STAFF REPORT

DATE: June 20, 2023

TO: City Council

FROM: Darren Pytel, Police Chief
Jason Best, Director, Information Systems
Stan Gryczko, Director, Public Works Utilities & Operations
Deanne Machado, Director, Parks & Community Services

SUBJECT: Surveillance Technology Renewals

Recommendation

Based on the City's surveillance technology ordinance, there are 18 different types of surveillance technology to review and reauthorize. Each has its own staff report and recommendations, although the format for the recommendations is the same for each type of technology:

1. Review the reports regarding the use of each type of technology (Accurint, Body and In-Car Cameras, Care Trak, Cellebrite, Covert Personal Recording Device, Crisis Negotiations Equipment, Explosive Ordnance Disposal Robot, GeoTime, GPS Trackers, License Plate Readers, Public Safety Cameras, Trail Cameras, First/F Parking Garage Cameras, 1818 5th Street Corporation Yard Cameras, Davis Community Transit Cameras, Wildlife Trail Cameras, Wildlife Video Cameras, Public Works Cameras)
2. Hold a public hearing to consider the continued use of the technologies
3. Determine that the continued use of the technologies is balanced with the need to investigate and prevent crimes; protect crime victims and society from those who commit crimes; protect civil rights and civil liberties, including privacy and free expression; and the costs to the city.
4. Approve the continued use of each technology and the respective use policies.

Fiscal Impact

There is no fiscal impact to this review. Each technology has costs associated with its purchase, upkeep and use, and those are handled through the regular citywide budget process.

Council Goal(s)

Ensure a safe, heathy, equitable community

Commission Input

After the annual review of the surveillance technology equipment in 2022, the Police Accountability Commission requested additional time for the 2023 review. The Police Department prepared and shared the usage reports with the Commission for their April

meeting. The Commission appointed a subcommittee to review the information and report back to the full Commission. The Commission was not prepared to speak to the item at the May meeting, but did discuss the surveillance technology at the June meeting. In general, they expressed interest in having more details for most of the technologies, however had no comments that would suggest the Departments should stop using any of the technologies. Below is a recap of their comments for each technology.

- Accurint Virtual Crime Center – The Commission felt the description was vague.

- Body-Worn and In-Car Cameras – The Commission engaged in some discussion about officer training and consequences if the cameras were not deployed appropriately. This information is included in the Use Policy.

- CelleBrite Universal Forensic Extraction Device – Commission wanted to clarify whether it was necessary to get a warrant to get into the phone.

- Automated License Plate Reader – The Commission thought it would be helpful to have additional explanation on how the technology is allowed to be used. Information can be found in the Use Policy.

- Remote Public Safety Cameras – The Commission would recommend that the Council consider installing additional cameras near the Highway 113 entrance/exit ramps.

- For the following technologies, the Commission had no comments: Care Track System, Crisis Negotiations Equipment, Covert Personal Recording, Explosive Ordnance Disposal Robot, GeoTime Computer Program, GPS Tracker, Trail Cameras.

Background and Analysis

The subsequent reports address the use of the following technologies:

- Accurint *
- Body-Worn and In-Car Cameras *
- Care Trak *
- Cellebrite *
- Covert Personal Recording Device
- Crisis Negotiations Equipment
- Explosive Ordnance Disposal Robot
- GeoTime
- GPS Trackers *
- License Plate Readers *
- Public Safety Cameras *
- Trail Cameras *

- IS 1st/F Parking Garage (non-Police)*
- IS 1818 Cameras (non-Police)*
- PCS - DCT Cameras (non-Police)*
- Public Works Wildlife Trail Cameras (non-Police)*
- Public Works Wildlife Video Cameras (non-Police)
- Public Works Cameras (non-Police)*

* = Item Used During Reporting Period

For the reporting period, four of the types of equipment used by the Police Department was not used; the remaining eight were. For the non-Police Department equipment, 3 types were used and one was not deployed during the reporting period.

There were two violations during the reporting period where a Body-Worn Camera was not activated when it should have been. Corrective action was taken. There were no other violations of equipment or complaints received about use of any of the equipment types.

The summary chart immediately following this staff report is intended to provide a quick-glance snapshot of the use of surveillance technology, along with any problems that arose with its use over the reporting period. Additional details and information are in each separate equipment report and in the accompanying use policies.

Attachments

1. Police Use Summary Chart
2. Accurint
3. Body-Worn and In-Car Cameras
4. Care Trak
5. Cellebrite
6. Covert Personal Recording Device
7. Crisis Negotiations Equipment
8. Explosive Ordnance Disposal Robot
9. GeoTime
10. GPS Trackers
11. License Plate Readers
12. Public Safety Cameras
13. Trail Cameras
14. IS 1st/F Parking Garage (non-Police)
15. IS 1818 Cameras (non-Police)
16. PCS - DCT Cameras (non-Police)
17. Public Works Wildlife Trail Cameras (non-Police)
18. Public Works Wildlife Video Cameras (non-Police)
19. Public Works Cameras (non-Police)

Surveillance Technology Annual Review 2023-Summary

Name	How Used	How Shared	Complaints or Violations	Info/Stats to Assess Effectiveness	Public Records Requests	PAC Input 2023
Accurint Virtual Crime Center (AVCC)	The system was used 622 times. The queried results were used for information gathering to support ongoing investigations or active incidents.	No information was shared.	None	The queried information was needed and useful. Additionally, partner agencies were able to query Davis information as needed for regional crime.	No	The Commission felt the description was vague.
Body Worn and In-Car Cameras	Sworn officers are issued body-worn cameras. Officers, including plain-clothes officers, are expected to record activities and interactions that include, but are not limited to, the following: • Arrests and detentions, or situations where an officer reasonably believes they will make an arrest or detention (to include pedestrian/traffic stops and consensual encounters made with the intent to develop reasonable suspicion to detain); • Assisting in an arrest or detention situation; • Uses of force; • Confrontational law enforcement related interactions; • Vehicle and foot pursuits; • Suspect interrogations and Miranda advisements (excluding interrogations occurring in a recorded interview room) and, generally, interviews of victims and witnesses; and • Forced entries, search warrants, and warrantless searches (including vehicles). Every police vehicle that is fully marked and whose primary purpose is for patrol use contains an in-car camera system. Unless exceptional circumstances exist, it is expected that the following incidents will be both audibly and visually recorded: Generally, any incident or event in which audio/video documentation would likely have evidentiary value. Such circumstances include, but are not limited to:	Information was routinely discovered to the District Attorney's Office. They were required to share videos to criminal defense attorneys pursuant to discovery law. The Department of Justice for use in criminal investigations. Private defense attorneys pursuant to subpoena requests. Defendants for traffic court pursuant to discovery law.	There were two violations where a BWC was not activated when it should have been. Corrective action was taken.	Crime statistics are not particularly relevant to this type of surveillance technology. As described in (a)(1) above, the cameras are activated during certain situations.	Body camera and in-car camera video was released to private defense attorneys pursuant to the Public Records Act.	The Commission engaged in some discussion about officer training and consequences if the cameras were not deployed appropriately. This information is included in the Use Policy.

Name	How Used	How Shared	Complaints or Violations	Info/Stats to Assess Effectiveness	Public Records Requests	PAC Input 2023
	• Traffic stops/ contacts, including pedestrian and bicycle stops/contacts • Vehicle pursuits • Crimes in progress • Arrests, contacts/field interviews, field investigative detentions • Any situation or event that the officer, through training and experience, believes audio/video recording/documentation would be prudent and beneficial for evidentiary or administrative purposes.					
Care Track	There are several residents wearing the Care Trak transmitters. None required locating.	No information was shared.	None	The Police Department continues to get requests from subscribers to use the system.	The Police Department continues to get requests from subscribers to use the system.	
Cellebrite Universal Forensic Extraction Device	CUFED was used to serve criminal search warrants on 26 devices for 18 felony investigations. 3 searches were also done based on consent from victims to gather evidence in felony cases.	Information was shared with District Attorney and the issuing judges pursuant to the search warrant returns. Information was also properly discovered as required.	None	The use of the device is still the most effective way to access electronic information on a cell phone	No	Commission wanted to clarify whether it was necessary to get a warrant to get into the phone.
Crisis Negotiations Equipment	Critical Incident Negotiations (CNT) equipment – The CNT equipment consists of a command module, two laptop computers that are used to run the software programs and record audio/video of the incident, and a “throw phone” which is equipped with multiple cameras. For evidentiary purposes,	No information was shared.	None	Crime statistics are not particularly relevant to this type of surveillance technology. The	No	

Name	How Used	How Shared	Complaints or Violations	Info/Stats to Assess Effectiveness	Public Records Requests	PAC Input 2023
	negotiations must be audio recorded. The majority of negotiations are accomplished by calling the subject on the phone. In some cases it is necessary to provide the subject with the “throw phone”. The throw phone is essentially a phone in a protective case with a very long phone cord attached to it. The equipment was not used during the reporting period.			equipment is deployed in reaction to a subject who has barricaded themselves and/or has taken hostages.		
Covert Personal Recording Devices	Equipment was not used during this review period.	No information was shared.	None	Equipment not used during this review period	No	
Explosive Ordnance Robot	The robot was not used in Davis.	No information was shared.	None	See uses	No	
GeoTime Computer Program	This system was not used.	No information was shared.	None	Department did not have crime analyst during most of the review period.	No	
GPS Trackers	Equipment was used 6 during a criminal investigation pursuant to search warrants for various felony crimes	The information was shared with prosecuting agencies and the courts on search warrant returns.	None	The use of trackers is still the most efficient and safest way to track vehicles and/or objects for criminal investigations.	No	
Automated License Plate Readers	The system was used for parking enforcement. The ALPR system consists of a high speed camera with an infrared (“IR”) filter or two cameras—one high resolution digital camera and one IR camera—to capture images of license plates; a processor and application capable of performing sophisticated optical character recognition (OCR) to transform the image of the plate into alphanumeric characters; and a user interface to display the images captured, the results of the OCR	Not shared	None	The ALPR systems are installed on parking enforcement vehicles and used for electronic chalking and e-permit verification.	No	The Commission thought it would be helpful to have additional explanation on how the technology is

Name	How Used	How Shared	Complaints or Violations	Info/Stats to Assess Effectiveness	Public Records Requests	PAC Input 2023
	transformation, and an alert capability to notify operators of violations (for timed zone parking enforcement and to determine whether the plate is associated with a parking permit).					allowed to be used. Information can be found in the Use Policy.
Remote Public Safety Cameras	The fixed cameras were used in several criminal investigations including hit and run cases at In-N-Out Burger, collisions occurring on Mace and Richards and organized retail theft at Target. A few notable cases: Assault with Deadly Weapon and Brandishing a firearm. Clearly showed entire incident and was used in the prosecution. Brandishing a firearm. Clearly showed the entire incident and were able to get suspect info/ vehicle info. Significant commercial burglary. Used to get clear video of license plates on both suspects vehicles. Missing person at-risk. Was able to confirm vehicle she left in and direction of travel. This person was later located by officers in a remote area and needed immediate medical care to save her life. Bank theft. Able to confirm license plates and ID co-conspirators.	Videos from the fixed cameras were used for criminal investigations throughout the year, including information that was used for cases submitted to the District Attorney.	None.	No new information	No	The Commission would recommend that the Council consider installing additional cameras near the Highway 113 entrance/ exit ramps.
Trail Cameras	A Trail Camera was deployed for a short period of time at a location where significant vandalism was occurring.	No information was shared.	None	The equipment was used at a particular location that was repeatedly vandalized. It was effective and the crimes stopped.	No	

Surveillance Technology Annual Review 2023-Summary

Name	How Used	How Shared	Complaints or Violations	Info/Stats to Assess Effectiveness	Public Records Requests	PAC Input 2023
IS 1st/F Parking Garage	This equipment was used 5 times to determine cause on property damage.	No information was shared	None		One PRA request for property damage without a police report.	
IS 1818 Cameras	This equipment was used 14 times to determine cause on property damage, locate missing equipment and staff training.	No information was shared	None		No	
PCS Davis Community Transit Cameras	Footage reviewed 1 time	No information was shared	None	In one instance, additional follow up was provided to customer regarding procedures.	No	
PW Wildlife Trail Cameras	A wildlife trail camera (1) was deployed from April 10 to April 21, 2023 at the North Davis Meadows Agricultural Buffer to monitor activity at an American kestrel nest box. A wildlife trail camera (2) was deployed in the Cannery Agricultural Buffer from April 21 to May 15, 2023 to monitor the effectiveness of ground squirrel control equipment.	No information was shared.	None	Data informed management planning related to the species.	No	
PW Wildlife Video Cameras	Wildlife video cameras were not used during this period	No information was shared	None	N/A	No	
Public Works Cameras	The equipment is used to monitor critical infrastructure and locations with chemical / fuel storage.	No information was shared.	None		No	

STAFF REPORT

DATE: June 20, 2023

TO: City Council

FROM: Darren Pytel, Police Chief

SUBJECT: Surveillance Technology – 2023 Annual Surveillance Report, Accurint Virtual Crime Center

---

Recommendation

1. Receive Annual Surveillance Report regarding the use of the Accurint Virtual Crime Center (26.070.060 (a) Davis Municipal Code (DMC)).
2. Hold a public hearing to consider the continued use of the Accurint Virtual Crime Center (26.070.060 (b) Davis Municipal Code (DMC)).
3. Determine the continued use of the Accurint Virtual Crime Center has been balanced with the need to investigate and prevent crimes; protect crime victims and society from those who commit crimes; protect civil rights and civil liberties, including privacy and free expression; and the costs to the City.
4. Approve the continued use of the Accurint Virtual Crime Center and the existing use policy (attachment 1).

Fiscal Impact

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

Council Goal(s)

This item is consistent with the Council goal to ensure a safe, healthy, equitable community. It is not tied to a specific task; however, it is part of normal city business activity.

Commission Involvement

This report and accompanying information were sent to the Police Accountability Commission for their April 3, 2023, meeting.

Background and Analysis

The Davis Municipal Code requires a city department that uses surveillance technology to provide an annual written report for each approved item. More specifically,

> ***Section 26.07.060 Oversight following council approval.***
>
> *(a) By the end of each fiscal year, a city department that uses surveillance technology must present a written annual surveillance report at a regular city council meeting for city council review for each approved surveillance technology item. If the city department is unable to meet the deadline, the department head shall notify the city council in writing of staff's request to extend this period, and the reasons for that request. The city council may grant reasonable extensions to comply with this section.*

(b) Based upon information in the annual surveillance report, the city council will, at a regular city council meeting, balance the need to: investigate and prevent crimes; protect crime victims and society from those who commit crimes; protect civil rights and civil liberties, including privacy and free expression; and the costs to the city and will determine whether to continue to allow the use of the surveillance technology item, cease use, or propose modifications to the corresponding Surveillance Use Policy.

At the June 28, 2022, city council meeting approving the continued use of this technology, council directed staff to provide the annual reports to the Police Accountability Commission (PAC) 75 days prior to reporting to the city council. The information in this report covers July 1, 2022, to March 17, 2023, when the reports were completed for the PAC. As this cycle continues in the future, the annual reports will cover April to April each year although council will not be asked to approve the continued use of the technology until June or later each year.

2023 Annual Surveillance Report – Accurint Virtual Crime Center (AVCC)

(a) The Annual Surveillance Report will include all of the following:

(1) A general description of how the surveillance technology was used;

The system was used 622 times. The queried results were used for information gathering to support ongoing investigations or active incidents.

(2) A general description of whether and how often data acquired through the use of the surveillance technology item was shared with outside entities, the name of any recipient entity, the type(s) of data disclosed, under what legal standard(s) the information was disclosed, and the justification for the disclosure(s);

The data was not queried for the specific purpose of sharing with outside entities. The data has been used in police reports, which may be discoverable.

(3) A summary of community complaints or concerns about the surveillance technology item;

No complaints or concerns were submitted to the Police Department.

(4) The results of any internal audits required by the Surveillance Use Policy, any information about violations of the Surveillance Use Policy, and a general description of any actions taken in response;

There were no violations of the Surveillance Use Policy.

(5) Information, including crime statistics, that help the City Council assess whether the surveillance technology has been effective at achieving its identified purposes;

The queried information was needed and useful. Additionally, partner agencies were able to query Davis information as needed for regional crime.

(6) Statistics and information about any related Public Records Act requests;

There have been no PRA requests regarding this surveillance technology.

(7) Total annual costs for the surveillance technology, including personnel and other ongoing costs, and what source of funding will fund the technology in the coming year;

Ongoing costs are currently $5,134 per year.

(8) Any requested modifications to the Surveillance Use Policy and a detailed basis for the request;

No recommended changes.

(9) Where applicable, a general breakdown of what physical objects the surveillance technology hardware was installed upon, using general descriptive terms; for surveillance technology software, a general breakdown of what data sources the surveillance technology was applied to.

Not applicable. This technology is not deployed.

(10) A summary of all requests for City Council approval for the use of the surveillance technology item, including whether the City Council approved or rejected the proposal and/or required changes to a proposed Surveillance Use Policy before approval

The City Council previously authorized use of the AVCC at the March 10, 2020, city council meeting, the September 21, 2021, city council meeting, and the June 28, 2022, city council meeting. No other requests have been made.

The City Council previously authorized use of the AVCC at the March 10, 2020, city council meeting[1], the September 21, 2021, city council meeting[2], and the June 28, 2022 city council meeting[3]. The information from those staff reports is still in effect and should be considered for the request of the continued use of the item.

Attachments

1. Use Policy – AVCC

[1] https://documents.cityofdavis.org/Media/Default/Documents/PDF/CityCouncil/CouncilMeetings/Agendas/2020/2020-03-10/04A-Accurint-Virtual-Crime-Center-Surveillance-Tech.pdf

[2] https://documents.cityofdavis.org/Media/Default/Documents/PDF/CityCouncil/CouncilMeetings/Agendas/2021/2021-09-21/06-Surveillance-Technology-Renewals.pdf

[3] https://documents.cityofdavis.org/Media/Default/Documents/PDF/CityCouncil/CouncilMeetings/Agendas/2022/2022-06-28/06-Surveillance-Technology-Renewals.pdf

DAVIS POLICE DEPARTMENT

ACCURINT
Policy and Procedure 6.10-B

DEPARTMENT MANUAL

On March 10, 2020, the Davis City Council, in accordance with the Surveillance Technology Ordinance, adopted the following ACCURINT Virtual Crime Center Use Policy (26.07.030 Davis Municipal Code)

Surveillance Use Policy

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

AVCC provides electronic access to regional law enforcement and open source data to assist in the expedient interdiction of crime. AVCC provides tools, such as hot spot mapping and link charting, to assist in the processing of crime and open source data. These tools exponentially increase the value of data by providing insight into patterns and connections at a pace necessary to disrupt crime.

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

This technology may only be used upon request by authorized personnel to advance or assist in the investigation of a criminal case. Access to this system will be reserved for use on a "need to know" and "right to know" basis. Employees assigned to Investigations, Crime Analysis, Dispatch AND who have also received AVCC training may use the technology.

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

Information available through access to AVCC may include, but is not limited to: call for service data, case narrative data, jail inmate data, vehicle records and field interview data. In addition to law enforcement data, AVCC also provides open source data to the requestor such as address data, court records, social media and white pages data.

