

INTRADEPARTMENTAL CORRESPONDENCE

August 14, 2014
1.0

BPC #14-0317

TO: The Honorable Board of Police Commissioners

FROM: Inspector General, Police Commission

SUBJECT: REVIEW OF THE DEPARTMENT'S VIDEO CAMERA SYSTEM

RECOMMENDED ACTION

REVIEW and APPROVE the Office of the Inspector General's Review of the Department's Video Camera System.

DISCUSSION

The OIG conducted a review of the Department's video camera system. The OIG therefore visited each of the Department's 21 stations and inspected their respective camera systems in order to evaluate potential risks to police officers and the public.

The OIG's inspections identified concerns with the placement of video cameras within the various stations. The OIG noted that the video coverage in several stations' holding cells and booking areas was inadequate. The OIG also found shortcomings with the Department's video retention practices that may inhibit the Department's ability to adequately investigate any critical incidents. The OIG also learned that there is no formal process to regularly inspect cameras to assess if they are working properly or to conduct quality of service audits of the video footage itself.

The Department concurs with the OIG's recommendations and, in response, has convened a working group comprised of representatives from the Office of Administrative Services (OAS), Facilities Management Division (FMD), Office of Operations (OO), Information Technology Bureau (ITB), Office of Special Operations (OSO), Counter-Terrorism and Special Operations Bureau (CTSOB), Special Assistant for Constitutional Policing (SACP), and the Office of the Inspector General (OIG). The working group will consult with the City Attorney to address all of the recommendations made by the OIG.

I am available to provide any information the Board may require.

E-Copy – Original Signature on File with the Police Commission

ALEXANDER A. BUSTAMANTE

Inspector General

Police Commission

Attachment

c: Executive Director Richard M. Tefank

Chief of Police Charles L. Beck

Assistant Chief Sandy Jo MacArthur, Director, Office of Administrative Services

Assistant Chief Michel Moore, Director, Office of Special Operations

Assistant Chief Earl C. Paysinger, Director, Office of Operations

Deputy Chief Michael Downing, Counter-Terrorism and Special Operations Bureau

Chief Information Officer Maggie Goodrich, Information Technology Bureau

Police Administrator Arif Alikhan, Special Assistant for Constitutional Policing

Police Administrator Thomas Brennan, Facilities Management Division

LOS ANGELES POLICE COMMISSION

**REVIEW OF THE DEPARTMENT'S
VIDEO CAMERA SYSTEM**



Conducted by the

OFFICE OF THE INSPECTOR GENERAL

ALEXANDER A. BUSTAMANTE
Inspector General

August 14, 2014

TABLE OF CONTENTS

I.	INTRODUCTION	1
II.	INSPECTION OF VIDEO CAMERA SYSTEM.....	2
	A) Video Coverage	2
	B) Policies for Use of the System	3
	1. Access to the System.....	3
	2. Security and Retention of Video Evidence	4
	C) Inspections and Audits.....	4
III.	RECOMMENDATIONS	5
IV.	DEPARTMENT’S RESPONSE	5

OFFICE OF THE INSPECTOR GENERAL

REVIEW OF THE DEPARTMENT'S

VIDEO CAMERA SYSTEM

I. INTRODUCTION

In September 2013, an individual was taken into police custody and suffered a medical emergency while being housed inside a Department holding cell. That individual later died in police custody. In April of the following year, a gunman entered a police station and began shooting at officers, injuring one officer. In each of these cases, the Department and the OIG attempted to obtain all relevant information and evidence to assess these incidents. In both cases, the video evidence only captured portions of the events. Based upon these two investigations, the OIG decided to perform a broader analysis of the Department's video camera systems. The OIG therefore visited each of the Department's 21 stations and inspected their respective camera systems in order to evaluate potential risks to police officers and the public.

The *Los Angeles Police Department Security Master Plan* (Security Master Plan) dated October 20, 2003, sets forth the minimum requirements for station security. The Security Master Plan was primarily designed to guide new construction and renovation of designated stations. There is no language in the document that appears to be binding. It is important to note that the Department intends to revise the Security Master Plan to meet the current needs of each facility. The existing document discusses the creation of "security zones" within stations to ensure that the area is properly monitored. The plan requires these zones to be secured through a combination of electronic systems.¹ For example, a station is generally equipped with video surveillance cameras that monitor the interior and exterior of the station and electronic access systems that limit the areas that unauthorized individuals may enter. For the purposes of this report, the OIG focused primarily on the Department's video camera systems.

