UNITED STATES POSTAL SERVICE®

Management Instruction

Date	August 6, 2007
Effective	August 6, 2007
Number	AS-882-2007-6
Obsoletes	AS-882-2006-3
Unit	Unit Chief Technology Officer

Robert L. Otto
Vice President
Chief Technology Office

Delores J. Killette
Vice President
Consumer Advocate

Postal Service Use of Retail and Cell-Phone Cameras

Purpose

This Management Instruction (MI) establishes the policy and procedures for: (1) Postal Service™ management's use of cameras for monitoring retail operations and (2) restrictions on employee's or contractor's use of handheld and cell-phone cameras in Postal Service facilities.

Scope

This MI applies to the following cameras used in Postal Service facilities:

- Cameras used for monitoring retail operations.
- Cameras used in retail kiosk equipment.
- Closed circuit television (CCTV) cameras used for monitoring retail operations by management as described in *Administrative Support Manual* 273.17, Closed Circuit Television System Security.
- Cell phones with camera capabilities or other handheld cameras used by employees or contractors in Postal Service facilities.

This MI does not apply to the following:

- Photography authorized by management for operational purposes, including images of mail, mail processing operations, retail marketing (including Passport cameras), or similar activities.
- Photography conducted in accordance with the collective bargaining agreement.
- Video teleconferencing, photography, or video recording of official meetings.
- Video teleconferencing, photography, or video recording of events such as award, retirement, training, or other similar functions.

CONTENTS

Purpose 1
Scope 1
Roles and Responsibilities 2
Permissions 3
Prohibitions 3
Notice 3
AIMS Registration Requirement 4
Network-Based Camera Settings 4
Security 5
Access Control 5
Disclosure 6
Data Retention 6
Violations 6

- Photography by nonPostal Service persons, including photographic activities subject to *Postal Operations Manual* 124.58, Photographs for News, Advertising, or Commercial Purposes.
- Cameras installed, operated, or maintained by the U.S. Postal Inspection Service or the Postal Service's Office of Inspector General. (The Inspection Service maintains camera policies and procedures, which address the issues presented below and conform to applicable federal law governing the use of such techniques).

Roles and Responsibilities

Retail: Headquarters (HQ) Retail Operations and HQ Retail Marketing will coordinate national compliance regarding cameras in retail lobbies, including customer notices for retail kiosk equipment and approved customer notice signage for retail lobbies where cameras are used to monitor retail operations.

Area and Headquarters: Vice presidents or their designees will administer the policy within their areas.

District: District managers or their designees will be responsible for deciding who in the district has a business need for camera access, such as postmasters or Human Resources managers. District managers or their designees will be responsible for decisions on the placement of district cameras for monitoring retail operations.

District information technology (IT)/information system (IS) managers or their designees will be responsible for implementing controls to limit unauthorized access to camera images. District IT/IS managers or their designees will also be responsible for ensuring current registration in the Assets Inventory Management System (AIMS) of all network-based, CCTV, or any cameras used in the district for monitoring retail operations.

Information Security: The Corporate Information Security Office (CISO) is responsible for policy to protect information stored or transmitted on electronic media. Implementation of such technology is subject to the Information Security Assurance (ISA) process. The CISO will request reports on cameras from the AIMS registration system as needed to implement the MI.

Privacy: The Privacy Office is responsible for providing direction and assistance regarding this MI, including privacy notice requirements and any other questions dealing with this policy.

Permissions

Under this policy, the following activities are permitted:

- The Postal Service may use network-based cameras in retail lobbies to monitor customer service and allocate Postal Service resources.
- The Postal Service may use cameras in self-service kiosks, automated postal centers, and similar self-service devices.

Prohibitions

Under this policy, the following activities are prohibited:

Video Monitoring Cameras in Retail Operations:

- Cameras must not be used to profile customers in any discriminatory fashion.
- Cameras must not be used to capture legible images of mail piece addresses or any documents, credit cards, or computer screens used in transactions.
- Camera images must not be transmitted via any network other than the Postal Service intranet (“Blue”).
- Wireless cameras must not be used without approval of the district IT manager.
- Camera microphones must not be used to record or monitor any form of audio information.

Privacy Act and Information Security Assurance: Retail Operations and Retail Marketing will notify the Privacy Office and the CISO, if at any time in the future, information is retrieved by personal identifiers (e.g., names) or individual appearance, or if information is maintained in an application requiring completion of the ISA process.