(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.

Products made using AVCC (maps, linkcharts) may only be used or accessed by the requesting Department member. If the product has evidentiary value and is therefore included as a supplement to a criminal case in our records management system, the product may be discoverable.

(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.

Products made using AVCC are generally kept in digital format and are password protected. If a requestor prints materials produced from AVCC, the requestor is responsible for keeping said materials in a locked location when not in use to prevent unauthorized access.

(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.

Materials produced from AVCC will be kept as long as necessary and that time period is case specific. At the conclusion of an investigation, should the requestor no longer need the materials, the requestor will shred physical copies and delete any digital copies.

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

Collected information cannot be accessed or used by members of the public. Criminal defendants and their attorneys may be entitled to the information through the criminal discovery process or as otherwise required by law.

(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.

Extracted data is generally only used by the Davis Police Department. However, extracted data may be shared with other law enforcement agencies who are involved in a joint criminal investigation, or who are conducting their own criminal investigation. Sharing data requires authorization from command staff. Data can also be shared with various prosecutors' offices, including District Attorney's, State Attorney or United States Attorney, as well as with criminal defendants and their attorneys through the criminal discovery process or as otherwise required by law.

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

Individuals who operate AVCC are trained in its use by the vendor or by trained Department members. Training by Department members will include a module on acquisition, retention, destruction and confidentiality around access.

(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.

Department administration is responsible for overseeing and auditing the use of the technology and to ensure this policy is followed.

The use of the technology is documented in a criminal police report or intelligence report. A member is subject to discipline and possible criminal prosecution for unauthorized use or misuse of criminal justice information.

The Police Chief or the authorized designee will conduct an annual review of the use of the technology. The review should include an analysis of the cost, benefit and effectiveness of the technology, 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.

Darren Pytel
Police Chief
3/2020

STAFF REPORT

DATE: June 20, 2023

TO: City Council

FROM: Darren Pytel, Police Chief

SUBJECT: Surveillance Technology – 2023 Annual Surveillance Report, Police Body-Worn Cameras/In-car Cameras

---

Recommendation

1. Receive Annual Surveillance Report regarding the use of police body-worn cameras and in-car camera systems (26.070.060 (a) Davis Municipal Code (DMC))
2. Hold a public hearing to consider the continued use of police body-worn cameras and in-car camera systems (26.070.060 (b) DMC).
3. Determine the continued use of the police body-worn cameras and in-car camera systems have been balanced with the need to investigate and prevent crimes; protect crime victims and society from those who commit crimes; protect civil rights and civil liberties, including privacy and free expression; and the costs to the City.
4. Approve the continued use of the police body-worn cameras and in-car camera systems and the existing use policies (Attachments 1 and 2).

Fiscal Impact

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

Council Goal(s)

This item is consistent with the Council goal to ensure a safe, healthy, equitable community. It is not tied to a specific task; however, it is part of normal city business activity.

Commission Involvement

This report and accompanying information were sent to the Police Accountability Commission for their April 3, 2023, meeting.

Background and Analysis

The Davis Municipal Code requires a city department that uses surveillance technology to provide an annual written report for each approved item. More specifically,

> ***Section 26.07.060 Oversight following council approval.***
>
> *(a) By the end of each fiscal year, a city department that uses surveillance technology must present a written annual surveillance report at a regular city council meeting for city council review for each approved surveillance technology item. If the city department is unable to meet the deadline, the department head shall notify the city council in writing of staff's request to extend this period, and the reasons for that request. The city council may grant reasonable extensions to comply with this section.*

(b) Based upon information in the annual surveillance report, the city council will, at a regular city council meeting, balance the need to: investigate and prevent crimes; protect crime victims and society from those who commit crimes; protect civil rights and civil liberties, including privacy and free expression; and the costs to the city and will determine whether to continue to allow the use of the surveillance technology item, cease use, or propose modifications to the corresponding Surveillance Use Policy.

At the June 28, 2022, city council meeting approving the continued use of this technology, council directed staff to provide the annual reports to the Police Accountability Commission (PAC) 75 days prior to reporting to the city council. The information in this report covers July 1, 2022, to March 17, 2023, when the reports were completed for the PAC. As this cycle continues in the future, the annual reports will cover April to April each year although council will not be asked to approve the continued use of the technology until June or later each year.

At the November 1, 2022, city council meeting, council approved the replacement purchase of the WatchGuard (Motorola Solutions) body-worn and in-car camera systems, which are at end of life. While the Department was in the process of upgrading the system, Motorola switched the primary computer operating system to a format the City does not support. The Department is in the process of selecting a new system for council consideration.

2023 Annual Surveillance Report – Police Body-Worn Cameras and In-Car Camera Systems**.**

(a)The Annual Surveillance Report will include all of the following:

(1)A general description of how the surveillance technology was used;

Sworn officers are issued body-worn cameras. Officers, including plain-clothes officers, are expected to record activities and interactions that include, but are not limited to, the following:

- *Arrests and detentions, or situations where an officer reasonably believes they will make an arrest or detention (to include pedestrian/traffic stops and consensual encounters made with the intent to develop reasonable suspicion to detain);*
- *Assisting in an arrest or detention situation;*
- *Uses of force;*
- *Confrontational law enforcement related interactions;*
- *Vehicle and foot pursuits;*
- *Suspect interrogations and Miranda advisements (excluding interrogations occurring in a recorded interview room) and, generally, interviews of victims and witnesses; and*
- *Forced entries, search warrants, and warrantless searches (including vehicles).*

Every police vehicle that is fully marked and whose primary purpose is for patrol use contains an in-car camera system. Unless exceptional circumstances exist, it is expected that the following incidents will be both audibly and visually recorded:

Generally, any incident or event in which audio/video documentation would likely have evidentiary value. Such circumstances include, but are not limited to:

- *Traffic stops/contacts, including pedestrian and bicycle stops/contacts*
- *Vehicle pursuits*

- *Crimes in progress*
- *Arrests, contacts/field interviews, field investigative detentions*
- *Any situation or event that the officer, through training and experience, believes audio/video recording/documentation would be prudent and beneficial for evidentiary or administrative purposes.*

(2)A general description of whether and how often data acquired through the use of the surveillance technology item was shared with outside entities, the name of any recipient entity, the type(s) of data disclosed, under what legal standard(s) the information was disclosed, and the justification for the disclosure(s);

Information was routinely discovered to the District Attorney's Office. They were required to share videos to criminal defense attorneys pursuant to discovery law.

The Department of Justice for use in criminal investigations.

Private defense attorneys pursuant to subpoena requests.

Defendants for traffic court pursuant to discovery law.

(3)A summary of community complaints or concerns about the surveillance technology item;

No complaints or concerns were submitted to the Police Department.

(4)The results of any internal audits required by the Surveillance Use Policy, any information about violations of the Surveillance Use Policy, and a general description of any actions taken in response;

There were no violations of the Surveillance Use Policy.

(5)Information, including crime statistics, that help the City Council assess whether the surveillance technology has been effective at achieving its identified purposes;

Crime statistics are not particularly relevant to this type of surveillance technology. As described in (a)(1) above, the cameras are activated during certain situations.

(6)Statistics and information about any related Public Records Act requests;

There were no requests.

(7)Total annual costs for the surveillance technology, including personnel and other ongoing costs, and what source of funding will fund the technology in the coming year;

Initial Purchase Cost

On March 13, 2018, the City Council approved a budget adjustment for $100,000 for purchase of the integrated police in-car and BWC systems.

Personnel Costs
Minimal to operate the systems.

Ongoing Costs
These are built into existing budget.

Potential Sources of Funding
The $100,000 came from Supplemental Law Enforcement Services grant funds ($80,000) and the equipment maintenance fund balance ($20,000).

On November 1, 2022, the City Council approved an ~$216,115.00 budget adjustment to purchase new equipment. This funding has not yet been used.

(8) Any requested modifications to the Surveillance Use Policy and a detailed basis for the request;

No recommended changes.

(9) Where applicable, a general breakdown of what physical objects the surveillance technology hardware was installed upon, using general descriptive terms; for surveillance technology software, a general breakdown of what data sources the surveillance technology was applied to.

The body-worn cameras consist of small cameras that are worn on the officer's person. The cameras are then synced in docking stations at the Police Department and the data is downloaded onto a Department server where the data is stored.

The in-car cameras consist of small cameras that are mounted inside of each patrol vehicle and face forward through the windshield. When the patrol vehicle returns to the parking lot of the Police Department, the cameras remotely sync to the Department server where the data is downloaded and stored.

(10) A summary of all requests for City Council approval for the use of the surveillance technology item, including whether the City Council approved or rejected the proposal and/or required changes to a proposed Surveillance Use Policy before approval

The City Council previously authorized use of the cameras at the July 31, 2018, city council meeting. The City Council continues the use of the cameras at the June 18, 2019, city council meeting, the September 22, 2020, city council meeting, the September 21, 2021, city council meeting, the June 28, 2023, city council meeting, and the November 1, 2022, city council meeting. No other requests have been made.

The City Council previously authorized use of the camera systems at the July 31, 2018, city council meeting[1], the June 18, 2019, city council meeting[2], the September 22, 2020[3],

[1] https://documents.cityofdavis.org/Media/Default/Documents/PDF/CityCouncil/CouncilMeetings/Agendas/20180731/08E-Surveillance-Tech-Public-Hearing-Body-Worn-and-In-Car-Cameras.pdf

[2] https://documents.cityofdavis.org/Media/Default/Documents/PDF/CityCouncil/CouncilMeetings/Agendas/20190618/08J-Surveillance-Tech-PD-Body-Worn-Camera.pdf

city council meeting, the September 21, 2021, city council meeting[4], the June 28, 2023[5], city council meeting, and the November 1, 2022, city council meeting[6]. The information from those staff reports is still in effect and should be considered for the request of the continued use of the item.

Attachments

1. Use Policy – Body-Worn Cameras
2. Use Policy – In-Car Cameras

---

[3] https://documents.cityofdavis.org/Media/Default/Documents/PDF/CityCouncil/CouncilMeetings/Agendas/2020/2020-09-22/04-Surveillance-Tech-Reauthorization.pdf

[4] https://documents.cityofdavis.org/Media/Default/Documents/PDF/CityCouncil/CouncilMeetings/Agendas/2021/2021-09-21/06-Surveillance-Technology-Renewals.pdf

[5] https://documents.cityofdavis.org/Media/Default/Documents/PDF/CityCouncil/CouncilMeetings/Agendas/2022/2022-06-28/06-Surveillance-Technology-Renewals.pdf

[6] https://documents.cityofdavis.org/Media/Default/Documents/PDF/CityCouncil/CouncilMeetings/Agendas/2022/2022-11-01/05A1-Surveillance-Technology-Body-Worn-In-Car-Cameras.pdf

DAVIS POLICE DEPARTMENT

BODY WORN VIDEO CAMERAS
Interim Policy and Procedure 4.12-A

DEPARTMENT MANUAL

Index as:
Body worn video cameras
BWC
Cameras, body worn
Video, body worn

On November 1, 2022, the Davis City Council, in accordance with the Surveillance Technology Ordinance, adopted the following Interim Body Worn Camera Use Policy (26.07.030 Davis Municipal Code).

I. POLICY

The Davis Police Department provides most sworn officers with body worn video cameras for use during the performance of their duties. All video recordings made while working as a member of the Davis Police Department – in any capacity – are the property of the Department, and subject to review by the Department and its agents. The use of personally owned video recording devices is prohibited.

It is the specific intent of this policy to capture/record all interactions, including phone calls, related to criminal investigations on body-worn cameras or other recording devices to the extent that can be done so without violating specific privacy rights contained in the law. Interactions related to non-criminal actions should be recorded when there is consent and/or as otherwise provided in this policy.

II. PURPOSE

The Davis Police Department recognizes that video and audio recordings of interactions between law enforcement personnel and the public can provide a record of those events. The use of body worn camera (BWC) equipment is intended to assist officers in the field during the performance of their duties, and enhance the mission of the Department, by capturing those interactions between sworn officers of the Department and members of the public. To multiple ends, BWC video can provide additional information regarding enforcement and/or investigative activities and public interactions, as well as assist in collecting evidence for use in criminal investigations, including identifying and apprehending offenders, and obtaining, collecting, and preserving evidence for use in criminal prosecutions.

Such recordings, however, provide a limited perspective of the encounters, and must be considered along with all other available evidence – such as witness statements, officer interviews, forensic analyses, and documentary evidence – when evaluating the appropriateness of an officer's actions.

The Department has adopted the use of BWCs and has established BWC procedures to:

- Collect evidence for use in criminal investigations and prosecution;
- Assist officers with accurately completing reports and providing court testimony;
- Promote accountability;
- Deter criminal activity and uncooperative behavior during police-public interactions;

- Assist in the investigation and resolution of complaints against officers; and
- Provide information to aid in officer evaluation, training, and continuous improvement.

III. PROCEDURE

A. Guidelines for Activation of BWC

1. Officers, including plain-clothes officers, are expected to record activities and interactions that include, but are not limited to, the following:

   - Arrests and detentions, or situations where an officer reasonably believes they will make an arrest or detention (to include pedestrian/traffic stops and consensual encounters made with the intent to develop reasonable suspicion to detain);
   - Assisting in an arrest or detention situation;
   - Uses of force;
   - Confrontational law enforcement related interactions;
   - Vehicle and foot pursuits;
   - Suspect interrogations and Miranda advisements (excluding interrogations occurring in a recorded interview room) and, generally, interviews of victims and witnesses; and
   - Forced entries, search warrants, and warrantless searches (including vehicles).

   Officers are expected to activate their BWC as soon as practicable upon encountering the above types of events. Optimally, officers should activate their BWC prior to arrival at these types of events in order to ensure the entire event is captured. When an officer is unable to activate their BWC at the beginning of an event, they should document the reason in their police report; if a police report is taken. At no time should an officer jeopardize their safety, or the safety of any other officer, in order to activate a BWC.

   Officers may use discretion when deciding whether or not to advise a person they are being recorded. Generally, officers should not cease recording based solely on the request or demand of a person.

2. Informal Community Interactions (Public Encounters) – Informal community interactions differ from the "consensual encounters" officers' conduct in an effort to develop reasonable suspicion to detain or probable cause for arrest. To strengthen relationships between police and the public, officers may use discretion regarding the recording of informal, non-enforcement related interactions with the public. In the event an encounter becomes adversarial or an enforcement action may take place, officers are expected to activate their BWC; without compromising their safety or the safety of others.

3. Victims and Witnesses of Crime – Officers are expected to record interviews of crime victims and witnesses. Officers have no obligation to advise victims or witnesses that they are being recorded, but may do so at their discretion. When a victim or witness requests they not be recorded, officers may consider their request when deciding whether to continue recording or not. Officers may offer to avert their BWC to capture only audio during the interview when doing so would facilitate obtaining a recorded statement.

   In cases where a victim or witness requests they not be recorded, and the officer agrees not to record, officers should record their request prior to turning off their BWC. Minimally, the person should be told that a criminal case could be hampered by not

recording the interview. When an officer is already recording, they shall record their explanation for turning off their BWC prior to doing so.

In the event a crime witness or a member of the public wishes to anonymously report or discuss criminal activity, officers have the discretion to not record.

4. Domestic Violence Victims – Officers are expected to record interviews of domestic violence victims to facilitate future prosecution efforts and discourage later recanting of statements. Officers are expected to also record interviews with children who witness domestic violence, when the child is willing.

5. Child Abuse and Sexual Assault Victims – Officers are expected to record interviews. In cases where the victim requests they not be video recorded, officers should minimally audio record the interview.

6. First Amendment Activity – Officers should not record individuals who are picketing, or engaged in peaceful protest or First Amendment protected speech/activities – unless the officer believes a violation of criminal law is occurring, may occur, or if the officer has direct interaction with a participant or third party to the event.

B. Knowledge of Recording

Penal Code Section 632 prohibits any individual from surreptitiously recording any conversation in which any party to the conversation has a reasonable belief that the conversation was private or confidential. However, Penal Code Section 633 expressly exempts law enforcement from this prohibition during the course of a criminal investigation.

- Any officer may surreptitiously record conversations during the normal course of duty related to a criminal investigation in which the officer reasonably believes that such a recording will be beneficial to the investigation.
- Any officer contacting an individual suspected of violating any law, or during the course of any official law enforcement related activity, shall be presumed to be engaged in a criminal investigation. This presumption shall not apply to contacts with other officers occurring for solely administrative purposes.
- Any individual contacted by an officer of the Department wearing a conspicuously mounted recording device (BWC) will be deemed to have knowledge that such a contact is being recorded.

C. Operating Procedures

1. Officers, including plain-clothes officers, who have been issued a BWC shall wear it at all times they may become involved in an enforcement situation. Officers shall position the BWC to facilitate an optimum recording field of view.

2. At the beginning of their shift, officers will inspect the BWC for any physical damage and to ensure the device is in working order. Any damaged, malfunctioning, or missing equipment shall be immediately reported to a supervisor. Additionally, as soon as practicable, notification of the equipment problem should be made, via email, to PDIS. Additionally, officers shall notify dispatch over the radio if they are not wearing a functional BWC. Dispatch shall log the information in CAD under the officer's unit history for their shift.

3. In general, once the BWC recorder is activated, officers are expected to continue recording until the incident has concluded, recording is no longer relevant, or there is no apparent value to continued recording.

    - A BWC may not be turned off during a use-of-force incident until the event has fully stabilized and never while in the presence of any person threatened with or subjected to force.
    - If the BWC is in use during any other situation, and it becomes necessary to discuss issues or concerns with another officer or supervisor in private away from any person who is being detained and/or in custody, the BWC may be turned off. The intention to stop the recording will be noted by the officer verbally before switching the device off. When the private conversation has ended, the BWC recording is expected to resume.

4. Either a patrol car's in-car camera or an officer's BWC must be activated during the transport of any person. Officers are expected to record the processing and/or booking, and all other interactions with a person who is in custody.

5. When an interview is to be recorded, and time and opportunity permit, the recording officer shall:

    - Test the recording device/equipment to ensure it is functioning and ready to record prior to commencing the interview or recording;
    - Make a statement at the beginning of the recording to identify:
        - The date and time of the interview or recording;
        - The location of the interview or recording; and
        - The identities of all parties involved in, or present at, the interview or recording.
    - Record any other pertinent and/or identifying information, such as phone numbers called during recorded interviews, informant numbers when name identities cannot be used, etc.;
    - Describe the time of, and reason for, any temporary stoppage of the recording and include the fact all parties had knowledge of the stoppage;
    - Record the date and time recording ended at the conclusion of each interview; and
    - Whenever possible, ensure the device recorded properly before the interviewed person leaves.

    When circumstances do not permit compliance with the above guidelines (i.e., spontaneous recordings) as much of the information as possible should be included at the end of the recording to identify the conversation.

6. Officers are responsible for transferring all recordings to the proper Department file server by the end of each shift and before going off-duty.

D. Prohibited/Restricted Recordings and Acts

1. BWCs shall not be used to record non-work-related, personal activity.

2. BWCs will not intentionally be activated in places where a heightened expectation of privacy exists, such as workplace locker rooms, dressing rooms, or restrooms.