The OIG's inspections identified concerns with the placement of video cameras within the various stations. The OIG noted that the video coverage in several stations' holding cells and booking areas was inadequate. The OIG also found shortcomings with the Department's video retention practices that may inhibit the Department's ability to adequately investigate any critical incidents.² The OIG also learned that there is no formal process to regularly inspect cameras to assess if they are working properly or to conduct quality of service audits of the video footage itself.

¹ Security Master Plan, pages 6 – 13.

² Critical incidents, as used in this report, may include such events as a use of force, in-custody death, assault or other crime, injury or accident, or other major security incident.

II. INSPECTION OF VIDEO CAMERA SYSTEM

A) Video Coverage

In general, each station's video system is made up of a combination of fixed and movable surveillance cameras. The cameras are networked with a software system that allows station personnel to monitor the live feed, including switching between camera views, while continuously recording video footage. Nearly all stations with surveillance capability were able to monitor station accessibility, such as parking lot gates and station entrances. The system is also set up to facilitate the downloading of specific footage based on location and time, which can be saved to a DVD or other storage drives.

The OIG's inspection found that the number of cameras at each station varied, ranging from no cameras at all to approximately 30. Newer stations, specifically ones constructed within the last ten years, had more external and internal cameras, with full or near-full coverage of all essential areas, than did the older stations. The OIG also noted that some stations did not have an operable video camera system, either because they had no cameras, an outdated system, or lacked the capability to record video.³

The Department stated that they have tried to obtain funding in their budget requests for both Fiscal Years 2013/14 and 2014/15 for a video camera system in the stations that had no system at all. Due to re-allocation of the requested funds by the City of Los Angeles, the Department was unable to upgrade the video camera systems. Additionally, the Department proposed the upgrade of the memory for all of the video camera systems in their budget request for Fiscal Year 2011/12, which was denied for similar reasons. The Department plans to include in their budget request for Fiscal Year 2015/16 funding for life-cycle upgrades for the older video camera equipment.

The OIG found camera coverage varied from station to station. For example, there were stations with cameras in each holding cell, while other stations had partial or no view of the interior of those holding cells. Similar disparities between stations existed in other high-risk areas. The OIG confirmed that some stations did not have full coverage of the station's lobby or other areas where the public has unrestricted or unescorted access. This lack of coverage fails to meet the minimum standards set forth by the Security Master Plan.⁴ The OIG noted that certain areas within each station present higher risks for injuries, uses of force, complaints by arrestees, or even death. It is crucial that such areas are monitored by cameras and that supervisors and the Department have the ability to retrieve and review footage in the event of a critical incident or alleged misconduct.

³ For example, there were a small number of stations that did not have the Departmentwide video-access software installed.

⁴ Security Master Plan, pages 9 – 11.

In addition to the identified coverage concerns, the OIG learned that cameras would malfunction or break without Department personnel readily identifying the problem. The stations did not have a key or index for identifying camera locations and many officers complained that they could not locate broken cameras by looking at the monitors. Although this raises maintenance issues, there are additional security concerns that arise when officers can view real-time video of the station without knowing the exact location of the feed.

The inspection also found that no Department personnel, other than Facilities Management Division (FMD), were aware of any plans or structural designs for the placement and positioning of cameras.

B) Policies for Use of the System

The second component of the OIG's review was an examination of any policies and procedures governing the access, retention, storage, and review of video footage. The OIG's review found that except for the Security Master Plan and the Operators Manual⁵ distributed to each station, there are no Department or station policies and procedures, Special Orders, or directives specific to station video cameras.

1. Access to the System

When meeting with station personnel, the OIG found that there was a general lack of training on how the video camera systems work and how to retrieve video footage. The inspection found that approximately one person per station was trained and designated to retrieve video footage. Although one person may have the training to retrieve the video data, there appears to be little or no limitation on who can access the video.⁶ Each station had a dedicated work station for access to the video camera software system, but at many stations, workstations were in an area where unauthorized personnel could have access.⁷ Additionally, the OIG noted that the Operators Manual, generally maintained near the video workstation, lists the universal login and password code for the system. This manual is also published on the Department's local area network, which can be accessed by any Department employee. The OIG noted there is no clear policy directing video footage to be immediately secured after a critical incident. Department policy simply states that the entity responsible for an investigation shall coordinate, collect, and preserve all appropriate evidence in an official investigation.⁸ As stated in the Security Master Plan, the LAPD requires strict internal controls on recorded video for public relations and internal security purposes.⁹

⁵ *Los Angeles Police Department Security Systems Operators Manual.*

⁶ As recently as July 17, 2014, confidential video footage of a use of force was retrieved and leaked to a local news station.

⁷ Some stations had more than one workstation.

⁸ Department Manual Section 3/815.01-General Investigation Guidelines.

⁹ Security Master Plan, page 23.

