provide complete data on core facilities.
    - In April 2004, USPS provided data files that were incomplete and contained a variety of problems, including
      - missing or incomplete survey data,
      - duplicative survey data, and
      - inclusion of noncore facility survey data.
    - The April 2004 files contained complete and accurate data on 119 of the 373 core facilities, which would allow a comparison of fiscal year 2001 with 2003/2004.

[6]We used the most recent survey available for each facility, either fiscal year 2003 or fiscal year 2004.

19

Objective 2: What Security Measures Have Been Implemented and What Security Problems Exist at USPS Core Facilities?

- For 119 core facilities, complete Facility Security Database information for fiscal years 2001 and 2003/2004 was available to determine the implementation of security measures.[7] Our analysis of this data showed implementation of some security measures increased at these 119 core facilities.[8]
  - Our analysis focused on what we determined to be key security measures from the Facility Security Database responses completed by core facilities.
    - We selected 28 of the 273 questions from the Facility Security Survey based on the questions' pertinence to our study.
    - Data for selected questions were obtained for both Fiscal Year 2001 and Fiscal Year 2003/2004. (See table 3.)

[7] Of the 373 core facilities, 254 did not have complete data or had invalid values.

[8] We used facilities for which data were available, but these facilities may not be representative of the universe of core facilities.

Objective 2: What Security Measures Have Been Implemented and What Security Problems Exist at USPS Core Facilities?

Table 3: Implementation of Selected Security Measures at 119 Core Facilities, 2001 and 2003 /2004[a]

Type of security measures implemented	Number of facilities where implemented in 2001	Number of facilities where implemented in 2003/2004	Increase in number of facilities implementing security measure
Building keys inventoried	67	92	25
Contingency plans in place	99	116	17
Electronic access control system	77	92	15
Emergency exits with audible alarm	67	78	11
CCTV cameras installed	62	71	9
Opening secured (e.g., heat ducts)	83	90	7

Source: GAO analysis of data provided by USPS.

Note: Facility Security Database information is self-reported by the facility in the Facility Security Survey.

[a]For these facilities, USPS was able to provide us with FSD data for fiscal years 2001 and 2003/2004.

21

Objective 2: What Security Measures Have Been Implemented and What Security Problems Exist at USPS Core Facilities?

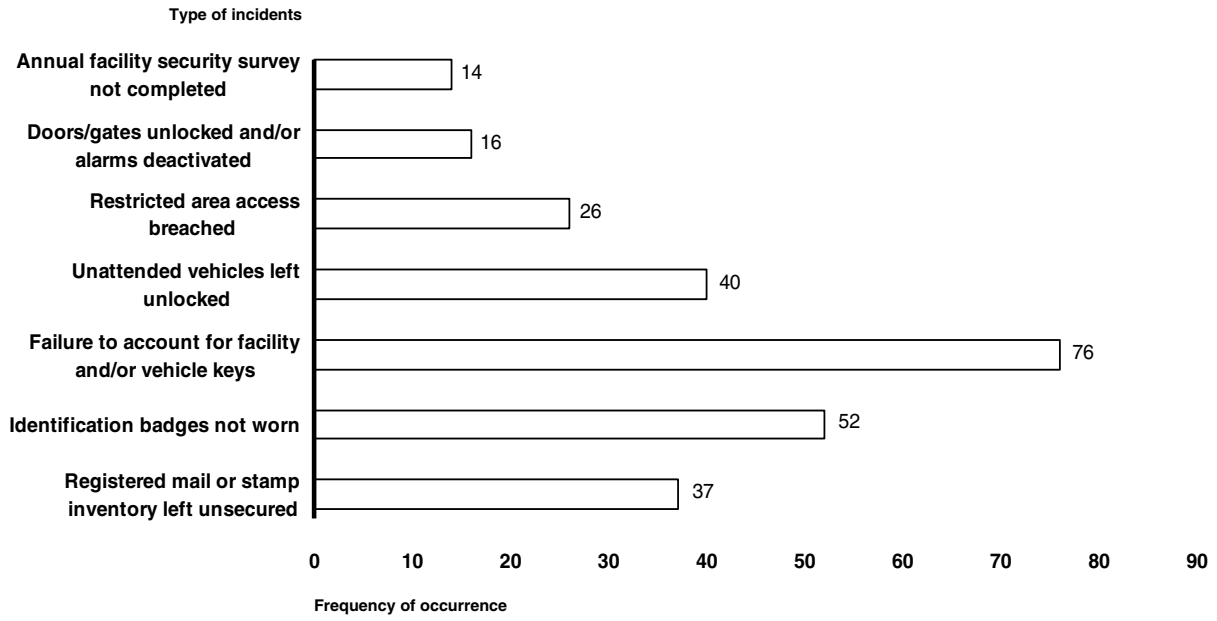
- Our analysis of Postal Inspection Service reports for fiscal year 2004 showed security problems at core facilities.
  - Postal Inspection Service performed 1,489 observation visits to core and noncore facilities from September through December 2003.
  - Postal Inspection Service's observations included 153 core facilities. (See fig. 1.)