3. No type of recording device may be intentionally activated to record the conversations of fellow members or superiors without their knowledge.

4. Officers should not record undercover officers or confidential informants, absent supervisor approval under limited circumstances.

5. When possible, officers should avoid recording exposed private areas of the body.

6. Officers should not record patients during any medical or psychological evaluation or treatment by a healthcare professional unless the person is engaging in violence or may engage in violence or when force was used against the person during their arrest or detention. While inside a medical or psychological facility, officers should avoid recording persons other than the intended person.

7. Recordings shall not be made or used for the sole purpose of ridiculing or embarrassing any Department member or member of the public.

8. Members shall not obtain or convert, for their personal use, any recordings obtained during the course of their official duties. The following are specifically prohibited:

    - Making personal copies of official recordings;
    - Re-recording of videos with other devices;
    - Posting of official video and/or audio to any non-Department sponsored social networking or other web sites; and
    - Posting of recordings on any Department sponsored site without the express permission from the Police Chief or their designee. Any video posted on a Department sponsored social media or other website will thereafter be considered public information.

9. Recordings shall not be transmitted, shared or transferred via e-mail (or by any other electronic process), except for official purposes, and only by personnel who have been authorized by the system administrator.

10. BWCs should not be used to record statements intended solely for civil liability purposes unless there is full consent from the person being recorded.

E. Review and Use of Recordings

1. Officers should review recordings to assist with their investigation, prior to the completion of their report. Recorded statements shall be summarized and documented within the narrative of the applicable report.

2. Critical Incidents – The Davis Police Department acknowledges that video recordings taken during critical incidents do not necessarily reflect the full extent of the nature of the event; or the experience, analysis, training, threat assessment, or state of mind of the individual officers(s) in a given incident. Moreover, recordings, especially video, have limitations, and may depict events differently than as honestly recalled by the involved officer(s). Specifically, it is understood that recording devices may capture information that may not have been heard or observed by the involved officers, and that officers may see and hear things not captured by recording devices.

    - For the purposes of this policy, critical incidents include:

        - Officer-involved shootings, regardless of whether a person was hit by gunfire;
        - A traffic collision involving death or serious bodily injury to another person;
        - A use of force resulting in death or serious bodily injury to another person; or

- All deaths while an arrestee/detainee is in the custodial care of the Department unless there is no preliminary evidence of any of the following: misconduct, a use of force, or an act committed by an arrestee/detainee that appears intended to cause injury or death.

- Officers involved in critical incidents should notify the responding supervisor of any related recordings. In the event a critical incident is recorded, and immediate retrieval of a recording is required, a supervisor shall secure the recording device as soon as possible and maintain the chain of custody. The supervisor or manager charged with coordinating the criminal investigation of the case shall coordinate the download or electronic transfer of the file, minimizing those involved with the chain of custody.

- Officers, either as subjects or witness, who are involved in any critical incident will be permitted to review recordings after providing a statement or making a written report, if needed. In such cases where the involved officer(s) will view a video recording of the incident, they shall be provided the following admonishment:

  "In this case, there is video evidence that you will have an opportunity to view after you have given your initial statement. Video evidence has limitations and may depict the events differently than you recall, and may not depict all of the events as seen or heard by you. Video has a limited field of view and may not capture events normally seen by the human eye. The "frame rate" of video may limit the camera's ability to capture movements normally seen by the human eye. Lighting as seen on the video may be different than what is seen by the human eye. Videos are a two dimensional medium and may not capture depth, distance, or positional orientation as well as the human eye. Remember, video evidence is intended to assist your memory and ensure that your initial statement explains your state of mind at the time of the incident."

F. Reviewing and Media Duplication

1. Officers will have review access to recorded media downloaded from BWC's. Officers are expected to view their videos daily to ensure that their equipment is functioning correctly.

2. The Property & Evidence Specialist will have review and copying access rights for all recordings. The access will be used for the express purpose of copying recordings for evidence.

3. Supervisors/managers will have review access rights for training, administrative purposes, and evidentiary purposes.

4. The release of video captured by a BWC to any third party will be processed in a manner consistent with applicable departmental policy, law and current discovery requests. When criminal charges are being sought, all related recordings will be provided to the District Attorney's Office.

5. The digitally recorded media and all recorded images are the property of the Davis Police Department. Dissemination outside the agency is strictly prohibited without specific authorization of the Police Chief or their designee, except as otherwise provided for under Policy & Procedure 4.13-A, Release of Video Evidence, which requires the release of certain video evidence.

G. Supervisor Responsibilities

Supervisors with BWC-equipped officers under their command shall:

1. Ensure that officers under their command have completed the required Department BWC training and are familiar with applicable policies and procedures;
2. Conduct periodic inspections of officers assigned BWC equipment and ensure that the BWCs are properly affixed to officers' uniforms and fully/properly operable;
3. Ensure officers upload all BWC recordings at the end of their shifts;
4. Ensure officers tag accidental/inadvertent/unnecessary BWC recordings – recordings made in error; and
5. Review relevant BWC recordings prior to submitting any reports.

H. Use in Training/Incident Debriefs

Use of any video for training purposes requires approval of the Police Chief or their designee.

I. System Administrator

The system administrator is the manager overseeing Property & Evidence. The system administrator has oversight responsibilities including, but not limited to, the following:

- Ensuring recordings of evidentiary value are secure and retained according to the Department's retention schedule;
- Ensuring all other files are maintained in accordance with the Department's retention schedule;
- Conducting periodic, random audits to ensure the BWC system is operating properly and the camera is being utilized in accordance with this Policy & Procedure;
- System evaluation;
- Assessment and recommendations for modification of policies, procedures and practices associated with video recording;
- Training; and
- Coordination with IS regarding system related issues.

J. Request for Deletion of Accidental Recording

In the event of an accidental or sensitive personal recording using a BWC, where the resulting recording is of no investigative or evidentiary value, the recording employee may request that the file be deleted by submitting an email request to the Office of the Police Chief. The administrator will review the file and recommend approval or denial of the request. In cases where the administrator denies the request to delete, an appeal may be submitted to the Police Chief for deletion authorization. In all cases of deletion requests, a determination should be made within 7 calendar days.

K. Media Retention

Pursuant to California Government Code Section 34090.6(a), "…the head of a department of a city or city and county, after one year, may destroy recordings of routine video monitoring…This destruction shall be approved by the legislative body and the written consent of the agency attorney shall be obtained. In the event that the recordings are evidence in any claim filed, or any pending litigation, they shall be preserved until that pending action/litigation is resolved."

It is the policy of the Davis Police Department to maintain recorded media for the minimum one year period prescribed by law. The retention period may be extended if the audio/video recording is known to have evidentiary value.

Darren Pytel
Police Chief
8/15

Revised: 4/18, changes to expectations
5/18, critical incident protocol amended
8/18, slight change as required by City Council
Reviewed 3/16, 08/17, 12/17, 05/19, 11/22

DAVIS POLICE DEPARTMENT

MOBILE VIDEO RECORDING EQUIPMENT AND STORAGE
Policy and Procedure 4.10-A

DEPARTMENT MANUAL

Index as:
In-Car Camera
Mobile Video
Camera, In-Car
Video, In-Car

On November 1, 2022, the Davis City Council, in accordance with the Surveillance Technology Ordinance, adopted the following Mobile Video Recording (MVR) Use Policy (26.07.030 Davis Municipal Code)

I. POLICY

It is the policy of the Davis Police Department to use audio-visual recorded media to provide additional evidence of criminal activity, to provide training opportunities for police officers, and to maintain public trust and citizen confidence in police procedures.

II. PROCEDURE

A. Definitions

In-Car Camera System and Mobile Video Recording are synonymous and defined as any in-car equipment that captures audio and visual signals.

B. Officer Responsibility

1. Inspection of MVR equipment shall be the responsibility of the officer assigned to that vehicle and shall occur at the beginning of the officer's shift prior to placing the vehicle in service. The assigned officer shall perform an inspection to ensure the MVR is performing in accordance with the manufacturer recommendations.

2. The officer shall inspect the following equipment to insure that it is operational:

    a. Remote Audio Transmitter:
        1. Ensure adequate power source
        2. Ensure it is connected to the recording equipment
        3. Ensure that remote activation is functioning

    b. Camera Lens:
        1. Windshield and camera lens are free of obstructions
        2. Camera facing intended direction

    c. Recording mechanism is capturing both audio and visual information and system plays back both audio and visual tracks.

3. Any malfunction of the in-car camera equipment shall be reported to the immediate supervisor prior to the unit being placed in service and the officer shall send an email to the PDIS email group clearly stating the malfunction. The supervisor shall assign the officer to a unit containing a functioning MVR. If the supervisor is unable to provide the officer with

a unit that has a functioning MVR and the vehicle is placed in service without an operational MVR, the officer shall contact dispatch and advise the dispatcher, via audio radio transmission, that the MVR is not operational. The dispatcher will make a notation on the officer's unit history for the day.

4. In the event that the inoperable MVR is located in a canine vehicle, the canine officer should continue to use their assigned vehicle and notify their supervisor and dispatch, via audio radio transmission, that the MVR is not operational. The dispatcher will make a notation on the officer's unit history for the day.

5. Damage or theft of the MVR shall be immediately documented and reported to the immediate supervisor. The officer shall send an email to the PDIS email group clearly stating what the damage is.

6. Unless exceptional circumstances exist, it is expected that the following incidents will be both audibly and visually recorded:

    a. Generally, any incident or event in which audio/video documentation would likely have evidentiary value. Such circumstances include, but are not limited to:

        1. Traffic stops/contacts, including pedestrian and bicycle stops/contacts
        2. Vehicle pursuits
        3. Crimes in progress
        4. Arrests, contacts/field interviews, field investigative detentions

    b. Any situation or event that the officer, through training and experience, believes audio/video recording/documentation would be prudent and beneficial for evidentiary or administrative purposes.

7. In general, once the MVR is activated, officers are expected to continue recording until the incident has concluded, recording is no longer relevant, or there is no apparent value to continued recording.

    - A MVR may not be turned off during a use-of-force incident until the event has fully stabilized and never while in the presence of any person threatened with or subjected to force.
    - If the MVR is in use during any other situation, and it becomes necessary to discuss issues or concerns with another officer or supervisor in private away from any person who is being detained and/or in custody, the MVR may be turned off. The intention to stop the recording will be noted by the officer verbally before switching the device off. When the private conversation has ended, the MVR recording is expected to resume.

8. Officers shall ensure the volume from other electronics devices within the police vehicle such as; radios, CD players etc, are turned down when the MVR is activated (this does not apply to police radios.)

9. When the officer detects that the recording time remaining on the media is less than 1 hour they should, when practical, return to the police department to the designated area and download the media via WiFi technology.

C. Supervisors Responsibilities

1. Supervisors informed of a malfunction of the equipment shall ensure that PDIS was notified by email or in person.

2. When an incident arises that requires the retrieval of the recorded media (serious crime scene, departmental shooting, departmental accidents, etc) a supervisor shall ensure that the recorded media is downloaded prior to putting the vehicle back into service.

D. Evidence Technician's Responsibilities

1. Responsible for duplicating the recorded media after receiving a request from the involved officer.

2. Responsible for all long-term storage of media deemed to be of evidentiary value in conjunction with Departmental regulations for the storage of evidence and the Department retention schedule.

F. Reviewing and Media Duplication

The primary purposes of the MVR system are to provide a depiction of events for courtroom presentation, enhance the officer's ability to document and review statements and actions for report purposes and provide an impartial measurement for self-critique for the officer. Therefore, the following personnel will have review and/or copying access to the recorded media:

1. Officers will have review access to recorded media downloaded from their assigned patrol car. An officer will not have review access to the recorded media of other officers, unless it is necessary for an investigation. Officers should periodically view their videos to insure that their equipment is functioning correctly. This shall be done at least once per work week. The audit log will display that officers are following this procedure.

2. The Evidence Technician will have review access and copying access for all MVR systems. The access will be used for the express purpose of copying MVR recordings for evidence.

3. Supervisors and FTO's will have review and copying access rights for training, administrative purposes, and evidentiary purposes.

4. An officer's MVR recordings may be made available for roll call training with the permission of the Police Chief.

5. The digitally recorded media and all recorded images are the property of the Davis Police Department and dissemination outside the agency is strictly prohibited without specific authorization of the Police Chief or their designee, except as otherwise provided for under Policy & Procedure 4.13-A, Release of Video Evidence, which requires the release of certain video evidence.

6. To prevent damage to or alteration of the original recorded media, it shall not be copied or viewed from any device not approved by the departmental media technician.

G. Media Retention

Pursuant to Section 34090.6(a) of the California Government Code, "…the head of a department of a city or city and county, after one year, may destroy recordings of routine video monitoring…This destruction shall be approved by the legislative body and the written consent of the agency attorney shall be obtained. In the event that the recordings are evidence in any claim filed or any pending litigation, they shall be preserved until pending litigation is resolved."

"Routine video monitoring" as defined by Section 34090.6(c) "means video taping by a video or electronic imaging system designed to record the regular and ongoing operations of the departments described in subdivision (a), including mobile in-car video systems…"

It is the policy of the Davis Police Department to maintain mobile video recorded media for the minimum one year period proscribed by law.

Darren Pytel
Police Chief

Created:
09/05

Revised:
12/05: Addition of Section III.C.6. and III.C.10. Deletion of Section III.C.7.c.
01/06: Addition of Section III.C.5. Revision of III.C.8. and III.F.3.
06/08: Changes to II, B 8, 9 and F
05/10: minor changes to recording contacts
06/18: minor edits to make consistent with BWC policy
08/18: minor edits for City Council approval

Reviewed:
11/05, 12/05, 1/06, 10/11, 08/17, 12/17, 05/19, 11/22

STAFF REPORT

DATE: June 20, 2023

TO: City Council

FROM: Darren Pytel, Police Chief

SUBJECT: Surveillance Technology – 2023 Annual Surveillance Report, Care Trak System

---

Recommendation

1. Receive Annual Surveillance Report regarding the use of the Care Trak System (26.070.060 (a) Davis Municipal Code (DMC)).
2. Hold a public hearing to consider the continued use of the Care Trak system (26.070.060 (b) Davis Municipal Code (DMC)).
3. Determine the continued use of the Care Trak system has been balanced with the need to investigate and prevent crimes; protect crime victims and society from those who commit crimes; protect civil rights and civil liberties, including privacy and free expression; and the costs to the City.
4. Approve the continued use of the Care Trak system and the existing use policy (attachment 1).

Fiscal Impact

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

Council Goal(s)

This item is consistent with the Council goal to ensure a safe, healthy, equitable community. It is not tied to a specific task; however, it is part of normal City business activity.

Commission Involvement

This report and accompanying information were sent to the Police Accountability Commission for their April 3, 2023, meeting.

Background and Analysis

The Davis Municipal Code requires a city department that uses surveillance technology to provide an annual written report for each approved item. More specifically,

> ***Section 26.07.060 Oversight following council approval.***
>
> *(a) By the end of each fiscal year, a city department that uses surveillance technology must present a written annual surveillance report at a regular city council meeting for city council review for each approved surveillance technology item. If the city department is unable to meet the deadline, the department head shall notify the city council in writing of staff's request to extend this period, and the reasons for that request. The city council may grant reasonable extensions to comply with this section.*

(b) Based upon information in the annual surveillance report, the city council will, at a regular city council meeting, balance the need to: investigate and prevent crimes; protect crime victims and society from those who commit crimes; protect civil rights and civil liberties, including privacy and free expression; and the costs to the city and will determine whether to continue to allow the use of the surveillance technology item, cease use, or propose modifications to the corresponding Surveillance Use Policy.

At the June 28, 2022, city council meeting approving the continued use of this technology, council directed staff to provide the annual reports to the Police Accountability Commission (PAC) 75 days prior to reporting to the city council. The information in this report covers July 1, 2022, to March 17, 2023, when the reports were completed for the PAC. As this cycle continues in the future, the annual reports will cover April to April each year although council will not be asked to approve the continued use of the technology until June or later each year.

2023 Annual Surveillance Report – Care Trak System

(a)The Annual Surveillance Report will include all of the following:

(1)A general description of how the surveillance technology was used;

There are several residents wearing the Care Trak transmitters. None required locating.

(2)A general description of whether and how often data acquired through the use of the surveillance technology item was shared with outside entities, the name of any recipient entity, the type(s) of data disclosed, under what legal standard(s) the information was disclosed, and the justification for the disclosure(s);

No information was shared.

(3)A summary of community complaints or concerns about the surveillance technology item;

No complaints or concerns were submitted to the Police Department.

(4)The results of any internal audits required by the Surveillance Use Policy, any information about violations of the Surveillance Use Policy, and a general description of any actions taken in response;

There were no violations of the Surveillance Use Policy.

(5)Information, including crime statistics, that help the City Council assess whether the surveillance technology has been effective at achieving its identified purposes;

The Police Department continues to get requests from subscribers to use the system.

(6)Statistics and information about any related Public Records Act requests;

There have been no PRA requests regarding this surveillance technology.

(7)Total annual costs for the surveillance technology, including personnel and other ongoing costs, and what source of funding will fund the technology in the coming year;

Use existing donated funds.

(8)Any requested modifications to the Surveillance Use Policy and a detailed basis for the request;

No recommended changes.

(9)Where applicable, a general breakdown of what physical objects the surveillance technology hardware was installed upon, using general descriptive terms; for surveillance technology software, a general breakdown of what data sources the surveillance technology was applied to.

Devices are applied to people who subscribe.

(10) A summary of all requests for City Council approval for the use of the surveillance technology item, including whether the City Council approved or rejected the proposal and/or required changes to a proposed Surveillance Use Policy before approval

The City Council previously authorized use of the Care Trak System at the July 31, 2018, city council meeting, the June 18, 2019, city council meeting, the September 22, 2020, city council meeting, the September 21, 2021, city council meeting, and the June 28, 2022, city council meeting. No other requests have been made.

The City Council previously authorized use of the Care Trak System at the July 31, 2018, city council meeting[1], the June 18, 2019, city council meeting[2], the September 22, 2020, city council meeting, the September 21, 2021, city council meeting[3], and the June 28, 2023, city council meeting[4]. The information from those reports is still in effect and should be considered for the request of the continued use of the item.

Attachments

1. Use Policy – Care Trak System

---

1 https://documents.cityofdavis.org/Media/Default/Documents/PDF/CityCouncil/CouncilMeetings/Agendas/20180731/08B-Surveillance-Tech-Public-Hearing-Care-Trak.pdf

2 https://documents.cityofdavis.org/Media/Default/Documents/PDF/CityCouncil/CouncilMeetings/Agendas/2020/2020-09-22/04-Surveillance-Tech-Reauthorization.pdf

3 https://documents.cityofdavis.org/Media/Default/Documents/PDF/CityCouncil/CouncilMeetings/Agendas/2021/2021-09-21/06-Surveillance-Technology-Renewals.pdf

4 https://documents.cityofdavis.org/Media/Default/Documents/PDF/CityCouncil/CouncilMeetings/Agendas/2022/2022-06-28/06-Surveillance-Technology-Renewals.pdf

DAVIS POLICE DEPARTMENT

CARE TRAK SYTEM
Policy and Procedure 6.01-B

DEPARTMENT MANUAL

On July 31, 2018, the Davis City Council, in accordance with the Surveillance Technology Ordinance, adopted the following Care Trak System Use Policy (26.07.030 Davis Municipal Code)

Surveillance Use Policy

(a) Purpose: The specific purpose(s) that the surveillance technology item is intended to advance.
This technology is specifically intended to assist in determining the physical location of an at-risk individual so that they may be brought to safety.

