

STAFF REPORT

DATE: July 10, 2018
TO: City Council
FROM: Darren Pytel, Police Chief
SUBJECT: Surveillance Technology - Remote Public Safety Cameras

Recommendation

Informational. The Police Department is submitting this informational staff report on consent calendar at least 30 days prior to asking the City Council to hold a public hearing to continue using remote public safety cameras. This informational staff report has been posted on the City website with the City Council agenda (26.07.030 (c) Davis Municipal Code (DMC)).

Fiscal Impact

There is no fiscal impact to this report. If Council provides direction, future actions could have fiscal impacts.

Council Goal(s)

Goal 7 - Ensure a Safe and Health Community. This item is not called out as a specific task.

Background and Analysis

A City department seeking approval to acquire/use surveillance technology as defined by 26.07.020 DMC shall submit to the City Council a Surveillance Impact Report and a proposed Surveillance Use Policy via an informational staff report on a regular City Council meeting consent calendar at least thirty (30) days prior to the public hearing required under 26.07.030 (a). The informational staff report shall be posted on the City website with the City Council agenda. This staff report is being submitted to fulfill the notice requirements.

Surveillance Impact Report

Information describing the surveillance technology and how it works, including product descriptions from manufacturers;

(a) Information on the proposed purpose(s) for the surveillance technology:

Remote Public Safety Camera Systems are portable cameras that are remotely accessed by police personnel. The cameras are web based and use a cell phone account as a means of accessing the device. Once accessed, users can monitor the device, toggle it remotely and record video, but not audio. Each camera has its own digital video recorder (DVR) which records data, which can then be accessed by an external hard drive or other device. Cameras can be attached to fixed objects such as buildings, traffic standards or light poles, or placed in parked automobiles or other stationary places. The devices can either be attached to a power

source or run by battery. Remote Cameras are used to monitor areas where crime has been reported, to surveille individuals who are suspected of committing crime and to monitor crowd size and dynamics at city events in order to better deploy resources.

(b) If applicable, the location(s) it may be deployed and crime statistics for any location(s);
Remote Cameras are commonly deployed on buildings, traffic standards, light poles, in parked cars and other fixed objects.

(c) An assessment identifying any potential impact on civil liberties and civil rights and discussing any plans to safeguard the rights of the public; Remote Surveillance Camera Systems are used by law enforcement to monitor locations where crime is suspected of occurring, monitoring crowds during public events so as to better deploy resources, and surveilling individuals who are suspected of being involved in crime. Remote Surveillance Cameras are placed in locations that are open to the public.

(d) The fiscal costs for the surveillance technology, including initial purchase, personnel and other ongoing costs, and any current or potential sources of funding;

Initial Purchase Cost

\$25,000 (already purchased through grant funding for use by Yolo County agencies)

Personnel Costs

Nominal to install cameras and operate.

Ongoing Costs

Each of the two DPD cameras requires a cellular plan at approximately \$600/year.

Potential Sources of Funding

Davis PD obtained agency owned cameras through grant funding. Cellular plans are paid out of the normal operating budget.

(e) Whether use or maintenance of the technology will require data gathered by the technology to be handled or stored by a third-party vendor on an ongoing basis;
Remote Cameras record video to an internal DVR, which is then downloaded to a removable drive. There is no third party storage of video.

(f) A summary of the experience, if any, other governmental entities have had with the proposed technology, including information about the effectiveness, any known adverse information about the technology such as unanticipated costs, failures, civil rights or civil liberties abuses.

Remote Cameras are commonly used by law enforcement, city governments and private entities. These cameras are portable and can be easily moved if needed. They are an effective tool at remotely monitoring designated public areas.

Surveillance Use Policy

Council must adopt a policy at a regularly scheduled City Council meeting for use of the surveillance technology that at a minimum specifies the following:

(a) Purpose: The specific purpose(s) that the surveillance technology item is intended to advance.

To provide remote video observation in designated public locations.

Equipment shall not be used in an unequal or discriminatory manner and shall not target protected individual characteristics including, but not limited to race, ethnicity, national origin, religion, disability, gender or sexual orientation.

Equipment shall not be used to harass, intimidate or discriminate against any individual or group.

(b) Authorized Use: The uses that are authorized, and the rules and processes required prior to such use.

Remote Cameras will be used to monitor certain city events where there are large crowds, provide remote surveillance for areas where criminal activity is occurring and of subjects suspected of being involved in criminal activity.

(c) Data Collection: The information that can be collected by the surveillance technology, including “open source” data.

Remote Cameras can collect still images and record video. The images and video are not open source data and are stored to an internal DVR on the individual camera.