Handheld and Cell-Phone Cameras: Cameras or cell-phone camera functions may not be used by Postal Service employees or contractors in restrooms, locker rooms, retail counter areas, mail processing areas, workroom floors, or any other areas unless approved by an area or headquarters vice president or his or her designee for business purposes. Cameras or cell phones used as cameras in violation of this prohibition may be subject to temporary confiscation.

Notice

Customer Notice: The Postal Service will notify customers when they are being video-monitored during a transaction, such as at a retail counter or self-service kiosk. Notice will be provided via a placard posted in Management Instruction AS-882-2007-6 plain view or by a

notice appearing on the computer screen prior to the beginning of the transaction. Appropriate notices on screen or via signage shall be coordinated by Retail Operations and Retail Marketing.

Privacy Act Notice: The Postal Service will notify customers, employees, or contractors if, at any time in the future, information will be retrieved from camera film or footage via their personal identifiers, thus necessitating the creation or amendment of a Privacy Act system of records. In such cases, the Postal Service will post a placard in plain view with the appropriate Privacy Act notice stating when and where the camera is operational.

AIMS Registration Requirement

Every network-based or CCTV video camera used for monitoring retail operations by the Postal Service in the field shall be registered by the district IT manager in AIMS for tracking and network utilization authorization. This registration is separate from, and in addition to, any existing registration requirement for controlling access to camera configuration capabilities. This registration requirement does not include conventional photography equipment, or handheld digital or video cameras.

Information Required for Complete Registration: The AIMS registration information for each camera will contain the following:

- Office name, mailing address, and finance number.
- By whom it was installed (Postal Service or name of contract firm).
- The times of operation.
- Camera name and Web page URL displayed on the applicable district Web page.
- Type of camera (make and model).
- The complete address of the hosting server on the network, or if the camera includes a self-contained imbedded server, the complete address of that server.

Network-Based Camera Settings

Network-based cameras must be configured and implemented correctly so that they do not negatively impact network performance. These cameras must not be configured in a manner that will send or receive video pictures in a streaming mode. The refresh rate should be set for every 60 seconds or slower.

Security

Security will be implemented in accessing, transmitting, storing, releasing, and disposing of data in accordance with Handbook AS-805, Information Security (Chapter 3, Information Designation and Control).

Access Control

This MI establishes management controls that permit appropriate camera uses and protect privacy by limiting access to only those persons with a business need. Access control includes the following:

- Designating those persons with a business need for access.
- Implementing a mechanism that limits access to only those persons.
- Providing the CISO and the Inspection Service all information required to disable access to individual cameras.

Designating Persons With Business Need: Access to camera images will be strictly limited to authorized employees and contractors on a need-to-know basis. The district manager or designee is responsible for designating who is authorized to view the network-based camera output within the facility, including access to camera images via district Web site links. Contractors who are given access to monitoring data as part of their job duties must be covered by contract clauses that protect Postal Service data, or they must sign nondisclosure agreements.

Implementing an Access Control Mechanism: The district IT manager or designee will implement processes to limit access to camera images to authorized persons only. Examples of how access control processes may be implemented include the following:

- Implementing an access control password application and providing a password only to persons authorized by the district manager or his or her designee.
- Removing all existing open links to camera pages, and providing a new page address by e-mail to those persons authorized by the district manager or their designee.

Providing Access Information to the CISO and the Inspection Service: However local access control is implemented, district IT managers are required to provide access information to their cameras via e-mails to the designated representatives of the Inspection Service and the CISO. The provided access information (when combined with the complete AIMS registration information required by this MI) must be adequate to enable either CISO or the Inspection Service to rapidly identify and remotely shut down access to any local camera, if required.

Disclosure

Records (including retained images) may only be disclosed outside the Postal Service as authorized or required by the Freedom of Information Act and the Privacy Act of 1974.

Data Retention

Film, video tapes, or other storage media may be retained for 90 days unless the district manager is requested to retain them longer for law enforcement, litigation purposes, or other purposes deemed appropriate. As a general matter, unless it has been determined otherwise, the retained images are not intended to be a system of records and are not to be retrieved by name or other personal identifier. Network-based camera data will be purged in accordance with Handbook AS-805, Information Security (Section 3-5.6, Disposal and Destruction of Information and Media).

Violations

The Postal Service may investigate and take appropriate action for violations of this policy.