22

GAO
Accountability * Integrity * Reliability

Objective 2: What Security Measures Have Been Implemented and What Security Problems Exist at USPS Core Facilities?

Figure 1: Security Problems Identified at 153 Core Facilities by Fiscal Year 2004 Inspection Service Reports



Source: GAO analysis of USPS data.

23

Objective 2: What Security Measures Have Been Implemented and What Security Problems Exist at USPS Core Facilities?

- Our site visits to 13 core facilities disclosed security problems consistent with those in Inspection Service reports. These 13 sites
  - were selected using general characteristics, such as age, size, and geographic distribution and
  - do not represent the universe of core facilities.

24

Objective 2: What Security Measures Have Been Implemented and What Security Problems Exist at USPS Core Facilities?

- Examples of security problems observed during our 13 site visits include the following:
  - At two locations, the most recent annual facility security surveys were prepared in calendar year 2000, although USPS requires an annual security survey.
  - At three locations, we gained access to the restricted dock areas by walking through a gate left open when a truck entered, following behind employees through a lockable entry door, and slipping through an unattended area between the parking lot and facility.
  - At one location, identification badges and/or access control cards were not recovered/deactivated for thousands of former employees.
  - At two locations, entry gates were left opened and unguarded.

25

Objective 3: What Are USPS's Plans to Respond to Identified Security Problems?

- USPS is aware of security problems and is taking steps to address them. Officials said that processes and plans are in place to improve security, such as
  - following up with facilities' management after the Inspection Service's Observation of Mail Condition (OMC) reviews,
  - creating new Inspection Service positions to address security concerns,
  - training facility security personnel,
  - prioritizing and establishing goals for improved security,
  - creating a new organizational group to focus on security matters, and
  - updating security-related databases.

26

Objective 3: What Are USPS's Plans to Respond to Identified Security Problems?

- Post OMC review follow-up with facilities:
  - Inspection Service officials meet with facilities' officials after OMC reviews to discuss physical security deficiencies and obtain management commitment to making corrections.
  - Inspection Service and Operations officials track facilities' plans to resolve deficiencies identified during OMC reviews.
  - Inspection Service's Deputy Chief Inspector conducted a fiscal year 2004 briefing for area vice presidents that identified key security problems.
- Inspection Service officials serve as security advisors to USPS operations officials, providing them with suggestions and guidance on security improvements.
  - The Inspection Service is currently filling 47 new Physical Security Specialist positions.
  - Physical Security Specialists will work side by side with inspectors and with headquarters operations officials to address security concerns.

27

Objective 3: What Are USPS's Plans to Respond to Identified Security Problems?

- In fiscal year 2004, USPS established training for SCOs, which includes
  - description of duties and responsibilities,
  - use of risk management to assess physical security, and
  - directions for completing the Facility Security Survey.
- 500 to 600 SCOs were trained by the end of fiscal year 2004.

28

Objective 3: What Are USPS's Plans to Respond to Identified Security Problems?

- An overall assessment of security by senior USPS management and Inspection Service officials is used to set yearly priorities and establish specific goals for improvement.
  - USPS officials told us they use a variety of sources, such as the Facility Security Survey, OMC data, and a risk-rating model to set budget priorities.
  - USPS officials believe local facility management, working with the Inspection Service, is in the best position to identify and address security needs. Therefore, local officials submit specific proposals to improve physical security; these proposals are reviewed and approved through a budget process with thresholds for approval authority.

29

Objective 3: What Are USPS's Plans to Respond to Identified Security Problems?

- According to USPS officials, an emergency preparedness organizational group has been created. This group is responsible for
  - developing and implementing ongoing measures to protect critical infrastructure, in collaboration with the Inspection Service and
  - managing the development and implementation of all training programs for protective measures.
- Some management positions have been filled, but the new group is not yet fully operational.

30

Objective 3: What Are USPS's Plans to Respond to Identified Security Problems?

- According to USPS officials, the Inspection Service is working to develop and improve the data on physical security at facilities.
  - USPS is refining a Facility Risk Rating Model (FRRM) to measure risks associated with core mail processing facilities and degree of implementation of measures to reduce these risks. Currently, FRRM
    - has data on two-thirds of USPS core facilities,[9]
    - utilizes 1990 census crime data that will be updated with 2000 census data,
    - has limited application for evaluating physical security until it is complete and updated, and
    - is used to set goals for improving security.
  - USPS told us that by fiscal year 2005 FRRM and the Facility Security Database will be integrated into one physical security evaluation and tracking tool, which officials acknowledge does not currently exist.