(d) Data Access: The category of individual who can access or use the collected information, and the rules and processes required prior to access or use of the information.

The video and/or images may be accessed by law enforcement officers during an investigation and court process. If the information is included as evidence in a criminal case, the information will be accessed by the prosecuting attorney and the defense attorney through the discovery process.

All downloaded media shall be stored in a secure area with access restricted to authorized persons. A recording needed as evidence shall be copied to a suitable medium and booked into evidence in accordance with established evidence procedures. All actions taken with respect to retention of media shall be appropriately documented.

(e) Data Protection: The general safeguards that protect information from unauthorized access, including encryption and access control mechanisms. Nothing in this subsection shall be construed to require the disclosure of information that could reveal vulnerabilities to, or otherwise increase the potential for an attack on, an information technology system of the City.

Information gathered by Remote Cameras can be stored to an internal DVR and then saved onto a removable drive. Video/images gathered as part of a law enforcement investigation are saved by the investigating officer and saved to a secure police evidence server.

All downloaded and retained media shall be treated in the same manner as other evidence. Media shall be accessed, maintained, stored and retrieved in a manner that ensures its integrity as evidence, including strict adherence to chain of custody requirements. Electronic trails, including encryption, digital masking of innocent or uninvolved individuals to preserve anonymity, authenticity certificates and date and time stamping, shall be used as appropriate to preserve individual rights and to ensure the authenticity and maintenance of a secure evidentiary chain of custody.

- (f) Data Retention: The time period, if any, for which information collected by the surveillance technology will be routinely retained, the reason such retention period is appropriate to further the purpose(s), the process by which the information is regularly deleted after that period lapses, and the specific conditions that must be met to retain information beyond that period.**

The type of video surveillance technology employed and the manner in which recordings are used and stored will affect retention periods. The recordings should be stored and retained in accordance with the established records retention schedule. If recordings are evidence in any claim filed or any pending litigation, they shall be preserved until pending litigation is resolved.

Any recordings needed as evidence in a criminal or civil proceeding shall be copied to a suitable medium and booked into evidence in accordance with current evidence procedures.

- (g) Public Access: How collected information can be accessed or used by members of the public, including criminal defendants.**

All recorded video images gathered by the cameras are for the official use of the Davis Police Department.

Requests for recorded video images from the public or the media shall be processed in the same manner as requests for department public records.

Members of the public do not have access to this information when it is gathered as part of a criminal investigation.

Requests for recorded images from other law enforcement agencies shall be referred to the Police Chief for release in accordance with a specific and legitimate law enforcement purpose.

Recorded video images that are the subject of a court order or subpoena shall be processed in accordance with the established department subpoena process.

- (h) Third Party Data Sharing: If and how other City or non-City entities can access or use the information, including any required justification or legal standard necessary to do so and any obligations imposed on the recipient of the information.**

Images gathered by Remote Cameras may be shared with other law enforcement agencies who are involved in a joint investigation, or who are conducting their own investigations. Images may also be shared with other law enforcement agencies who are involved in a joint investigation, or who are conducting their own investigations. Also images can be shared with various prosecutors' offices, including District Attorney's, State Attorney or United States Attorney, as well as with defense attorneys through the discovery process when they are evidence.

- (i) Training: The training required for any individual authorized to use the surveillance technology or to access information collected by the surveillance technology.**

All department members authorized to operate or video shall receive appropriate training. Training should include guidance on the use of cameras, interaction with dispatch and patrol operations and a review regarding relevant policies and procedures, including this policy. Training should also address state and federal law related to the use of video equipment and privacy.

- (j) Auditing and Oversight: The mechanisms to ensure that the Surveillance Use Policy is followed, including internal personnel assigned to ensure compliance with the policy, internal record keeping of the use of the technology or access to information collected by the technology, technical measures to monitor for misuse, any independent person or entity with oversight authority, and the legally enforceable sanctions for violations of the policy.**

Remote Cameras must be authorized by a police sergeant, Lieutenant or other sworn administrator. Use of these cameras for criminal investigations is documented in police report. These devices are stored at the police department or other law enforcement facility while not in use. A member is subject to discipline for unauthorized use or misuse.

The Police Chief or the authorized designee will conduct an annual review of the public safety video surveillance system. The review should include an analysis of the cost, benefit and effectiveness of the system, including any public safety issues that were effectively addressed or any significant prosecutions that resulted, and any systemic operational or administrative issues that were identified, including those related to training, discipline or policy.

The results of each review shall be appropriately documented and maintained by the Police Chief or the authorized designee and other applicable advisory bodies. Any recommendations for training or policy will be promptly addressed.