(b) Authorized Use: The uses that are authorized, and the rules and processes required prior to such use.
Personnel are permitted to use this technology only when a locate request is made by a participant (or their family/care taker). Only trained operators are permitted to use the technology.

(c) Data Collection: The information that can be collected by the surveillance technology, including "open source" data.
None.

(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.
Any Davis Police Department employee who is a trained operator may use the technology.

(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.
The participant list is only accessible by police employees. To access the list in electronic format, employees must use the records management system which is password protected and includes an audit trail for each user. The physical, hard-copy list may only be accessed by the program administrator and is kept in a secure, locked location.

(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.

Information retained as part of this technology includes a participant list, in both hard copy and digital formats. The participant list is updated when/if a participant notifies the police department that they are no longer interested in participating in the program.

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

N/A

(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.

N/A

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

Prior to obtaining authorization to use this technology, the operator must complete a training program which is currently facilitated by a Davis Police Department employee.

(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.

The facility administrator is responsible for tracking/auditing all components of the program annually.

The subscriber Agreement is attached. (Attachment 1)

Attachments

1. Subscriber Agreement

Darren Pytel
Police Chief
July 31, 2018

Attachment 1

DAVIS POLICE DEPARTMENT

Care Trak Agreement

This agreement is made on the _____day of 20 _____, by and between the **Davis Police Department** (hereafter, **DPD**) and _____ _____(hereafter, **RESPONSIBLE PARTY**) whose address is _____City _____ State ____ Zip_____ for the care of _____(hereafter, **CLIENT**) whose address is_____ City _____ State ____ Zip_____

Whereas, DPD is voluntarily undertaking a program for search using electronic signaling devices (the Care Trak device) as an aid in searching for lost persons who suffer in one form or another from diminished mental capacity or other disability; and,

Whereas, DPD is under no legal or other duty to provide such a search system to persons suffering from diminished capacity or disability; and,

Whereas, DPD does not act as an agent, representative, or surrogate for any other person, body or legal entity in undertaking the program, and neither obligates nor is able to obligate any other person, body or legal entity by undertaking a program; and,

Whereas, the **RESPONSIBLE PARTY** named herein is empowered, able and authorized to act in the name of and on the behalf of the **CLIENT** named above; and,

Whereas, the **RESPONSIBLE PARTY** desires to participate for the benefit of the **CLIENT** in the program being undertaken:

Therefore, IN CONSIDERATION OF THE MUTUAL PROMISES MADE HEREIN, the above parties agree as follows:

1. **DPD** agrees to furnish the **CLIENT** named above the use and benefit of a tracking system consisting of a transmitter wristband and tracking services appropriate and necessary for the use of such equipment.

2. The **RESPONSIBLE PARTY** agrees to pay a one-time equipment fee of $_____ for the purchase of the transmitter wristband and testing device and a maintenance fee of $_____ per month for a transmitter battery and attaching band.

Purchase will be made directly by the **RESPONSIBLE PARTY** to Care Trak. The cost may increase at the sole discretion of Care Trak.

3. It is the duty of the **RESPONSIBLE PARTY** to immediately notify **DPD** at: **(530) 758-3600, 2600 Fifth St. Davis, CA 95618** in the event the designated **CLIENT** of the tracking bracelet is discovered missing from the **RESPONSIBLE PARTY'S** care. **RESPONSIBLE PARTY** must call if **CLIENT** is not located within five (5) minutes of searching.

4. In the event the transmitter wristband is no longer needed by the **CLIENT**, **RESONSIBLE PARTY** is to notify **DPD** immediately so that said bracelet can be removed and the **CLIENT'S** frequency can be re-assigned.

5. If the transmitter wristband is lost or otherwise rendered unusable, the **RESPONSIBLE PARTY** shall immediately notify **DPD**. Any re-purchase or replacement cost is the sole responsibility of **RESPONISBLE PARTY**. Replacement parts and equipment can be purchased through Care Trak.

6. It is expressly understood and agreed that the **RESONSIBLE PARTY** is responsible for the routine maintenance of the equipment provided hereunder. **DPD** is not responsible in any respect for any technical failure due to manufacturing or material defects of the equipment herein provided. It is expressly understood and agreed that the **DPD** makes no warranties of any kind with regard to the equipment described herein, the operation or effectiveness of the equipment described herein, the fitness or suitability of the equipment described herein for a particular purpose, or the merchantability of the equipment described herein.

7. It is specifically agreed and understood that the **RESPONSIBLE PARTY** shall retain ownership in said equipment.

8. This agreement may be terminated at the option of either party upon thirty (30) days written notice to the other party.

9. The **RESPONSIBLE PARTY** specifically acknowledges and agrees that the tracking system is **NOT** intended to replace the direct care, monitoring, attention and oversight to be provided by the **RESPONSIBLE PARTY** to the **CLIENT** named above. The **RESPONSIBLE PARTY**, on behalf of the **CLIENT**, accepts the use of the equipment and the services described above with the understanding that the equipment and services are intended to be merely an additional and ancillary (supplementary) tool providing an extra means of locating the **CLIENT** in the event the **CLIENT** is discovered missing. The **RESPONSIBLE PARTY** further agrees to check the operation of the tracking bracelet a minimum of **two times per day at 12 hour intervals** and log the times checked on the **Transmitter Tester Log** for examination by **DPD**. The **RESPONSIBLE PARTY** also agrees to keep and maintain Transmitter Tester Log readings each day.

10. The **RESPONSIBLE PARTY**, hereby releases **DPD** from any and all liability arising from early failure of the equipment or any failure of whatever sort, kind, or nature,

regarding the performance and fulfillment of the monitoring, response and tracking services described, or any other ends for which this agreement is made. **DPD** shall not be held responsible for any failure, delay, default, interruption, stoppage or interference of any other failure of any kind, manner, or nature regarding the performance of the equipment of services under this contract.

The **RESPONSIBLE PARTY** hereby releases and holds harmless **DPD** for all action and interaction on its part and indemnifies **DPD** against all claims, actions, lawsuits, or causes of action brought against **DPD** whether by **RESPONSIBLE PARTY**, or on **RESPONSIBLE PARTY'S** behalf, or by others even if such claim is false or fraudulent, and regardless of who the parties may be.

11. The **RESPONSIBLE PARTY** understands and agrees that the **DPD** makes no warranties, guarantees, assurances, or promise of any kind as to the effectiveness or success of the tracking services provided herein or of any search or searches undertaken utilizing the system or other electronic equipment used during the term of this contract or program.

12. The **RESPONSIBLE PARTY** specifically agrees and promises not to rely upon the equipment or services herein for the safety, security, welfare, finding or retrieval of the **CLIENT** wearing the transmitter wristband.

    The **RESPONSIBLE PARTY** agrees and understands that the equipment and services provided under this contract may be ineffective and unavailing for the purpose provided. Therefore, the **PRESPONSIBLE PARTY** specifically disclaims any reliance, expectation of success, or dependence upon the equipment or services for the health, safety, welfare, finding, rescue, or retrieval of the **CLIENT** named above.

    By signing below; I, the **RESPONSIBLE PARTY**, affirm that I have read and understood this contract, including the waiver and release of liability and the non-reliance provisions, and that it is my desire and intention to enter into this agreement. By affixing my signature below, I hereby agree to the terms and provisions of this contract.

_____	_____
RESPONSIBLE PARTY	DAVIS POLICE DEPARTMENT
_____	_____
Street Address / P.O. Box	Street Address / P.O. Box
_____	_____
City, State, Zip	City, State, Zip
_____	_____

Telephone Telephone

STAFF REPORT

DATE: June 20, 2023

TO: City Council

FROM: Darren Pytel, Police Chief

SUBJECT: Surveillance Technology – 2023 Annual Surveillance Report, Cellebrite Universal Forensic Extraction Device

---

Recommendation

1. Receive Annual Surveillance Report regarding the use of the Cellebrite Universal Forensic Extraction Device (CUFED) (26.070.060 (a) Davis Municipal Code (DMC)).
2. Hold a public hearing to consider the continued use of the CUFED (26.070.060 (b) DMC).
3. Determine the continued use of the CUFED has been balanced with the need to investigate and prevent crimes; protect crime victims and society from those who commit crimes; protect civil rights and civil liberties, including privacy and free expression; and the costs to the City.
4. Approve the continued use of the CUFED and the existing use policy (Attachment 1).

Fiscal Impact

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

Council Goal(s)

This item is consistent with the Council goal to ensure a safe, healthy, equitable community. It is not tied to a specific task; however, it is part of normal city business activity.

Commission Involvement

This report and accompanying information were sent to the Police Accountability Commission for their April 3, 2023, meeting.

Background and Analysis

The Davis Municipal Code requires a city department that uses surveillance technology to provide an annual written report for each approved item. More specifically,

> ***Section 26.07.060 Oversight following council approval.***
>
> *(a) By the end of each fiscal year, a city department that uses surveillance technology must present a written annual surveillance report at a regular city council meeting for city council review for each approved surveillance technology item. If the city department is unable to meet the deadline, the department head shall notify the city council in writing of staff's request to extend this period, and the reasons for that request. The city council may grant reasonable extensions to comply with this section.*

(b) Based upon information in the annual surveillance report, the city council will, at a regular city council meeting, balance the need to: investigate and prevent crimes; protect crime victims and society from those who commit crimes; protect civil rights and civil liberties, including privacy and free expression; and the costs to the city and will determine whether to continue to allow the use of the surveillance technology item, cease use, or propose modifications to the corresponding Surveillance Use Policy.

At the June 28, 2022, city council meeting approving the continued use of this technology, council directed staff to provide the annual reports to the Police Accountability Commission (PAC) 75 days prior to reporting to the city council. The information in this report covers July 1, 2022, to March 17, 2023, when the reports were completed for the PAC. As this cycle continues in the future, the annual reports will cover April to April each year although council will not be asked to approve the continued use of the technology until June or later each year.

2023 Annual Surveillance Report – CUFED

(a)The Annual Surveillance Report will include all of the following:

(1)A general description of how the surveillance technology was used;

CUFED was used to serve criminal search warrants on 26 devices for 18 felony investigations. 3 searches were also done based on consent from victims to gather evidence for felony cases.

(2)A general description of whether and how often data acquired through the use of the surveillance technology item was shared with outside entities, the name of any recipient entity, the type(s) of data disclosed, under what legal standard(s) the information was disclosed, and the justification for the disclosure(s);

Information was shared with District Attorney and the issuing judges pursuant to the search warrant returns. Information was also properly discovered as required.

(3)A summary of community complaints or concerns about the surveillance technology item;

No complaints or concerns were submitted to the Police Department.

(4)The results of any internal audits required by the Surveillance Use Policy, any information about violations of the Surveillance Use Policy, and a general description of any actions taken in response;

There were no violations of the Surveillance Use Policy.

(5)Information, including crime statistics, that help the City Council assess whether the surveillance technology has been effective at achieving its identified purposes;

The use of the device is still the most effective way to access electronic information on a cell phone.

(6)Statistics and information about any related Public Records Act requests;

There have been no PRA requests regarding this surveillance technology.

(7)Total annual costs for the surveillance technology, including personnel and other ongoing costs, and what source of funding will fund the technology in the coming year;

Staff costs to operate the device and prepare reports. $4,654.75 (plus tax) license fee.

(8)Any requested modifications to the Surveillance Use Policy and a detailed basis for the request;

No recommended changes.

(9)Where applicable, a general breakdown of what physical objects the surveillance technology hardware was installed upon, using general descriptive terms; for surveillance technology software, a general breakdown of what data sources the surveillance technology was applied to.

Not Applicable.

(10) A summary of all requests for City Council approval for the use of the surveillance technology item, including whether the City Council approved or rejected the proposal and/or required changes to a proposed Surveillance Use Policy before approval

The City Council previously authorized use of the CUFED at the October 30, 2018, city council meeting, the June 18, 2019, city council meeting, the September 22, 2020, city council meeting, the September 21, 2021, city council meeting, and the June 28, 2023, city council meeting. No other requests have been made.

The City Council previously authorized use of the CUFED at the October 30, 2018, city council meeting[1], the June 18, 2019, city council meeting[2], the September 22, 2020, city council meeting[3], the September 21, 2021, city council meeting[4], and the June 28, 2022, city council meeting[5]. The information from the previous staff reports is still in effect and should be considered for the request of the continued use of the item.

---

1 https://documents.cityofdavis.org/Media/Default/Documents/PDF/CityCouncil/CouncilMeetings/Agendas/20181030/08B-Surveillance-Technology-Cellebrite.pdf

2 https://documents.cityofdavis.org/Media/Default/Documents/PDF/CityCouncil/CouncilMeetings/Agendas/20190618/08D-Surveillance-Tech-PD-Cellebrite.pdf

3 https://documents.cityofdavis.org/Media/Default/Documents/PDF/CityCouncil/CouncilMeetings/Agendas/2020/2020-09-22/04-Surveillance-Tech-Reauthorization.pdf

4 https://documents.cityofdavis.org/Media/Default/Documents/PDF/CityCouncil/CouncilMeetings/Agendas/2021/2021-09-21/06-Surveillance-Technology-Renewals.pdf

5 https://documents.cityofdavis.org/Media/Default/Documents/PDF/CityCouncil/CouncilMeetings/Agendas/2022/2022-06-28/06-Surveillance-Technology-Renewals.pdf

Attachments

1. Use Policy – CUFED

DAVIS POLICE DEPARTMENT

CELLEBRITE USE
Policy and Procedure 6.04-B

DEPARTMENT MANUAL

On October 30, 2018, the Davis City Council, in accordance with the Surveillance Technology Ordinance, adopted the following Cellebrite Universal Forensic Extraction Device (CUFED) Use Policy (26.07.030 Davis Municipal Code)

Surveillance Use Policy

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

The CUFED is used to extract data from cell phones, smart phones or PDA's for use in criminal investigations.

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

The CUFED will be used to extract data from cell phones, smart phones or PDA's during criminal investigations via search warrant, written owner consent or when command staff has determined that exigent circumstances exist and that data must be extracted without delay (in these cases, a search warrant shall be secured within 3 days following the search as required by California Penal Code Part. 2, Title 12, Chapter 3.6).

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

Data includes;

- Device Information – Phone Number, IMEI, IMSI, MEID, ESN & MAC ID (identifying device info.)
- Phonebook – Contact Name and Numbers
- Call Logs
- Text and Picture Messages
- Videos and Pictures (in some cases with GeoTag-location info) and creation date and time
- Audio Files
- Emails and Web Browsing Information (in some devices)
- GPS and Location Information (in some devices)
- Social Networking messages and contacts (in some devices)
- Deleted Data – Call Logs, Messages, Emails (in some devices)
- PIN Locked and Pattern Locked Bypass & Data Extraction – (on some devices – not all phones bypassed)
- Attached Media or memory card extraction (Pictures, files, app data – located on media card)
- Wireless (WI-FI) networks connected to the device (can assist in localizing a phone to a specific area)

(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 CUFED can only be used by authorized police department personnel who are trained in its use and with approval of command staff when authorized by state and federal law.

(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.

Data gathered by the CUFED is stored on a secure department server by downloading to a connected desktop computer. Data can then be printed hardcopy, loaded to a portable drive or burned to disc. All data is protected by password. The CUFED is secured in a locked area within the police building while phones and devices awaiting inspection are stored in the secured evidence room.

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.

Extracted data is attached to criminal investigations. Records related to criminal investigations are kept for statutorily varying periods depending on the type of record, whether a person has been prosecuted and/or whether the record has been lawfully sealed. Records that are no longer needed will be destroyed in accordance with laws relating to the destruction of evidence when it is no longer needed or as required by the Electronic Communications Privacy Act or court order.

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

All data is for the official use of the Davis Police Department.

Requests for data 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; it is exempt from public disclosure pursuant to a public records request.

Data that is the subject of a court order or subpoena shall be processed in accordance with the established department subpoena process.

Criminal defendants have access to information pursuant to state and federal laws relating to discovery. Discovery is overseen by the courts.

(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.

Extracted data is generally only used by the Davis Police Department. However, extracted data may be shared with other law enforcement agencies who are involved in a joint criminal investigation, or who are conducting their own criminal investigation. Sharing data requires authorization from command staff. Data can also be shared with various prosecutors' offices, including District Attorney's, State Attorney or United States Attorney, as well as with criminal defendants and their attorneys through the criminal discovery process or as otherwise required by law.

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

Individuals who operate the CUFED are trained in its use by department trainers and may also receive training directly from the vendor.

(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.

The use of the device is documented in a criminal police report. These devices are stored at the police department when 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 use of the device. The review should include an analysis of the cost, benefit and effectiveness of the device, 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.

Darren Pytel
Police Chief
October 30, 2018

STAFF REPORT

DATE: June 20, 2023

TO: City Council

FROM: Darren Pytel, Police Chief

SUBJECT: Surveillance Technology – 2023 Annual Surveillance Report, Crisis Negotiations Equipment

---

Recommendation

1. Receive Annual Surveillance Report regarding the use of the Crisis Negotiations Equipment (26.070.060 (a) Davis Municipal Code (DMC)).
2. Hold a public hearing to consider the continued use of the Crisis Negotiations Equipment (26.070.060 (b) DMC).
3. Determine the continued use of the Crisis Negotiations equipment has been balanced with the need to investigate and prevent crimes; protect crime victims and society from those who commit crimes; protect civil rights and civil liberties, including privacy and free expression; and the costs to the City.
4. Approve the continued use of the Crisis Negotiations Equipment and the existing use policy (Attachment 1).

Fiscal Impact

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

Council Goal(s)

This item is consistent with the Council goal to ensure a safe, healthy, equitable community. It is not tied to a specific task; however, it is part of normal city business activity.

Commission Involvement

This report and accompanying information were sent to the Police Accountability Commission for their April 3, 2023, meeting.

Background and Analysis

The Davis Municipal Code requires a city department that uses surveillance technology to provide an annual written report for each approved item. More specifically,

> ***Section 26.07.060 Oversight following council approval.***
>
> *(a) By the end of each fiscal year, a city department that uses surveillance technology must present a written annual surveillance report at a regular city council meeting for city council review for each approved surveillance technology item. If the city department is unable to meet the deadline, the department head shall notify the city council in writing of staff's request to extend this period, and the reasons for that request. The city council may grant reasonable extensions to comply with this section.*

(b) Based upon information in the annual surveillance report, the city council will, at a regular city council meeting, balance the need to: investigate and prevent crimes; protect crime victims and society from those who commit crimes; protect civil rights and civil liberties, including privacy and free expression; and the costs to the city and will determine whether to continue to allow the use of the surveillance technology item, cease use, or propose modifications to the corresponding Surveillance Use Policy.