2. Security and Retention of Video Evidence

As noted above, one area of concern for the OIG is the ability of the Department to retrieve and secure video evidence in the event of a critical incident -- such as an officer-involved shooting, in-custody death, serious use of force -- or where a complaint of misconduct has been made.

The OIG's inspection determined that the average retention of video footage is 30 days, after which it is automatically overwritten by the system.^{10, 11} While this may be a sufficient retention period for some types of incidents, the OIG noted that it may not be adequate to ensure the availability of footage related to a complaint investigation. This is particularly true in cases where the complainant initiates the complaint after the retention period has passed but may also be an issue even when the complaint is made soon after the event. Because the investigation of a complaint may begin several months after it is initiated, there is a possibility that footage will have been overwritten by the time it is requested.

The Department stated that during their budget request for Fiscal Year 2015/16, they will include an upgrade for the video retention to a period of time that the City Attorney recommends to be compliant with the applicable codes.¹²

The OIG also noted a lack of a consistent process for securing and tracking video evidence after it has been downloaded. For example, some station personnel reported that, after burning video footage to a DVD, they also maintained a copy of the video on the dedicated camera workstation. Because of the evidentiary value, the videos should be carefully maintained.¹³ This is particularly important in cases involving potential litigation and in Categorical Use of Force investigations.

C) Inspections and Audits

The OIG noted during its inspection that some cameras at different stations were not working, and at times, it was only during the OIG's visit that personnel became aware of an inoperable camera. Some stations have a process in place to check their cameras at certain intervals to ensure that all cameras are working; however, the majority of the stations do not conduct any type of regular inspection of their cameras. In fact, some personnel indicated that there had been instances in which they did not become aware that a video camera was inoperative until video footage was requested and they were unable to retrieve it.

¹⁰ A few stations reported a longer retention period, but none were longer than 70 days. This is based on system settings, with a few set to record only when there is motion or at a lower frame rate.

¹¹ As described in the Security Master Plan, "The system will also have the capability (although not initially configured as such) to store video from all cameras for a minimum of five (5) years via both on-line and archive storage."

¹² California Government Code Section 34090.6 & City of Los Angeles Administrative Code Section 12.3(b)(5).

¹³ Security Master Plan, page 23.

Additionally, the OIG learned that there is no process for Department personnel to conduct any type of qualitative analysis of video camera footage that may have captured an unreported critical incident.

III. RECOMMENDATIONS

The OIG recommends the Department conduct an assessment of station security protocols, including existing security camera coverage, in order to determine whether all high-risk areas are properly monitored or otherwise secured. The Department's security assessment should be provided to the Commission for its review.

The OIG recommends the Department ensure that video cameras are placed in a location and manner to record the Department's processing and detention of civilians for arrest, including arrestee benches, booking stalls, and holding cells.

The OIG recommends the Department ensure that multiple supervisors within a station have appropriate training to access, secure, and retrieve recorded video footage in the event of a critical incident. The OIG further recommends that the Department develop an access control system for the video workstations and develop guidelines prohibiting unauthorized access to such records.

The OIG recommends the Department standardize the video retention procedures for every division and ensure that any such procedures are consistent with current record keeping requirements, as described in Section 12.3 (b)(5) of the City of Los Angeles Administrative Code.

The OIG also recommends the Department develop and implement written protocols for the prompt retrieval of footage upon notification of a personnel complaint or any incident requiring investigation. The Department should also develop a policy that requires a record of the chain-of-custody for video footage that is downloaded and obtained by Department personnel.

The OIG recommends the Department develop and implement a policy requiring station personnel to check video cameras on a regular basis to determine whether any video cameras are inoperable.

IV. DEPARTMENT'S RESPONSE

The Department concurs with the OIG's recommendations and, in response, has convened a working group comprised of representatives from the Office of Administrative Services (OAS), Facilities Management Division (FMD), Office of Operations (OO), Information Technology Bureau (ITB), Office of Special Operations (OSO), Counter-Terrorism and Special Operations Bureau (CTSOB), Special Assistant for Constitutional Policing (SACP), and the Office of the Inspector General (OIG). The working group will consult with the City Attorney to address all

of the recommendations made by the OIG. Among the working group's top priorities will be to conduct a cost assessment pertaining to the implementation of the recommendations and to submit a comprehensive budget request for the Fiscal Year 2015/16 budget.¹⁴

In addition, ITB has worked with the City Attorney to clarify the retention requirements for police video and has begun discussions with the video camera vendor to develop a technology plan for the necessary system upgrades and/or replacements.

¹⁴ The OIG has already met with the Commanding Officer of OAS and other Department staff officers to discuss this report, the recommendations, and issues to be addressed in future working group meetings.