

Department of the Interior Departmental Manual

Effective Date: 6/4/08

Series: Law Enforcement and Security

Part 444: Physical Protection and Facility Security

Chapter 3: Closed Circuit Television

Originating Office: Office of Law Enforcement, Security, and Emergency Management

444 DM 3

3.1 Purpose. This chapter establishes policy for the use of closed circuit television (CCTV) at Icons, Critical Infrastructure and Key Resource sites, and at other Departmental facilities and areas. This policy applies to the monitoring and/or recording of video/visual images only without a court order in public areas, or areas within DOI facilities consistent with law. Areas within and around DOI facilities may include, but are not limited to, interior entrances/exits/hallways and storage rooms.

3.2 Applicability. This policy applies to the use of CCTV technology by DOI employees and contractors, whether recorded or not, in all areas within the jurisdiction of the Department, whether the areas are open to the public or not. The primary purpose for using CCTV shall be for physical protection, facility security and public safety. All use of CCTV shall be consistent with this policy.

3.3 Responsibilities.

A. The senior Departmental/Bureau official having jurisdiction over an office, building, or other facility is responsible for ensuring that sufficient policies and procedures are in place, consistent with this policy and any guidance from the Office of the Solicitor, to safeguard and secure video images captured by the use of CCTV.

B. Each bureau/office head is responsible for implementing, maintaining, and monitoring procedures consistent with the purposes of this chapter.

C. The Director, Office of Law Enforcement, Security, and Emergency Management (OLESEM), is responsible for development, direction, coordination, compliance, and implementation of the Department's CCTV program, to include the establishment of policy and guidelines.

D. Each bureau/office Security Officer is responsible for complying with Departmental CCTV program policy and developing written CCTV policy and safeguards at sites under the jurisdiction of their bureau/office employees.

E. Each employee is responsible for compliance with the Departmental and bureau/office CCTV program directives.

3.4 **Policy.**

A. It is the policy of the Department to use CCTV only to further law enforcement, security, administrative, and public safety objectives.

B. Any requests for release of CCTV recordings by the public will be processed in accordance with the Freedom of Information Act and 43 CFR Part 2 and/or any other statutes and applicable regulations.

C. CCTV shall not be utilized to overhear and/or record audio conversations unless the provisions of 18 U.S.C. § 2511 are followed.

3.5 **Objectives.**

A. CCTV will only be used to visually monitor within and around DOI administered public areas or within and around DOI facilities.

B. CCTV will be used for the following objectives:

- (1) Protection of individuals, property, buildings and resources;
- (2) Preventing/deterring crime and public disorder;
- (3) Identifying criminal or terrorist activity and suspects;
- (4) Identifying and gathering evidence for law enforcement, security, administrative and public safety objectives;
- (5) Documenting the actions of law enforcement personnel to safeguard citizen and law enforcement officer rights;
- (6) Confirmation of alarms;
- (7) Patrol of public areas;
- (8) Investigation of terrorist or criminal activity; and
- (9) Improving the allocation and deployment of public safety assets.

3.6 **Operation and Use.**

A. Prior to installing new and/or additional surveillance cameras in a building with unionized federal employees, management of the bureau/office shall fulfill its obligations under the Federal-Service Labor Management Relations Statute, 5 U.S.C. § 7114.

B. CCTV cameras will be operated by Departmental or contract personnel to further law enforcement, security, administrative, and public safety objectives.

C. All staff involved in CCTV monitoring will be appropriately trained and supervised in the responsible use of this technology. At a minimum, this training will consist of:

- (1) A review of the Departmental and bureau policies concerning CCTV; and
- (2) A session on the technical operation of the system being used.

D. No person will be targeted or monitored merely because of race, religion, gender, sexual orientation, disability, national origin, or political affiliation/views.

E. CCTV will not target or focus on the faces of persons engaging in First Amendment activity unless there is a reasonable indication of suspicious or criminal activity, or a threat to public safety.

F. Disclosure and use of any information obtained will be limited to appropriate law enforcement, public safety, and administrative purposes.

G. Signs may be posted which give notice of the use of CCTV as deemed appropriate to enhance the crime prevention value of the system.

H. The use of any temporary CCTV systems for special events/emergency operations will be in full compliance with this policy.

3.7 **Controlled Facility.**

A. CCTV images will come through secured tamper-alert feeds and monitoring will be done from a controlled facility by a trained and supervised operator whose identity, while operating the CCTV system, will be documented by an electronic or paper log.

B. Access to the controlled facility will be limited to authorized law enforcement, security, maintenance and repair personnel, department managers, government attorneys, and designated government/policy officials, by using appropriate control measures.

C. The supervisory official assigned to, or responsible for, the controlled facility shall monitor the activities of assigned personnel to ensure full compliance with this Section.

3.8 Management Controls.

A. All images will be maintained by location, date and/or time in a manner consistent with the Federal Records Act and other applicable laws.

B. Access to live or recorded images shall be limited to authorized law enforcement personnel, security personnel, agency managers, system administrators, security control center operators, and government attorneys for law enforcement and public safety purposes, and to government attorneys and police managers for civil litigation and administrative purposes as appropriate, or as otherwise provided by law.

C. Any recorded video images shall be documented and stored in a secure location with controlled access that is limited to authorized personnel.

D. The Federal Records Act requires bureaus to retain records, including recordings from security cameras, for the length of time specified in approved records schedules. Bureaus/Offices shall maintain video recordings in accordance with Departmental and National Archives and Records Administration (NARA) guidelines. Bureaus/Offices may retain video recordings longer than the minimum retention periods as deemed necessary.

E. Upon the written consent of the Bureau Director of Law Enforcement, selected photographic stills or portions of the video recording may be reproduced and retained for historical or training purposes. Any photographic stills or portions of video recording which are reproduced and retained solely for historical or training purposes shall not reveal or be retrieved by any citizen's identity. Any identifying images should be blurred so that no citizen's identity can be discerned. The original video or photographic still shall be destroyed in accordance with paragraph D. Consistent with NARA guidelines, items may be retained for evidentiary purposes.

3.9 Accountability.

A. Violations of this policy shall result in the initiation of appropriate disciplinary action.

B. Each Bureau/Office Director of Law Enforcement will insure that periodic audits are conducted to ensure full compliance with this directive.

C. Nothing in this directive is intended to create any rights, privileges, or benefits not otherwise recognized by law.