At the June 28, 2022, city council meeting approving the continued use of this technology, council directed staff to provide the annual reports to the Police Accountability Commission (PAC) 75 days prior to reporting to the city council. The information in this report covers July 1, 2022, to March 17, 2023, when the reports were completed for the PAC. As this cycle continues in the future, the annual reports will cover April to April each year although council will not be asked to approve the continued use of the technology until June or later each year.

2023 Annual Surveillance Report – Crisis Negotiations Equipment

(a)The Annual Surveillance Report will include all of the following:

(1)A general description of how the surveillance technology was used;

Critical Incident Negotiations (CNT) equipment – The CNT equipment consists of a command module, two laptop computers that are used to run the software programs and record audio/video of the incident, and a "throw phone" which is equipped with multiple cameras. For evidentiary purposes, negotiations must be audio recorded. The majority of negotiations are accomplished by calling the subject on the phone. In some cases, it is necessary to provide the subject with the "throw phone". The throw phone is essentially a phone in a protective case with a very long phone cord attached to it.

The equipment was not used in any incidents during the reporting period. This is equipment is now used primarily for training and is a backup to newer equipment that is used/deployed in this area by mutual aid partners.

(2)A general description of whether and how often data acquired through the use of the surveillance technology item was shared with outside entities, the name of any recipient entity, the type(s) of data disclosed, under what legal standard(s) the information was disclosed, and the justification for the disclosure(s);

No information was shared.

(3)A summary of community complaints or concerns about the surveillance technology item;

No complaints or concerns were submitted to the Police Department.

(4)The results of any internal audits required by the Surveillance Use Policy, any information about violations of the Surveillance Use Policy, and a general description of any actions taken in response;

There were no violations of the Surveillance Use Policy.

(5)Information, including crime statistics, that help the City Council assess whether the surveillance technology has been effective at achieving its identified purposes;

Crime statistics are not particularly relevant to this type of surveillance technology. The equipment is deployed in reaction to a subject who has barricaded themselves and/or has taken hostages.

At this point, the equipment is more than 10-years old and is need of replacement. The current systems are entirely different and use cellular technology rather than wired technology.

(6)Statistics and information about any related Public Records Act requests;

There have been no PRA requests regarding this surveillance technology.

(7)Total annual costs for the surveillance technology, including personnel and other ongoing costs, and what source of funding will fund the technology in the coming year;

There was a one-time initial cost to purchase the existing equipment which was done through a grant. Since the equipment was purchased, there have been no costs associated with the equipment.

The Department is requesting the council authorize replacement equipment as follows:
Base Service: $1,495.00
LETS Respond: $995.00
LETS Bundle: $5,895.00

Existing funds would be used.

(8)Any requested modifications to the Surveillance Use Policy and a detailed basis for the request;

No recommended changes.

(9)Where applicable, a general breakdown of what physical objects the surveillance technology hardware was installed upon, using general descriptive terms; for surveillance technology software, a general breakdown of what data sources the surveillance technology was applied to.

Not Applicable.

(10) A summary of all requests for City Council approval for the use of the surveillance technology item, including whether the City Council approved or rejected the proposal and/or required changes to a proposed Surveillance Use Policy before approval

The City Council previously authorized the use of the Crisis Negotiations Equipment at the July 31, 2018, city council meeting, the June 18, 2019, city council meeting, the September 22, 2020, city council meeting, the September 21, 2021, city council meeting, and the June 28, 2023, city council meeting. No other requests have been made.

The City Council previously authorized use of the Crisis Negotiations Equipment at the July 31, 2018, city council meeting[1], the June 18, 2019, city council meeting[2], the September 22, 2020, city council meeting[3], the September 21, 2021, city council meeting[4], and the June 28, 2023, city council meeting[5]. The information from those council meetings is still in effect and should be considered for the request of the continued use of the item.

Attachments

1. Use Policy – Crisis Negotiations Equipment

---

1 https://documents.cityofdavis.org/Media/Default/Documents/PDF/CityCouncil/CouncilMeetings/Agendas/20180731/08C-Surveillance-Tech-Public-Hearing-Crisis-Negotiations-Equipment.pdf

2 https://documents.cityofdavis.org/Media/Default/Documents/PDF/CityCouncil/CouncilMeetings/Agendas/20190618/08F-Surveillance-Tech-PD-Crisis-Negotiations-Equipment.pdf

3 https://documents.cityofdavis.org/Media/Default/Documents/PDF/CityCouncil/CouncilMeetings/Agendas/2020/2020-09-22/04-Surveillance-Tech-Reauthorization.pdf

4 https://documents.cityofdavis.org/Media/Default/Documents/PDF/CityCouncil/CouncilMeetings/Agendas/2021/2021-09-21/06-Surveillance-Technology-Renewals.pdf

5 https://documents.cityofdavis.org/Media/Default/Documents/PDF/CityCouncil/CouncilMeetings/Agendas/2022/2022-06-28/06-Surveillance-Technology-Renewals.pdf

DAVIS POLICE DEPARTMENT

CRISIS NEGOTATIONS EQUIPMENT
Policy and Procedure 6.02-B

DEPARTMENT MANUAL

On July 31, 2018, the City Council, in accordance with the Surveillance Technology Ordinance adopted, the following Crisis Negotiations Equipment Use Policy (26.07.030 Davis Municipal Code)

Surveillance Use Policy

Crisis Negotiations Equipment – The equipment consists of a command module, two laptop computers that are used to run the software programs and record audio/video of the incident, and a "throw phone." The equipment is manufactured by 836 Technologies and is widely used throughout the region and country for use in crisis negotiation communications. For evidentiary purposes, negotiations must be audio recorded. The majority of negotiations are accomplished by calling the person on the phone. In some cases it is necessary to provide the person with the "throw phone". The throw phone is essentially a phone in a protective case with a very long phone cord attached to it.

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

The safe negotiation and eventual surrender of a person in crisis without injury to them, hostages, officers or members of the public.

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

Those authorized to use the equipment must be members of the Yolo County Crisis Negotiations Team (CNT). Those team members are trained how to use the equipment.

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

The technology records audio and potentially video of the incident. The technology does not use "open source" data.

(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.

Any member of the Yolo County CNT can access the data during the incident. At the conclusion of the event, the data is stored on a CD and that CD is then booked into evidence at the Davis Police Department.

(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.

Only those CNT members who are trained to use the equipment can access the data. Once the data is put on a CD, only those members who would normally have access to evidence would be able to access the data.

(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 data is considered evidence. The time period the data would be retained would be dictated by the court process.

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

The general public would not have access to the data. If criminal charges are filed against the person, they would have access to a copy of the data booked into evidence. The copy of the data is provided to the defendant through their attorney.

(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.

The technology does not use Third Party Data Sharing.

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

Several members of the CNT were initially trained by the manufacturers of the technology. The technology is used on an on-going basis.

(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.

The technology and the storage of the data is supervised and managed by the Davis Police Department Sergeant and Lieutenant assigned to the CNT.

Darren Pytel
Police Chief
July 31, 2018

STAFF REPORT

DATE: June 20, 2023

TO: City Council

FROM: Darren Pytel, Police Chief

SUBJECT: Surveillance Technology – Annual Surveillance Report, Covert Personal Recording Devices

---

Recommendation

1. Receive Annual Surveillance Report regarding the use of the Covert Personal Recording Devices (26.070.060 (a) Davis Municipal Code (DMC)).
2. Hold a public hearing to consider the continued use of Covert Personal Recording Devices (26.070.060 (b) DMC).
3. Determine the continued use of the Covert Personal Recording Devices has been balanced with the need to investigate and prevent crimes; protect crime victims and society from those who commit crimes; protect civil rights and civil liberties, including privacy and free expression; and the costs to the City.
4. Approve the continued use of the Covert Personal Recording Devices and the existing use policy (Attachment 1).

Fiscal Impact

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

Council Goal(s)

This item is consistent with the Council goal to ensure a safe, healthy, equitable community. It is not tied to a specific task; however, it is part of normal city business activity.

Commission Involvement

This report and accompanying information were sent to the Police Accountability Commission for their April 3, 2023, meeting.

Background and Analysis

The Davis Municipal Code requires a city department that uses surveillance technology to provide an annual written report for each approved item. More specifically,

> ***Section 26.07.060 Oversight following council approval.***
>
> *(a) By the end of each fiscal year, a city department that uses surveillance technology must present a written annual surveillance report at a regular city council meeting for city council review for each approved surveillance technology item. If the city department is unable to meet the deadline, the department head shall notify the city council in writing of staff's request to extend this period, and the reasons for that request. The city council may grant reasonable extensions to comply with this section.*

(b) Based upon information in the annual surveillance report, the city council will, at a regular city council meeting, balance the need to: investigate and prevent crimes; protect crime victims and society from those who commit crimes; protect civil rights and civil liberties, including privacy and free expression; and the costs to the city and will determine whether to continue to allow the use of the surveillance technology item, cease use, or propose modifications to the corresponding Surveillance Use Policy.

At the June 28, 2022, city council meeting approving the continued use of this technology, council directed staff to provide the annual reports to the Police Accountability Commission (PAC) 75 days prior to reporting to the city council. The information in this report covers July 1, 2022, to March 17, 2023, when the reports were completed for the PAC. As this cycle continues in the future, the annual reports will cover April to April each year although council will not be asked to approve the continued use of the technology until June or later each year.

2023 Annual Surveillance Report – Covert Personal Recording Devices

(a)The Annual Surveillance Report will include all of the following:

(1)A general description of how the surveillance technology was used;

Equipment was not used during this review period.

(2)A general description of whether and how often data acquired through the use of the surveillance technology item was shared with outside entities, the name of any recipient entity, the type(s) of data disclosed, under what legal standard(s) the information was disclosed, and the justification for the disclosure(s);

No information was shared.

(3)A summary of community complaints or concerns about the surveillance technology item;

No complaints or concerns were submitted to the police department.

(4)The results of any internal audits required by the Surveillance Use Policy, any information about violations of the Surveillance Use Policy, and a general description of any actions taken in response;

There were no violations of the Surveillance Use Policy.

(5)Information, including crime statistics, that help the City Council assess whether the surveillance technology has been effective at achieving its identified purposes;

Equipment was not used during this review period.

(6)Statistics and information about any related Public Records Act requests;

There have been no PRA requests regarding this surveillance technology.

(7)Total annual costs for the surveillance technology, including personnel and other ongoing costs, and what source of funding will fund the technology in the coming year;

No additional costs nor are any anticipated.

(8)Any requested modifications to the Surveillance Use Policy and a detailed basis for the request;

No recommended changes.

(9)Where applicable, a general breakdown of what physical objects the surveillance technology hardware was installed upon, using general descriptive terms; for surveillance technology software, a general breakdown of what data sources the surveillance technology was applied to.

Not Applicable.

(10) A summary of all requests for City Council approval for the use of the surveillance technology item, including whether the City Council approved or rejected the proposal and/or required changes to a proposed Surveillance Use Policy before approval

The City Council previously authorized use of the Covert Personal Recording Devices at the October 30, 2018, city council meeting, the June 18, 2019, city council meeting, the September 22, 2020, city council meeting, the September 21, 2021, city council meeting, and the June 28, 2022, city council meeting. No other requests have been made.

The City Council previously authorized use of the Covert Personal Recording Devices at the October 30, 2018[1], city council meeting, the June 18, 2019, city council meeting[2], the September 22, 2020, city council meeting[3], the September 21, 2021, city council meeting[4], and the June 28, 2022, city council meeting[5]. The information from those staff reports is still in effect and should be considered for the request of the continued use of the item.

---

1 https://documents.cityofdavis.org/Media/Default/Documents/PDF/CityCouncil/CouncilMeetings/Agendas/20181030/08C-Surveillance-Technology-Covert-Personal-Recording-Device.pdf

2 https://documents.cityofdavis.org/Media/Default/Documents/PDF/CityCouncil/CouncilMeetings/Agendas/20190618/08E-Surveillance-Tech-PD-Covert-Personal-Recording-Device.pdf

3 https://documents.cityofdavis.org/Media/Default/Documents/PDF/CityCouncil/CouncilMeetings/Agendas/2020/2020-09-22/04-Surveillance-Tech-Reauthorization.pdf

4 https://documents.cityofdavis.org/Media/Default/Documents/PDF/CityCouncil/CouncilMeetings/Agendas/2021/2021-09-21/06-Surveillance-Technology-Renewals.pdf

5 https://documents.cityofdavis.org/Media/Default/Documents/PDF/CityCouncil/CouncilMeetings/Agendas/2022/2022-06-28/06-Surveillance-Technology-Renewals.pdf

Attachments

1. Use Policy – Covert Personal Recording Devices

DAVIS POLICE DEPARTMENT

COVERT PERSONAL RECORDING DEVICE USE
Policy and Procedure 6.05-B

DEPARTMENT MANUAL

On October 30, 2018, the Davis City Council, in accordance with the Surveillance Technology Ordinance, adopted the following Covert Personal Recording Devices Use Policy (26.07.030 Davis Municipal Code)

Surveillance Use Policy

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

Improve public safety by providing an effective tool used to record undercover or covert police operations.

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

Covert Personal Recording Devices will be used for undercover operations during criminal investigations and will be used or monitored by sworn peace officers. Use of the devices must be authorized by a supervisor or manager.

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.

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

Covert Personal Recording Devices record voice conversations or video images. The data is not open source and is stored on a vendor secure server.

(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 information will 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 Covert Personal Recording Devices can be stored in one of two ways. Devices that are simply recording to a receiver that is controlled by the investigating officer, generally stores the information on the device and later downloads it onto a secure police evidence server. Devices that require vendor support generally keep information stored on the vendors secure servers.

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 and for a minimum of one year. If recordings are evidence in any claim filed or any pending litigation, they shall be preserved until pending litigation is fully resolved.

Recordings are generally attached to criminal investigations. Records related to criminal investigations are kept for statutorily varying periods depending on the type of record, whether a person has been prosecuted and/or whether the record has been lawfully sealed.

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. Records that are no longer needed will be destroyed in accordance with laws relating to the destruction of evidence or by court order.

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

All recordings are for the official use of the Davis Police Department.

Requests for records 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 recordings when they are gathered as part of a criminal investigation; it is exempt from public disclosure pursuant to a public records request.

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

Criminal defendants have access to information pursuant to state and federal laws relating to discovery. Discovery is overseen by the courts.

(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.

Information gathered by Covert Personal Recording Devices may be shared with other law enforcement agencies who are involved in a joint investigation, or who are conducting their own investigations. Information can also be shared with various prosecutors' offices, including the District Attorney, State Attorney or United States Attorney. Recordings may also be shared with defendants and their attorneys through the discovery process, as established by state and federal law and overseen by the courts.

(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 a Covert Personal Recording Device shall receive appropriate training. Training will include guidance on the use of the devices, interaction with dispatch and patrol operations and a review regarding relevant policies and procedures, including this policy. Training will also address state and federal law related to the use of video surveillance 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.

Covert Personal Recording Devices must be authorized by a police sergeant, lieutenant or other sworn administrator. Use of these devices for criminal investigations is documented in the police report. 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 use of the devices. 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 should be promptly addressed.

Darren Pytel
Police Chief
October 30, 2018

STAFF REPORT

DATE: June 20, 2023

TO: City Council

FROM: Darren Pytel, Police Chief

SUBJECT: Surveillance Technology – 2023 Annual Surveillance Report, Explosive Ordnance Disposal (EOD) Robot

---

Recommendation

1. Receive Annual Surveillance Report regarding the use of the EOD Robot (26.070.060 (a) Davis Municipal Code (DMC)).
2. Hold a public hearing to consider the continued use of the EOD robot (26.070.060 (b) (DMC).
3. Determine the continued use the EOD robot has been balanced with the need to investigate and prevent crimes; protect crime victims and society from those who commit crimes; protect civil rights and civil liberties, including privacy and free expression; and the costs to the City.
4. Approve the continued use of the EOD robot and the existing use policy (Attachment 1).

Fiscal Impact

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

Council Goal(s)

This item is consistent with the Council goal to ensure a safe, healthy, equitable community. It is not tied to a specific task; however, it is part of normal city business activity.

Commission Involvement

This report and accompanying information were sent to the Police Accountability Commission for their April 3, 2023, meeting.

Background and Analysis

The Davis Municipal Code requires a city department that uses surveillance technology to provide an annual written report for each approved item. More specifically,

> ***Section 26.07.060 Oversight following council approval.***
>
> *(a) By the end of each fiscal year, a city department that uses surveillance technology must present a written annual surveillance report at a regular city council meeting for city council review for each approved surveillance technology item. If the city department is unable to meet the deadline, the department head shall notify the city council in writing of staff's request to extend this period, and the reasons for that request. The city council may grant reasonable extensions to comply with this section.*

(b) Based upon information in the annual surveillance report, the city council will, at a regular city council meeting, balance the need to: investigate and prevent crimes; protect crime victims and society from those who commit crimes; protect civil rights and civil liberties, including privacy and free expression; and the costs to the city and will determine whether to continue to allow the use of the surveillance technology item, cease use, or propose modifications to the corresponding Surveillance Use Policy.

At the June 28, 2022, city council meeting approving the continued use of this technology, council directed staff to provide the annual reports to the Police Accountability Commission (PAC) 75 days prior to reporting to the city council. The information in this report covers July 1, 2022, to March 17, 2023, when the reports were completed for the PAC. As this cycle continues in the future, the annual reports will cover April to April each year although council will not be asked to approve the continued use of the technology until June or later each year.

2023 Annual Surveillance Report – EOD Robot

(a)The Annual Surveillance Report will include all of the following:

(1)A general description of how the surveillance technology was used;

The robot was not used in Davis during the reporting period.

(2)A general description of whether and how often data acquired through the use of the surveillance technology item was shared with outside entities, the name of any recipient entity, the type(s) of data disclosed, under what legal standard(s) the information was disclosed, and the justification for the disclosure(s);

No information was shared.

(3)A summary of community complaints or concerns about the surveillance technology item;

No complaints or concerns were submitted to the Police Department.

(4)The results of any internal audits required by the Surveillance Use Policy, any information about violations of the Surveillance Use Policy, and a general description of any actions taken in response;

There were no violations of the Surveillance Use Policy.

(5)Information, including crime statistics, that help the City Council assess whether the surveillance technology has been effective at achieving its identified purposes;

See above.

(6)Statistics and information about any related Public Records Act requests;

There have been no PRA requests regarding this surveillance technology.

(7)Total annual costs for the surveillance technology, including personnel and other ongoing costs, and what source of funding will fund the technology in the coming year;

There are no ongoing costs for the EOD robot. Maintenance is performed during scheduled EOD training time.

(8)Any requested modifications to the Surveillance Use Policy and a detailed basis for the request;

No recommended changes.

(9)Where applicable, a general breakdown of what physical objects the surveillance technology hardware was installed upon, using general descriptive terms; for surveillance technology software, a general breakdown of what data sources the surveillance technology was applied to.

Not Applicable.