[9]The remaining one-third of facilities will be completed by fiscal year 2005.

31

Objective 3: What Are USPS's Plans to Respond to Identified Security Problems?

- Efforts are under way to address Facility Security Database data problems.
  - A committee comprised of different USPS functional areas is responsible for correcting problems with the data that supply information to Facility Security Database.
  - Various functional areas at USPS headquarters have agreed to be "stewards" of facility data to ensure accuracy of the database.

32

Conclusions

- USPS officials acknowledge that there is no integrated system for tracking systemic security problems. The Facility Security Database has the potential to be an effective management tool for identifying, tracking, and correcting security issues. However, its current problems, such as incomplete and duplicative data, prevent it from being used by USPS management to assess the implementation of required security standards and progress in correcting deficiencies. USPS is taking steps to address deficiencies in the Facility Security Database. At this time, USPS lacks an overall plan—with objectives, time frames, and resources needed—that would help ensure that these problems will be addressed.

33

Recommendations

- We recommend that the Postmaster General
  - Develop a plan, with objectives, time frames, and resources needed for completing, correcting, and updating USPS' security database so USPS can accurately assess the status of physical security at core facilities, identify needed improvements, and assess progress that facilities have made.

34

Comments from the U.S. Postal Service

PATRICK R. DONAHOE
CHIEF OPERATING OFFICER
AND EXECUTIVE VICE PRESIDENT

UNITED STATES POSTAL SERVICE

October 29, 2004

Mr. Peter F. Guerrero
Director, Physical Infrastructure Issues
United States Government Accountability Office
Washington, DC 20548-0001

Dear Mr. Guerrero:

Thank you for providing the Postal Service with the opportunity to review and comment on the draft report, U.S. Postal Service: Physical Security Measures Have Increased at Some Core Facilities, but Security Problems Continue.

We are pleased that the GAO recognizes that we take physical security at our core facilities very seriously and that we are working on a number of initiatives that, when implemented, will lead to improved security at all of our facilities. As the report also notes, we still have room for improvement at many facilities. Basic security deficiencies such as unlocked doors and unguarded gates are continuing problems and ones that we routinely discuss with field managers at all levels.

When we build or lease new facilities, we install the appropriate level of security technology, such as electronic access controls and closed circuit camera systems, based on the mandatory requirements specified in our physical security regulations. For existing facilities, we work with local management to prioritize their security needs and develop cost-effective solutions to increase compliance with security requirements. For example, some older facilities may need to have access control systems installed or fencing upgraded. At others, occasional reminders to employees of the requirement to wear their ID badges will improve security compliance.

One of the most important duties of the Postal Inspection Service is to monitor and report on how well our nearly 38,000 facilities are complying with physical security requirements. To facilitate better collection and evaluation of Inspection Service- and local management-generated security reports, we have been working with the Inspection Service to upgrade and expand our facility security information system. As the report recommends, we will develop a plan that will identify the resources and time frames needed to complete work on the project. Once we have up-to-date and accurate data on the status of security measures at our facilities, we can more reliably identify those facilities in need of security improvements and make sure they are being implemented in a timely and efficient manner.

If you or your staff would like to discuss any of these comments further, I am available at your convenience.

Sincerely,

Patrick R. Donahoe

475 L'ENFANT PLAZA SW
WASHINGTON DC 20260-0080
www.usps.com

GAO's Mission

The Government Accountability Office, the audit, evaluation and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's Web site (www.gao.gov). Each weekday, GAO posts newly released reports, testimony, and correspondence on its Web site. To have GAO e-mail you a list of newly posted products every afternoon, go to www.gao.gov and select "Subscribe to Updates."

Order by Mail or Phone

The first copy of each printed report is free. Additional copies are $2 each. A check or money order should be made out to the Superintendent of Documents. GAO also accepts VISA and Mastercard. Orders for 100 or more copies mailed to a single address are discounted 25 percent. Orders should be sent to:

U.S. Government Accountability Office
441 G Street NW, Room LM
Washington, D.C. 20548

To order by Phone: Voice: (202) 512-6000
TDD: (202) 512-2537
Fax: (202) 512-6061

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Gloria Jarmon, Managing Director, JarmonG@gao.gov (202) 512-4400
U.S. Government Accountability Office, 441 G Street NW, Room 7125
Washington, D.C. 20548

Public Affairs

Susan Becker, Acting Manager, BeckerS@gao.gov (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, D.C. 20548

United States
Government Accountability Office
Washington, D.C. 20548-0001

Official Business
Penalty for Private Use $300

Address Service Requested

Presorted Standard
Postage & Fees Paid
GAO
Permit No. GI00