(10) A summary of all requests for City Council approval for the use of the surveillance technology item, including whether the City Council approved or rejected the proposal and/or required changes to a proposed Surveillance Use Policy before approval

The City Council previously authorized use of the EOD Robot at the July 31, 2018, city council meeting, the June 18, 2019, city council meeting, the September 22, 2020, city council meeting, the September 21, 2021, city council meeting, and the June 28, 2022, city council meeting. No other requests have been made

The City Council previously authorized use of the EOD equipment at the July 31, 2018, city council meeting[1], the June 18, 2019, city council meeting[2], the September 22, 2020, city council meeting[3], the September 21, 2021, city council meeting[4], and the June 28, 2022, city council meeting[5]. The information from those staff reports is still in effect and should be considered for the request of the continued use of the item.

---

1 https://documents.cityofdavis.org/Media/Default/Documents/PDF/CityCouncil/CouncilMeetings/Agendas/20180731/08D-Surveillance-Tech-Public-Hearing-EOD-Robot.pdf

2 https://documents.cityofdavis.org/Media/Default/Documents/PDF/CityCouncil/CouncilMeetings/Agendas/20190618/08G-Surveillance-Tech-PD-EOD-Robot.pdf

3 https://documents.cityofdavis.org/Media/Default/Documents/PDF/CityCouncil/CouncilMeetings/Agendas/2020/2020-09-22/04-Surveillance-Tech-Reauthorization.pdf

4 https://documents.cityofdavis.org/Media/Default/Documents/PDF/CityCouncil/CouncilMeetings/Agendas/2021/2021-09-21/06-Surveillance-Technology-Renewals.pdf

5 https://documents.cityofdavis.org/Media/Default/Documents/PDF/CityCouncil/CouncilMeetings/Agendas/2022/2022-06-28/06-Surveillance-Technology-Renewals.pdf

Attachments

1. Use Policy – EOD Robot

DAVIS POLICE DEPARTMENT

EOD ROBOT
Policy and Procedure 6.03-B

DEPARTMENT MANUAL

On July 31, 2018, the Davis City Council, in accordance with the Surveillance Technology Ordinance, adopted the following Explosive Ordnance Disposal (EOD) Robot Use Policy (26.07.030 Davis Municipal Code)

Surveillance Use Policy
EOD robot – The equipment consists of a remotely controlled robot, control module, and digital recorder. The EOD robot is equipped with multiple cameras and a microphone to record audio and video during an incident. The equipment was manufactured by Andros and is used throughout the world for EOD operations.

(a) Purpose: The specific purpose(s) that the surveillance technology item is intended to advance.
To safeguard bomb technicians by allowing remote search, diagnostic, and render-safe procedures during EOD and critical incident operations. This equipment is generally used to locate and manipulate known or suspected explosives, explosive and WMD devices, and suspicious packages.

(b) Authorized Use: The uses that are authorized, and the rules and processes required prior to such use.
Those authorized to use the equipment must be members of the YCBS. Those team members are trained how to use the equipment.

(c) Data Collection: The information that can be collected by the surveillance technology, including "open source" data.
The technology records audio and video of the incident. The technology does not utilize "open source" data.

(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.
Any member of the YCBS can access the data during the incident. At the conclusion of the event, the data is stored on a DVD which is booked into evidence at the Davis Police Department.

(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.

Only those YCBS members who are trained to use the equipment can access the data. Once the data is recorded on a DVD, only those members who would normally have access to evidence would be able to access the data.

(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 data is considered evidence. The time period the data would be retained would be dictated by the court process.

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

The general public would not have access to the data. If criminal charges are filed against a person, that person would have access to a copy of the data booked into evidence. The copy of the data is provided to the defendant through their attorney.

(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.

The technology does not use Third Party Data Sharing.

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

Members of the YCBS receive annual training from the manufacturer of this equipment in addition to ongoing regional training received on a monthly basis.

(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.

The technology and the storage of the data is supervised and managed by a Davis Police Department Sergeant and a West Sacramento Police Department Sergeant who are in charge of the YCBS.

Darren Pytel
Police Chief
July 31, 2018

STAFF REPORT

DATE: June 20, 2023

TO: City Council

FROM: Darren Pytel, Police Chief

SUBJECT: Surveillance Technology – 2023 Annual Surveillance Report, GeoTime Computer Program

---

Recommendation

1. Receive Annual Surveillance Report regarding the use of the GeoTime Computer Program (26.070.060 (a) Davis Municipal Code (DMC)).
2. Hold a public hearing to consider the continued use of the GeoTime Computer Program (26.070.060 (b) DMC).
3. Determine the continued use of the GeoTime Computer Program has been balanced with the need to investigate and prevent crimes; protect crime victims and society from those who commit crimes; protect civil rights and civil liberties, including privacy and free expression; and the costs to the City.
4. Approve the continued use of the GeoTime Computer Program and existing use policy (Attachment 1).

Fiscal Impact

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

Council Goal(s)

This item is consistent with the Council goal to ensure a safe, healthy, equitable community. It is not tied to a specific task; however, it is part of normal city business activity.

Commission Involvement

This report and accompanying information were sent to the Police Accountability Commission for their April 3, 2023, meeting.

Background and Analysis

The Davis Municipal Code requires a city department that uses surveillance technology to provide an annual written report for each approved item. More specifically,

> ***Section 26.07.060 Oversight following council approval.***
>
> *(a) By the end of each fiscal year, a city department that uses surveillance technology must present a written annual surveillance report at a regular city council meeting for city council review for each approved surveillance technology item. If the city department is unable to meet the deadline, the department head shall notify the city council in writing of staff's request to extend this period, and the reasons for that request. The city council may grant reasonable extensions to comply with this section.*

(b) Based upon information in the annual surveillance report, the city council will, at a regular city council meeting, balance the need to: investigate and prevent crimes; protect crime victims and society from those who commit crimes; protect civil rights and civil liberties, including privacy and free expression; and the costs to the city and will determine whether to continue to allow the use of the surveillance technology item, cease use, or propose modifications to the corresponding Surveillance Use Policy.

At the June 28, 2022, city council meeting approving the continued use of this technology, council directed staff to provide the annual reports to the Police Accountability Commission (PAC) 75 days prior to reporting to the city council. The information in this report covers July 1, 2022, to March 17, 2023, when the reports were completed for the PAC. As this cycle continues in the future, the annual reports will cover April to April each year although council will not be asked to approve the continued use of the technology until June or later each year.

2023 Annual Surveillance Report – GeoTime Computer Program

(a)The Annual Surveillance Report will include all of the following:

(1)A general description of how the surveillance technology was used;

This technology was not used during this period.

(2)A general description of whether and how often data acquired through the use of the surveillance technology item was shared with outside entities, the name of any recipient entity, the type(s) of data disclosed, under what legal standard(s) the information was disclosed, and the justification for the disclosure(s);

No information was shared.

(3)A summary of community complaints or concerns about the surveillance technology item;

No complaints or concerns were submitted to the Police Department.

(4)The results of any internal audits required by the Surveillance Use Policy, any information about violations of the Surveillance Use Policy, and a general description of any actions taken in response;

There were no violations of the Surveillance Use Policy.

(5)Information, including crime statistics, that help the City Council assess whether the surveillance technology has been effective at achieving its identified purposes;

None not identified in original staff report.

(6)Statistics and information about any related Public Records Act requests;

There have been no PRA requests regarding this surveillance technology.

(7)Total annual costs for the surveillance technology, including personnel and other ongoing costs, and what source of funding will fund the technology in the coming year;

The total annual cost includes a $924/year maintenance fee for the software and negligible personnel costs.

(8)Any requested modifications to the Surveillance Use Policy and a detailed basis for the request;

No recommended changes.

(9)Where applicable, a general breakdown of what physical objects the surveillance technology hardware was installed upon, using general descriptive terms; for surveillance technology software, a general breakdown of what data sources the surveillance technology was applied to.

The software is physically installed on one computer in the Police Department. Access to this computer is restricted by password. The technology used phone records resulting from search warrants and crime event data gathered from the Police Department's records management system.

(10) A summary of all requests for City Council approval for the use of the surveillance technology item, including whether the City Council approved or rejected the proposal and/or required changes to a proposed Surveillance Use Policy before approval

The City Council previously authorized use of the GeoTime Computer Program at the October 30, 2018, city council meeting, the June 18, 2019, city council meeting, the September 22, 2020, city council meeting, the September 21, 2021, city council meeting, and the June 28, 2022, city council meeting. No other requests have been made.

The City Council previously authorized use of the GeoTime Computer Program at the October 30, 2018, city council meeting[1], the June 18, 2019, city council meeting[2], the September 22, 2020, city council meeting[3], the September 21. 2021, city council meeting[4],

1 https://documents.cityofdavis.org/Media/Default/Documents/PDF/CityCouncil/CouncilMeetings/Agendas/20181030/08D-Surveillance-Technology-GeoTime.pdf

2 https://documents.cityofdavis.org/Media/Default/Documents/PDF/CityCouncil/CouncilMeetings/Agendas/20190618/08H-Surveillance-Tech-PD-GeoTime-Program.pdf

3 https://documents.cityofdavis.org/Media/Default/Documents/PDF/CityCouncil/CouncilMeetings/Agendas/2020/2020-09-22/04-Surveillance-Tech-Reauthorization.pdf

4 https://documents.cityofdavis.org/Media/Default/Documents/PDF/CityCouncil/CouncilMeetings/Agendas/2021/2021-09-21/06-Surveillance-Technology-Renewals.pdf

and the June 28, 2022, city council meeting[5]. The information from those staff reports is still in effect and should be considered for the request of the continued use of the item.

Attachments

1. Use Policy – GeoTime Computer Program

[5] https://documents.cityofdavis.org/Media/Default/Documents/PDF/CityCouncil/CouncilMeetings/Agendas/2022/2022-06-28/06-Surveillance-Technology-Renewals.pdf

DAVIS POLICE DEPARTMENT

GeoTime Program USE
Policy and Procedure 6.06-B

DEPARTMENT MANUAL

On October 30, 2018, the Davis City Council, in accordance with the Surveillance Technology Ordinance, adopted the following GeoTime Use Policy (26.07.030 Davis Municipal Code)

Surveillance Use Policy

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

This technology is specifically intended to assist in the investigation of criminal investigations by collating and displaying raw phone call and text detail records on a map and into other analytical products such as charts, PPTs, videos, and timelines.

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

This technology may only be used upon request by a sworn officer to advance or assist in the investigation of a criminal case. Employees assigned to Investigations or Crime Analysis AND who have also received official GeoTime training may use the technology.

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

GeoTime does not independently collect data; however, GeoTime is compatible with open source data using metadata on many different types of open source files.

(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.

Products made using GeoTime (maps, PPTs, timelines, etc.) may only be used or accessed by the requesting department member. If the product has evidentiary value and is therefore included as a supplement to a criminal case in our RMS, the product may be discoverable.

(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.

Products made using GeoTime are generally kept in digital format and are password protected. If a requestor prints materials produced from GeoTime, the requestor is responsible for keeping said materials in a locked location when not in use to prevent unauthorized access.

(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.

Materials produced from GeoTime will be kept as long as necessary and that time period is case specific. At the conclusion of an investigation, should the requestor no longer need the materials, the requestor will shred physical copies and delete any digital copies.

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

This is confidential investigation information and exempt from public disclosure when used for criminal prosecutions. It is available to the prosecutor and defense through the discovery process which is governed by state and federal law and overseen by the courts.

Crime maps are public information and are shared via the web, media, social media and other public forums.

(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.

Extracted data that is not public information is generally only used by the Davis Police Department. Extracted data may be shared with other law enforcement agencies who are involved in a joint criminal investigation, or who are conducting their own criminal investigation. Sharing data requires authorization from command staff. Data can also be shared with various prosecutors' offices, including District Attorney's, State Attorney or United States Attorney, as well as with criminal defendants and their attorneys through the criminal discovery process or as otherwise required by law.

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

Access to information produced by GeoTime is restricted to sworn officers, attorneys and those assigned to Crime Analysis. Employees assigned to Investigations or Crime Analysis AND who have also received official GeoTime training may use the technology.

(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.

The Police Support Services Manager is responsible for overseeing and auditing the use of the technology and to ensure this policy is followed.

The use of the technology is documented in a criminal police report. 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 use of the technology. The review should include an analysis of the cost, benefit and effectiveness of the technology, 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.

Darren Pytel
Police Chief
October 30, 2018

STAFF REPORT

DATE: June 20, 2023

TO: City Council

FROM: Darren Pytel, Police Chief

SUBJECT: Surveillance Technology – 2023 Annual Surveillance Report, Global Positioning System (GPS) Trackers

---

Recommendation

1. Receive Annual Surveillance Report regarding the use of the Global Positioning System (GPS) Trackers (26.070.060 (a) Davis Municipal Code (DMC)).
2. Hold a public hearing to consider the continued use of the GPS Trackers (26.070.060 (b) DMC).
3. Determine the continued use of the GPS Trackers has been balanced with the need to investigate and prevent crimes; protect crime victims and society from those who commit crimes; protect civil rights and civil liberties, including privacy and free expression; and the costs to the City.
4. Approve the continued use of the GPS Trackers and the existing use policy (Attachment 1).

Fiscal Impact

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

Council Goal(s)

This item is consistent with the Council goal to ensure a safe, healthy, equitable community. It is not tied to a specific task; however, it is part of normal city business activity.

Commission Involvement

This report and accompanying information were sent to the Police Accountability Commission for their April 3, 2023, meeting.

Background and Analysis

The Davis Municipal Code requires a city department that uses surveillance technology to provide an annual written report for each approved item. More specifically,

> ***Section 26.07.060 Oversight following council approval.***
>
> *(a) By the end of each fiscal year, a city department that uses surveillance technology must present a written annual surveillance report at a regular city council meeting for city council review for each approved surveillance technology item. If the city department is unable to meet the deadline, the department head shall notify the city council in writing of staff's request to extend this period, and the reasons for that request. The city council may grant reasonable extensions to comply with this section.*

(b) Based upon information in the annual surveillance report, the city council will, at a regular city council meeting, balance the need to: investigate and prevent crimes; protect crime victims and society from those who commit crimes; protect civil rights and civil liberties, including privacy and free expression; and the costs to the city and will determine whether to continue to allow the use of the surveillance technology item, cease use, or propose modifications to the corresponding Surveillance Use Policy.

At the June 28, 2022, city council meeting approving the continued use of this technology, council directed staff to provide the annual reports to the Police Accountability Commission (PAC) 75 days prior to reporting to the city council. The information in this report covers July 1, 2022, to March 17, 2023, when the reports were completed for the PAC. As this cycle continues in the future, the annual reports will cover April to April each year although council will not be asked to approve the continued use of the technology until June or later each year.

2023 Annual Surveillance Report – GPS Trackers

(a)The Annual Surveillance Report will include all of the following:

(1)A general description of how the surveillance technology was used;

Equipment was used 6 times during criminal investigations pursuant to search warrants for various felony crimes.

(2)A general description of whether and how often data acquired through the use of the surveillance technology item was shared with outside entities, the name of any recipient entity, the type(s) of data disclosed, under what legal standard(s) the information was disclosed, and the justification for the disclosure(s);

The information was shared with prosecuting agencies and the courts on search warrant returns.

(3)A summary of community complaints or concerns about the surveillance technology item;

No complaints or concerns were submitted to the Police Department.

(4)The results of any internal audits required by the Surveillance Use Policy, any information about violations of the Surveillance Use Policy, and a general description of any actions taken in response;

There were no violations of the Surveillance Use Policy.

(5)Information, including crime statistics, that help the City Council assess whether the surveillance technology has been effective at achieving its identified purposes;

The use of trackers is still the most efficient and safest way to track vehicles and/or objects for criminal investigations.

(6)Statistics and information about any related Public Records Act requests;

There have been no PRA requests regarding this surveillance technology.

(7)Total annual costs for the surveillance technology, including personnel and other ongoing costs, and what source of funding will fund the technology in the coming year;

One of the trackers was inadvertently located by a person being tracked. The device ended up in a landfill and could not be located. The device will be replaced using existing funds.

(8)Any requested modifications to the Surveillance Use Policy and a detailed basis for the request;

No recommended changes.

(9)Where applicable, a general breakdown of what physical objects the surveillance technology hardware was installed upon, using general descriptive terms; for surveillance technology software, a general breakdown of what data sources the surveillance technology was applied to.

Not Applicable.

(10) A summary of all requests for City Council approval for the use of the surveillance technology item, including whether the City Council approved or rejected the proposal and/or required changes to a proposed Surveillance Use Policy before approval

The City Council previously authorized use of the GPS Trackers *at the October 30, 2018, city council meeting, the June 18, 2019, city council meeting, the September 22, 2020, city council meeting, the September 21, 2021, city council meeting, and the June 28, 2022, city council meeting. No other requests have been made.*

The City Council previously authorized use of the GPS Trackers at the October 30, 2018, city council meeting[1], the June 18, 2019, city council meeting[2], the September 22, 2020, city council meeting[3], the September 21, 2021, city council meeting[4], and the June 28,

1 https://documents.cityofdavis.org/Media/Default/Documents/PDF/CityCouncil/CouncilMeetings/Agendas/20181030/08E-Surveillance-Technology-GPS-Trackers.pdf

2 https://documents.cityofdavis.org/Media/Default/Documents/PDF/CityCouncil/CouncilMeetings/Agendas/20190618/08I-Surveillance-Tech-PD-GPS-Tracker.pdf

3 https://documents.cityofdavis.org/Media/Default/Documents/PDF/CityCouncil/CouncilMeetings/Agendas/2020/2020-09-22/04-Surveillance-Tech-Reauthorization.pdf

4 https://documents.cityofdavis.org/Media/Default/Documents/PDF/CityCouncil/CouncilMeetings/Agendas/2021/2021-09-21/06-Surveillance-Technology-Renewals.pdf

2022, city council meeting[5]. The information from those staff reports is still in effect and should be considered for the request of the continued use of the item.

Attachments

1. Use Policy – GPS Trackers

5 https://documents.cityofdavis.org/Media/Default/Documents/PDF/CityCouncil/CouncilMeetings/Agendas/2022/2022-06-28/06-Surveillance-Technology-Renewals.pdf

DAVIS POLICE DEPARTMENT

GPS TRACKER DEVISE USE
Policy and Procedure 6.07-B

DEPARTMENT MANUAL

On October 30, 2018, the Davis City Council, in accordance with the Surveillance Technology Ordinance, adopted the following GPS Tracker Device Use Policy (26.07.030 Davis Municipal Code)

Surveillance Use Policy

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

Improve public safety by providing an effective method of investigating criminal activity. GPS trackers can be used to track items instead of using human surveillance. This is a cost effective way to investigate crime.

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

GPS tracking devices can be used during criminal investigations and 'bait" type operations. GPS tracking devices will be used by sworn peace officers. Use of the devices must be authorized by a supervisor or manager and a warrant or waiver is required for non-bait surveillance operations.

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

Devices use Global Positioning System (GPS) technology to track the location of the device by longitude and latitude. The information gathered by the device includes geographic location (Latitude/Longitude), time, speed and direction. The information is not open source and is only accessible by the account holder and vendor.

(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 information will 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. The service vendor is bound by strict requirements that they may not share any information collected by the Davis Police Department.

(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.

GPS tracking device accounts require an account administrator be assigned by the agency using their product. The administrator assigned at the Davis PD for administrating GPS tracking device accounts is the Investigations Division Sergeant and/or lieutenant. The

account administrator has the ability to assign "users" who have the ability to change certain settings on the device and make reports, or assign individuals the ability to "view only", which limits access to only logging in and viewing real time data. The account administrator can also assign passwords, change passwords and delete data.

(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.**
Data is attached to criminal investigations. Records related to criminal investigations are kept for statutorily varying periods depending on the type of record, whether a person has been prosecuted and/or whether the record has been lawfully sealed. Records that are no longer needed will be destroyed in accordance with laws relating to the destruction of evidence when it is no longer needed or as required by court order.

Any data that is not attached to a criminal case is deleted.

(g) Public Access: How collected information can be accessed or used by members of the public, including criminal defendants.
All data is for the official use of the Davis Police Department.

Requests for data 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 (it is exempt from public disclosure pursuant to a public records request).

Data that is the subject of a court order or subpoena shall be processed in accordance with the established department subpoena process.

Criminal defendants have access to information pursuant to state and federal laws relating to discovery or as otherwise required by law. Discovery is overseen by the courts.

(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.**
Data is generally only used by the Davis Police Department. However, data may be shared with other law enforcement agencies who are involved in a joint criminal investigation, or who are conducting their own criminal investigation. Sharing data requires authorization from command staff. Data can also be shared with various prosecutors' offices, including District Attorney's, State Attorney or United States Attorney, as well as with criminal defendants and their attorneys through the criminal discovery process or as otherwise required by law.

(i) Training: The training required for any individual authorized to use the surveillance technology or to access information collected by the surveillance technology.
GPS Device users are trained by other officers on how to use the device and obtain the data.

(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.

The use of a device is documented in a criminal police report. These devices are stored at the police department when 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 use of the devices. The review should include an analysis of the cost, benefit and effectiveness of the device, 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.

Darren Pytel
Police Chief
October 30, 2018

STAFF REPORT

DATE: June 20, 2023

TO: City Council

FROM: Darren Pytel, Police Chief

SUBJECT: Surveillance Technology – 2023 Annual Surveillance Report, Automated License Plate Readers (ALPR)

Recommendation

1. Receive Annual Surveillance Report regarding the use of the ALPR system (26.070.060 (a) Davis Municipal Code (DMC)).
2. Hold a public hearing to consider the continued use of the ALPR system (26.070.060 (b) DMC) and California Civil Code § 1798.90.55).
3. Determine the continued use of the ALPR system has been balanced with the need to investigate and prevent crimes; protect crime victims and society from those who commit crimes; protect civil rights and civil liberties, including privacy and free expression; and the costs to the city.
4. Approve the continued use of the ALPR system and the existing use policy (Attachment 1).

Fiscal Impact

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

Council Goal(s)

This item is consistent with the Council goal to ensure a safe, healthy, equitable community. It is not tied to a specific task; however, it is part of normal city business activity.

Commission Involvement

This report and accompanying information were sent to the Police Accountability Commission for their April 3, 2023, meeting.

Background and Analysis

The Davis Municipal Code requires a city department that uses surveillance technology to provide an annual written report for each approved item. More specifically,

> ***Section 26.07.060 Oversight following council approval.***
>
> *(a) By the end of each fiscal year, a city department that uses surveillance technology must present a written annual surveillance report at a regular city council meeting for city council review for each approved surveillance technology item. If the city department is unable to meet the deadline, the department head shall notify the city council in writing of staff's request to extend this period, and the reasons for that request. The city council may grant reasonable extensions to comply with this section.*

(b) Based upon information in the annual surveillance report, the city council will, at a regular city council meeting, balance the need to: investigate and prevent crimes; protect crime victims and society from those who commit crimes; protect civil rights and civil liberties, including privacy and free expression; and the costs to the city and will determine whether to continue to allow the use of the surveillance technology item, cease use, or propose modifications to the corresponding Surveillance Use Policy.

At the June 28, 2022, city council meeting approving the continued use of this technology, council directed staff to provide the annual reports to the Police Accountability Commission (PAC) 75 days prior to reporting to the city council. The information in this report covers July 1, 2022, to March 17, 2023, when the reports were completed for the PAC. As this cycle continues in the future, the annual reports will cover April to April each year although council will not be asked to approve the continued use of the technology until June or later each year.

2023 Annual Surveillance Report – ALPR

(a)The Annual Surveillance Report will include all of the following:

(1)A general description of how the surveillance technology was used;

The system was used for parking enforcement. The ALPR system consists of a high speed camera with an infrared ("IR") filter or two cameras—one high resolution digital camera and one IR camera—to capture images of license plates; a processor and application capable of performing sophisticated optical character recognition (OCR) to transform the image of the plate into alphanumeric characters; and a user interface to display the images captured, the results of the OCR transformation, and an alert capability to notify operators of violations (for timed zone parking enforcement and to determine whether the plate is associated with a parking permit).

(2)A general description of whether and how often data acquired through the use of the surveillance technology item was shared with outside entities, the name of any recipient entity, the type(s) of data disclosed, under what legal standard(s) the information was disclosed, and the justification for the disclosure(s);

None

(3)A summary of community complaints or concerns about the surveillance technology item;

No complaints or concerns were submitted to the Police Department.

(4)The results of any internal audits required by the Surveillance Use Policy, any information about violations of the Surveillance Use Policy, and a general description of any actions taken in response;

There were no violations of the Surveillance Use Policy.

(5)Information, including crime statistics, that help the City Council assess whether the surveillance technology has been effective at achieving its identified purposes;

The ALPR systems are installed on parking enforcement vehicles and used for electronic chalking and e-permit verification. Because parking permits are entirely electronic now, should we no longer us the ALPR the entire permit process would need to revert back to stickers and in-person sales. Federal appeals courts in other circuits around the country have ruled that chalking tires was a violation of the 4th Amendment; however, the 9th Circuit, which covers California, recently ruled there was no 4th Amendment violation in some cases. Therefore, ALPR is currently the best way to conduct timed zone enforcement without using parking meters.

(6)Statistics and information about any related Public Records Act requests;

There have been no PRA requests regarding this surveillance technology.

(7)Total annual costs for the surveillance technology, including personnel and other ongoing costs, and what source of funding will fund the technology in the coming year;

The annual costs can be found with the original staff report with fiscal analysis to acquire and maintain the technology, can be found here: http://documents.cityofdavis.org/Media/Default/Documents/PDF/CityCouncil/CouncilMeetings/Agendas/20160315/06-Parking.pdf

The computers in the parking vehicles were upgraded in 2022; however, that was done as routine replacement using existing replacement accounts. Importantly, the LPR software and cameras are the same so there was no adjustment of the surveillance technology.

(8) Any requested modifications to the Surveillance Use Policy and a detailed basis for the request;

No recommended changes.

(9)Where applicable, a general breakdown of what physical objects the surveillance technology hardware was installed upon, using general descriptive terms; for surveillance technology software, a general breakdown of what data sources the surveillance technology was applied to.

The ALPR systems are installed on parking enforcement vehicles and used for electronic chalking and e-permit verification and data installed on a City server.

(10) A summary of all requests for City Council approval for the use of the surveillance technology item, including whether the City Council approved or rejected the proposal and/or required changes to a proposed Surveillance Use Policy before approval

The City Council previously authorized use of the ALPR system at the July 31, 2018, city council meeting, the June 18, 2019, city council meeting, the September 22, 2020, city council meeting, the September 21, 2022, city council meeting, and the June 28, 2022, city council meeting. The Department proposed adding additional ALPR systems at the March 10, 2020, city council meeting, however, the request was not approved.

The City Council previously authorized use of the ALPR system at the July 31, 2018, city council meeting[1], the June 19, 2019, city council meeting[2] , the September 22, 2020, city council meeting[3], the September 21, 2022, city council meeting[4], and the June 28, 2022, city council meeting[5]. The information from those reports is still in effect and should be considered for the request of the continued use of the item.

Attachments

1. Use Policy – ALPR

[1] https://documents.cityofdavis.org/Media/Default/Documents/PDF/CityCouncil/CouncilMeetings/Agendas/20180731/08A-Surveillance-Tech-Public-Hearing-ALPR.pdf

[2] https://documents.cityofdavis.org/Media/Default/Documents/PDF/CityCouncil/CouncilMeetings/Agendas/20190618/08B-Surveillance-Tech-PD-Automated-License-Plate-Readers.pdf

[3] https://documents.cityofdavis.org/Media/Default/Documents/PDF/CityCouncil/CouncilMeetings/Agendas/2020/2020-09-22/04-Surveillance-Tech-Reauthorization.pdf

[4] https://documents.cityofdavis.org/Media/Default/Documents/PDF/CityCouncil/CouncilMeetings/Agendas/2021/2021-09-21/06-Surveillance-Technology-Renewals.pdf

[5] https://documents.cityofdavis.org/Media/Default/Documents/PDF/CityCouncil/CouncilMeetings/Agendas/2022/2022-06-28/06-Surveillance-Technology-Renewals.pdf

DAVIS POLICE DEPARTMENT

Automated License Plate Readers (ALPR) Policy and Procedure 2.41-A

DEPARTMENT MANUAL

Index as:
ALRP
Automated License Plate Readers (ALPR)
Parking Enforcement, ALPR

On July 31, 2018, the Davis City Council, in accordance with the Surveillance Technology Ordinance, adopted the following ALPR Use Policy (26.07.030 Davis Municipal Code)

I. POLICY

The Davis Police Department uses ALPR as part of comprehensive parking management system, including electronic vehicle chalking to enforce time limit parking restrictions and electronic parking permit management. The purpose of this policy is to provide guidance for the capture, storage and use of digital data obtained through the use of ALPR technology.

The policy of the Davis Police Department is to utilize ALPR technology to capture and store digital license plate data and images while recognizing the established privacy rights of the public. All data and images gathered by the ALPR are for the official use of this department. Because such data may contain confidential information, it is not open to public review.

The Department shall implement specific security measures as agreed to by the Department and T2 Systems, Inc, who has an agreement with Genetec AutoVu, who hosts ALPR technology and data for the Davis Police Department. The Agreement with T2 Systems, Inc. and Genetec AutoVu is specifically incorporated by reference.

The Davis City Council, at a regularly agendized meeting, allowed for public comment regarding the implementation of an ALRP program on March 15, 2016 (Civil Code § 1798.90.55). After receiving public comment, the City Council approved the purchase and use of ALRP technology by unanimous vote.

II. PROCEDURE

A. Management

The Davis Police Department, by and through the Police Chief, is solely responsible for the day-to-day operation and management of the ALPR system and for all tasks ancillary to its operation and management.

The Police Services Specialist Supervisor assigned to the Parking Unit shall be responsible for keeping this policy up to date in order to comply with the requirements of Civil Code §

1798.90.5 et seq. This includes, but is not limited to (Civil Code § 1798.90.51; Civil Code § 1798.90.53):

- A description of the job title or other designation of the members and independent contractors who are authorized to use or access the ALPR system or to collect ALPR information.
- Training requirements for authorized users.
- A description of how the ALPR system will be monitored to ensure the security of the information and compliance with applicable privacy laws.
- Procedures for system operators to maintain records of access in compliance with Civil Code § 1798.90.52.
- The title and name of the current designee in overseeing the ALPR operation.
- Working with the Custodian of Records on the retention and destruction of ALPR data.
- Ensuring this policy and related procedures are conspicuously posted on the department's website.

B. Authorized Access

The following personnel will have regular access to the ALPR system:

- Police Chief
- Police Department Administration
- Parking Supervisor
- Police Services Specialist

The Police Chief may authorize representatives from T2, Inc. (parking management system), Genetec AutoVu (ALPR system) and PCS Mobile (wireless transmission services) to access the ALPR system for parking citation processing, training and maintenance services as provided for in written agreements.

The Police Chief may authorize other city employees to access the ALPR system to study parking patterns as part of a comprehensive parking management plan.

The Police Chief, through his or her designee, shall ensure that the ALPR system is operated in conformity with this Policy and other Department policies, procedures, rules and regulations.

C. Operations

Use of an ALPR is restricted to the purposes outlined below. Department members shall not use, or allow others to use the equipment or database records for any unauthorized purpose (Civil Code § 1798.90.51; Civil Code § 1798.90.53).

1. Installation and Functioning

   ALPR cameras may be mounted on marked parking enforcement vehicles. ALPR equipment will passively read the license plates of parked motor vehicles using ALPR optical character recognition technology. The ALPR data may be used as part of the comprehensive parking management system (electronic vehicle chalking and e-permit management plan). An ALPR may be used in conjunction with any routine patrol operation or criminal investigation. Reasonable suspicion or probable cause is not required before using an ALPR. Data may also be compared against various hot lists

uploaded or created by the Davis Police Department. Scanned data files collected by the system will, on an ongoing basis, be automatically uploaded from the ALPR camera to the ALPR database.

2. Hot Lists

   The Department may utilize hot lists where there is a legitimate and specific law enforcement reason for identifying a vehicle associated with an outstanding arrest warrant, vehicles related to missing persons investigations, vehicles associated with AMBER Alerts, stolen vehicles, vehicles that are reasonably believed to be involved in the commission of a crime, vehicles which are registered to or are reasonably believed to be operated by persons who do not have a valid operator's license or who are on the revoked or suspended list, vehicles with expired registrations, vehicles registered to persons who are subject to a restraining order issued by a court or by the Parole Board, or who are subject to any other duly issued order restricting their movements, vehicles registered to persons wanted by a law enforcement agency who are of interest in a specific investigation, vehicles that have outstanding parking citations, or vehicles registered to persons who are on any watch list issued by a State or Federal agency responsible for homeland security when information has been received concerning a specific individual.

   Designation of hot lists to be utilized by the ALPR system shall be made by the Chief or their designee. Hot lists shall be obtained or compiled from sources as may be consistent with the purposes of the ALPR system set forth in this Policy. These sources may include:

   - NCIC Stolen Vehicle files, as available;
   - NCIC Stolen plates and Stolen Canadian plates, as available;
   - NCIC Wanted persons, as available;
   - NCIC Missing or Endangered person files, as available;
   - NCIC Supervised Release (Federal Probationers), as available;
   - NCIC Nationwide Domestic Violence Protection Orders, as available;
   - NCIC Violent Gang and Terrorist Organization File, as available;
   - NCIC Sexual Offender;
   - DMV Records of Suspended/Revoked Registrations.
   - Parking Citation Data Files

   If practicable, an officer should verify an ALPR response through the California Law Enforcement Telecommunications System (CLETS) before taking enforcement action that is based solely on an ALPR alert.

3. Training - No member of this Department shall operate ALPR equipment or access ALPR data without first completing Department-approved training. Training may be provided by T2, Inc and Genetec AutoVu as part of the services agreement. Follow up training may be provided by the Department.

4. Login/Log-Out Procedure - All ALPR data downloaded to the mobile workstation and in storage shall be accessible only through a login/password-protected system capable of documenting all access of information by name, date and time (Civil Code § 1798.90.52). To ensure proper operation and facilitate oversight of the ALPR system, all users will be required to have individual credentials for access and use of the systems and/or data. A

routine check to ensure the equipment is working properly should be done at the beginning of each shift by the user logging into the system.

5. Auditing and Oversight - To ensure proper oversight into the use of the system and adherence to this policy, all activities (plate detections, queries, reports, etc.) are automatically recorded by the system for auditing purposes. System audits shall be conducted by the Parking Supervisor on a regular basis.

6. Permitted/Impermissible Uses

   An ALPR shall only be used for official law enforcement business. The ALPR system, and all data collected, is the property of the Davis Police Department. Department personnel may only access and use the ALPR system for official and legitimate law enforcement purposes consistent with this Policy. The following uses of the ALPR system are specifically prohibited:

   - Invasion of Privacy: Except when done pursuant to a court order such as a search warrant, it is a violation of this Policy to utilize the ALPR to record license plates except those of vehicles that are exposed to public view (e.g., vehicles on a public road or street, or that are on private property but whose license plate(s) are visible from a public road, street, or a place to which members of the public have access, such as the parking lot of a shop or other business establishment).

   - Harassment or Intimidation: It is a violation of this Policy to use the ALPR system to harass and/or intimidate any individual or group.

   - Personal Use: It is a violation of this Policy to use the ALPR system or associated scan files or hot lists for any personal purpose.

   - Anyone who engages in an impermissible use of the ALPR system or associated scan files or hot lists may be subject to:

     - Criminal prosecution,
     - Civil liability, and/or administrative sanctions, up to and including termination.

7. While an ALPR may be used to canvass license plates around any crime scene, particular consideration should be given to using ALPR-equipped cars to canvass areas around homicides, shootings and other major incidents. Partial license plates reported during major crimes should be entered into the ALPR system in an attempt to identify suspect vehicles.

D. Database Access and Privacy Concerns

The ALPR system shall be restricted to legitimate law enforcement uses for the purpose of furthering legitimate law enforcement goals and enhancing public safety. Such uses and goals include, but are not limited to, parking management, providing information to officers that will assist in on-going criminal investigations, crime prevention, crime detection, the apprehension of wanted persons, ensuring the safety of vulnerable individuals through the recovery of missing and endangered persons, and improving the quality of life in our community through the identification and removal of stolen or unregistered motor vehicles.

1. The ALPR system database and software resides in a data center featuring full redundancy and access controls. The data remains property of the Davis Police Department, and is managed according to this Policy.

2. The ALPR system is governed by the Permitted/Impermissible Uses as outlined in this Policy.

3. No ALPR operator may access department, state or federal data unless otherwise authorized to do so.

4. The ALPR data contains no Personally Identifiable Information (PII) that may be used to connect license plate detection to an individual. It is only with permissible purpose that an investigator may make this connection (using other systems) and this access is already governed by the Federal Driver's Privacy Protection Act (DPPA).

5. All investigative queries into collected ALPR data are logged by user and available for auditing and review by the Department as outlined in this Policy.

6. The ALPR system has a full audit log, which contains the following information

    a. The date and time the information is accessed.
    b. The license plate number or other data elements used to query the ALPR system.
    c. The username of the person who accesses the information, and, as applicable, the organization or entity with whom the person is affiliated.
    d. The purpose for accessing the information.

E. Data Retention

All data and images gathered by an ALPR are for the official use of the Davis Police Department and because such data may contain confidential CLETS information, it is not open to public review, except as part of the parking citation review/appeal process, which viewing is limited to vehicle information regarding the offender and their vehicle. ALPR information gathered and retained by this Department may be used and shared with prosecutors or others only as permitted by law. The sale, sharing, or transfer of ALPR information, except as permitted by law, is prohibited. All ALPR data downloaded to the hosted server will be stored for a period of one-year, and thereafter shall be purged unless it has become, or it is reasonable to believe it will become, evidence in a criminal or civil action or is subject to a lawful action to produce records. In those circumstances, the applicable data should be downloaded from the server onto portable media and booked into evidence.

Darren Pytel
Police Chief
03/16

8/18 – approved by City Council

Rev. 12/17, 05/19

STAFF REPORT

DATE: June 20, 2023

TO: City Council

FROM: Darren Pytel, Police Chief

SUBJECT: Surveillance Technology – 2023 Annual Surveillance Report, Remote Public Safety Cameras

---

Recommendation

1. Receive Annual Surveillance Report regarding the use of the Remote Public Safety Cameras (26.070.060 (a) Davis Municipal Code (DMC)).
2. Hold a public hearing to consider the continued use of Public Safety Cameras (26.070.060 (b) DMC).
3. Determine the continued use of the Public Safety Cameras has been balanced with the need to investigate and prevent crimes; protect crime victims and society from those who commit crimes; protect civil rights and civil liberties, including privacy and free expression; and the costs to the City.
4. Approve the continued use of the Public Safety Cameras and the existing use policy (Attachment 1).

Fiscal Impact

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

Council Goal(s)

This item is consistent with the Council goal to ensure a safe, healthy, equitable community. It is not tied to a specific task; however, it is part of normal city business activity.

Commission Involvement

This report and accompanying information were sent to the Police Accountability Commission for their April 3, 2023, meeting.

Background and Analysis

The Davis Municipal Code requires a city department that uses surveillance technology to provide an annual written report for each approved item. More specifically,

> ***Section 26.07.060 Oversight following council approval.***
>
> *(a) By the end of each fiscal year, a city department that uses surveillance technology must present a written annual surveillance report at a regular city council meeting for city council review for each approved surveillance technology item. If the city department is unable to meet the deadline, the department head shall notify the city council in writing of staff's request to extend this period, and the reasons for that request. The city council may grant reasonable extensions to comply with this section.*

(b) Based upon information in the annual surveillance report, the city council will, at a regular city council meeting, balance the need to: investigate and prevent crimes; protect crime victims and society from those who commit crimes; protect civil rights and civil liberties, including privacy and free expression; and the costs to the city and will determine whether to continue to allow the use of the surveillance technology item, cease use, or propose modifications to the corresponding Surveillance Use Policy.

At the June 28, 2022, city council meeting approving the continued use of this technology, council directed staff to provide the annual reports to the Police Accountability Commission (PAC) 75 days prior to reporting to the city council. The information in this report covers July 1, 2022, to March 17, 2023, when the reports were completed for the PAC. As this cycle continues in the future, the annual reports will cover April to April each year although council will not be asked to approve the continued use of the technology until June or later each year.

2023 Annual Surveillance Report – Remote Public Safety Cameras

(a)The Annual Surveillance Report will include all of the following:

(1)A general description of how the surveillance technology was used;

A portable camera was deployed on City controlled property where there has been a significant amount of vandalism. The fixed cameras are installed at Richards/Olive and Mace/I-80.

(2)A general description of whether and how often data acquired through the use of the surveillance technology item was shared with outside entities, the name of any recipient entity, the type(s) of data disclosed, under what legal standard(s) the information was disclosed, and the justification for the disclosure(s);

Videos from the fixed cameras were used for criminal investigations throughout the year, including information that was used for cases submitted to the District Attorney.

The fixed cameras were used in several criminal investigations, including hit and run cases at In-N-Out Burger, collisions occurring on Mace and Richards and organized retail theft at Target.

A few notable cases in addition to the above:

Assault with Deadly Weapon and Brandishing a firearm. Clearly showed entire incident and was used in the prosecution.

Brandishing a firearm. Clearly showed the entire incident and were able to get suspect info/ vehicle info.

Significant commercial burglary. Used to get clear video of license plates on both suspects vehicles.

Missing person at-risk. Was able to confirm vehicle she left in and direction of travel. This person was later located by officers in a remote area and needed immediate medical care to save her life.

Bank theft. Able to confirm license plates and ID co-conspirators.

(3)A summary of community complaints or concerns about the surveillance technology item;

No complaints or concerns were submitted to the Police Department. The Police Department did present an expanded camera program to the city council in March 2020. Several community members did express concerns regarding the use of cameras.

(4)The results of any internal audits required by the Surveillance Use Policy, any information about violations of the Surveillance Use Policy, and a general description of any actions taken in response;

There were no violations of the Surveillance Use Policy.

(5)Information, including crime statistics, that help the City Council assess whether the surveillance technology has been effective at achieving its identified purposes;

No new information

(6)Statistics and information about any related Public Records Act requests;

There have been no PRA requests regarding this surveillance technology.

(7)Total annual costs for the surveillance technology, including personnel and other ongoing costs, and what source of funding will fund the technology in the coming year;

Very minimal staff cost to deploy.

(8)Any requested modifications to the Surveillance Use Policy and a detailed basis for the request;

No recommended changes.

(9)Where applicable, a general breakdown of what physical objects the surveillance technology hardware was installed upon, using general descriptive terms; for surveillance technology software, a general breakdown of what data sources the surveillance technology was applied to.

Mobile and to existing City poles.

(10) A summary of all requests for City Council approval for the use of the surveillance technology item, including whether the City Council approved or rejected the proposal and/or required changes to a proposed Surveillance Use Policy before approval

The City Council previously authorized use of the Remote Public Safety Cameras at the October 30, 2018, city council meeting, the June 18, 2019, council meeting, the September 22, 2020, city council meeting, the September 21, 2021, city council meeting, and the June 28, 2022, city council meeting. The City Council approved additional fixed cameras at the March 10, 2020, city council meeting.

The City Council previously authorized use of the Remote Public Safety Cameras at the October 30, 2018, city council meeting[1], the June 18, 2019, city council meeting[2], the March 10, 2020, city council meeting[3], the September 22, 2020, city council meeting[4], the September 21, 2022, city council meeting[5], and the June 28, 2022, city council meeting[6]. The information from those staff reports is still in effect and should be considered for the request of the continued use of the item.

Attachments

1. Use Policy – Remote Public Safety Cameras

---

1 https://documents.cityofdavis.org/Media/Default/Documents/PDF/CityCouncil/CouncilMeetings/Agendas/20181030/08F-Surveillance-Technology-Public-Safety-Cameras.pdf

2 https://documents.cityofdavis.org/Media/Default/Documents/PDF/CityCouncil/CouncilMeetings/Agendas/20190618/08L-Surveillance-Tech-PD-Public-Safety-Camera.pdf

3 https://documents.cityofdavis.org/Media/Default/Documents/PDF/CityCouncil/CouncilMeetings/Agendas/2020/2020-03-10/04B-Remote-Public-Safety-Cameras-LPR-Surveillance-Tech.pdf

4 https://documents.cityofdavis.org/Media/Default/Documents/PDF/CityCouncil/CouncilMeetings/Agendas/2020/2020-09-22/04-Surveillance-Tech-Reauthorization.pdf

5 https://documents.cityofdavis.org/Media/Default/Documents/PDF/CityCouncil/CouncilMeetings/Agendas/2021/2021-09-21/06-Surveillance-Technology-Renewals.pdf

6 https://documents.cityofdavis.org/Media/Default/Documents/PDF/CityCouncil/CouncilMeetings/Agendas/2022/2022-06-28/06-Surveillance-Technology-Renewals.pdf

DAVIS POLICE DEPARTMENT

PUBLIC SAFETY CAMERA USE
Policy and Procedure 6.08-B

DEPARTMENT MANUAL

On October 30, 2018, the Davis City Council, in accordance with the Surveillance Technology Ordinance, adopted the following Remote Public Safety Cameras Use Policy (26.07.030 Davis Municipal Code). Fixed cameras were approved by the Davis City Council in 2020.

Surveillance Use Policy

(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. The Davis City Council also authorized fixed cameras at Richards Blvd & I-80 and Mace & I-80.

(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.

In those cases where the video is part of a criminal or civil investigation/litigation, the video must be kept for a period of at least two years or until it is no longer needed for litigation.

The Police Chief may destroy recordings of routine video monitoring after one year.

Routine video monitoring may also be destroyed after 90 days if a written log is kept of the recording.

Most video falls within the 90 day retention period meaning that only a written log of what was recorded is kept. In those cases where the video has something of evidentiary value, it will be kept for at least 2 years or until any litigation has been resolved.

(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.

Criminal defendants have access to information pursuant to state and federal laws relating to discovery. Discovery is overseen by the courts.

(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 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 will 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 will 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 a 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.

Darren Pytel
Police Chief
October 30, 2018
Revised May 2022 for fixed cameras.

STAFF REPORT

DATE: June 20, 2023

TO: City Council

FROM: Darren Pytel, Police Chief

SUBJECT: Surveillance Technology – 2023 Annual Surveillance Report, Trail Cameras

---

Recommendation

1. Receive Annual Surveillance Report regarding the use of the Trail Cameras (26.070.060 (a) Davis Municipal Code (DMC)).
2. Hold a public hearing to consider the continued use of Trail Cameras (26.070.060 (b) DMC).
3. Determine the continued use of the Trail Cameras has been balanced with the need to investigate and prevent crimes; protect crime victims and society from those who commit crimes; protect civil rights and civil liberties, including privacy and free expression; and the costs to the City.
4. Approve the continued use of the Trail Cameras and the existing use policy (Attachment 1).

Fiscal Impact

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

Council Goal(s)

This item is consistent with the Council goal to ensure a safe, healthy, equitable community. It is not tied to a specific task; however, it is part of normal city business activity.

Commission Involvement

This report and accompanying information were sent to the Police Accountability Commission for their April 3, 2023, meeting.

Background and Analysis

The Davis Municipal Code requires a city department that uses surveillance technology to provide an annual written report for each approved item. More specifically,

> ***Section 26.07.060 Oversight following council approval.***
>
> *(a) By the end of each fiscal year, a city department that uses surveillance technology must present a written annual surveillance report at a regular city council meeting for city council review for each approved surveillance technology item. If the city department is unable to meet the deadline, the department head shall notify the city council in writing of staff's request to extend this period, and the reasons for that request. The city council may grant reasonable extensions to comply with this section.*

(b) Based upon information in the annual surveillance report, the city council will, at a regular city council meeting, balance the need to: investigate and prevent crimes; protect crime victims and society from those who commit crimes; protect civil rights and civil liberties, including privacy and free expression; and the costs to the city and will determine whether to continue to allow the use of the surveillance technology item, cease use, or propose modifications to the corresponding Surveillance Use Policy.

At the June 28, 2022, city council meeting approving the continued use of this technology, council directed staff to provide the annual reports to the Police Accountability Commission (PAC) 75 days prior to reporting to the city council. The information in this report covers July 1, 2022, to March 17, 2023, when the reports were completed for the PAC. As this cycle continues in the future, the annual reports will cover April to April each year although council will not be asked to approve the continued use of the technology until June or later each year.

2023 Annual Surveillance Report – Trail Cameras

(a)The Annual Surveillance Report will include all of the following:

(1)A general description of how the surveillance technology was used;

A Trail Camera was deployed for a short period of time at a location where significant vandalism was occurring.

(2)A general description of whether and how often data acquired through the use of the surveillance technology item was shared with outside entities, the name of any recipient entity, the type(s) of data disclosed, under what legal standard(s) the information was disclosed, and the justification for the disclosure(s);

No information was shared.

(3)A summary of community complaints or concerns about the surveillance technology item;

No complaints or concerns were submitted to the Police Department.

(4)The results of any internal audits required by the Surveillance Use Policy, any information about violations of the Surveillance Use Policy, and a general description of any actions taken in response;

There were no violations of the Surveillance Use Policy.

(5)Information, including crime statistics, that help the City Council assess whether the surveillance technology has been effective at achieving its identified purposes;

The equipment was used at a particular location that was repeatedly vandalized. It was effective as an investigative tool. The crimes stopped.

(6)Statistics and information about any related Public Records Act requests;

There have been no PRA requests regarding this surveillance technology.

(7)Total annual costs for the surveillance technology, including personnel and other ongoing costs, and what source of funding will fund the technology in the coming year;

No additional costs nor are any anticipated.

(8)Any requested modifications to the Surveillance Use Policy and a detailed basis for the request;

No recommended changes.

(9)Where applicable, a general breakdown of what physical objects the surveillance technology hardware was installed upon, using general descriptive terms; for surveillance technology software, a general breakdown of what data sources the surveillance technology was applied to.

On a City pole.

(10) A summary of all requests for City Council approval for the use of the surveillance technology item, including whether the City Council approved or rejected the proposal and/or required changes to a proposed Surveillance Use Policy before approval

The City Council previously authorized use of the Trail Cameras at the October 30, 2018, city council meeting, the June 18, 2019, city council meeting, the September 22, 2020, city council meeting, the September 21, 2022, city council meeting, and the June 28, 2022, city council meeting. No other requests have been made.

The City Council previously authorized use of the Trail Cameras at the October 30, 2018, city council meeting[1], the June 18, 2019, city council meeting[2], the September 22, 2020, city council meeting[3], the September 21, 2022, city council meeting[4], and the June 28, 2022, city council meeting[5]. The information from those staff reports is still in effect and should be considered for the request of the continued use of the item.

---

1 https://documents.cityofdavis.org/Media/Default/Documents/PDF/CityCouncil/CouncilMeetings/Agendas/20181030/08H-Surveillance-Technology-Trail-Cameras.pdf

2 https://documents.cityofdavis.org/Media/Default/Documents/PDF/CityCouncil/CouncilMeetings/Agendas/20190618/08M-Surveillance-Tech-PD-Trail-Camera.pdf

3 https://documents.cityofdavis.org/Media/Default/Documents/PDF/CityCouncil/CouncilMeetings/Agendas/2020/2020-09-22/04-Surveillance-Tech-Reauthorization.pdf

4 https://documents.cityofdavis.org/Media/Default/Documents/PDF/CityCouncil/CouncilMeetings/Agendas/2021/2021-09-21/06-Surveillance-Technology-Renewals.pdf

5 https://documents.cityofdavis.org/Media/Default/Documents/PDF/CityCouncil/CouncilMeetings/Agendas/2022/2022-06-28/06-Surveillance-Technology-Renewals.pdf

Attachments

1. Use Policy – Trail Cameras

DAVIS POLICE DEPARTMENT

TRAIL CAMERA USE
Policy and Procedure 6.09-B

DEPARTMENT MANUAL

On October 30, 2018, the Davis City Council, in accordance with the Surveillance Technology Ordinance, adopted the following Trail Camera Use Policy (26.07.030 Davis Municipal Code)

Surveillance Use Policy

(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.

Trail cameras will be used at fixed locations to monitor ongoing criminal activity such as graffiti, theft or other crimes. The cameras will be used by sworn police officers and authorized for use by a supervisor.

Trail cameras are used only in areas where reasonable suspicion exists that criminal activity is occurring or may occur. Trail cameras do not surreptitiously capture or monitor conversations, and only capture images when activated by a motion sensor trigger.

Trail cameras will not intentionally be used to invade the privacy of individuals or observe areas where a reasonable expectation of privacy exists.

Trail cameras 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.

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

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

Trail cameras are located temporarily in areas where criminal activity is suspected in order to capture images of potential suspects. The cameras capture still images, or very short video when the camera is triggered. The cameras are generally left in an area and the camera is triggered by movement. The images or video is not open source data.

(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.

Although the trail cameras are not password protected, if information gathered is retained for a criminal investigation, the SD cards containing the images or video are stored as evidence.

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.

In those cases where the video is part of a criminal or civil investigation/litigation, the video must be kept for a period of at least two years or until it is no longer needed for litigation.

The Police Chief may destroy recordings of routine video monitoring after one-year.

Routine video monitoring may also be destroyed after 90 days if a written log is kept of the recording.

Most video falls within the 90 day retention period meaning that only a written log of what the recording was is kept. In those cases where the video has something of evidentiary value, it will be kept for at least 2 years or until any litigation has been resolved.

(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.

Criminal defendants have access to information pursuant to state and federal laws relating to discovery. Discovery is overseen by the courts.

(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 cameras may be shared with other law enforcement agencies who are involved in a joint investigation, or who are conducting their own investigations. Images can also be shared with various prosecutors' offices, including the District Attorney, 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 will 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 will 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.

Cameras must be authorized by a police sergeant, lieutenant or other sworn administrator. Use of these cameras for criminal investigations is documented in a 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 trail cameras. 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.

Darren Pytel
Police Chief
October 30, 2018

STAFF REPORT

DATE: June 20, 2023

TO: City Council

FROM: Jason Best, IT Director

SUBJECT: Surveillance Technology – 2023 Annual Surveillance Report for the 1st and F Street Parking Garage Security Cameras

---

Recommendation

1. Receive Annual Surveillance Report regarding the use of the 1st and F Street Parking Garage Security Cameras (26.070.060 (a) Davis Municipal Code (DMC)).
2. Hold a public hearing to consider the continued use of the cameras (26.070.060 (b) DMC).
3. Make a determination that the continued use of the cameras has been balanced with the need to investigate and prevent crimes; protect crime victims and society from those who commit crimes; protect civil rights and civil liberties, including privacy and free expression; and the costs to the city.
4. Approve the continued use of the Security Cameras at the 1st and F Street Parking Garage and the Attached existing use policy.

Fiscal Impact

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

Council Goal(s)

This item is consistent with the Council goal to ensure a safe, healthy, equitable community. It is not tied to a specific task; however, it is part of normal city business activity.

Commission Involvement

Review of the Surveillance Technology is standard operating procedure, with the City Council providing direct authority for approval.

Background and Analysis

The Davis Municipal Code requires a city department that uses surveillance technology to provide an annual written report for each approved item. More specifically,

> ***Section 26.07.060 Oversight following council approval.***
>
> *(a) By the end of each fiscal year, a city department that uses surveillance technology must present a written annual surveillance report at a regular city council meeting for city council review for each approved surveillance technology item. If the city department is unable to meet the deadline, the department head shall notify the city council in writing of staff's request to extend this period, and the reasons for that request. The city council may grant reasonable extensions to comply with this section.*

(b) Based upon information in the annual surveillance report, the city council will, at a regular city council meeting, balance the need to: investigate and prevent crimes; protect crime victims and society from those who commit crimes; protect civil rights and civil liberties, including privacy and free expression; and the costs to the city and will determine whether to continue to allow the use of the surveillance technology item, cease use, or propose modifications to the corresponding Surveillance Use Policy.

2023 Annual Surveillance Report – the 1st and F Street Parking Garage Camera System

The Annual Surveillance Report will include all of the following:

(1)A general description of how the surveillance technology was used;

The camera equipment was used to investigate building and vehicle damage.

(2)A general description of whether and how often data acquired through the use of the surveillance technology item was shared with outside entities, the name of any recipient entity, the type(s) of data disclosed, under what legal standard(s) the information was disclosed, and the justification for the disclosure(s);

No information was shared.

(3)A summary of community complaints or concerns about the surveillance technology item;

No complaints or concerns were submitted to the city.

(4)The results of any internal audits required by the Surveillance Use Policy, any information about violations of the Surveillance Use Policy, and a general description of any actions taken in response;

There were no violations of the Surveillance Use Policy.

(5)Information, including crime statistics, that help the City Council assess whether the surveillance technology has been effective at achieving its identified purposes;

This equipment was used 5 times to determine cause on property damage.

(6)Statistics and information about any related Public Records Act requests;

One PRA request for property damage without a police report.

(7)Total annual costs for the surveillance technology, including personnel and other ongoing costs, and what source of funding will fund the technology in the coming year;

Ongoing costs are about $4,500 for storage and equipment damage.

(8)Any requested modifications to the Surveillance Use Policy and a detailed basis for the request;

None

(9)Where applicable, a general breakdown of what physical objects the surveillance technology hardware was installed upon, using general descriptive terms; for surveillance technology software, a general breakdown of what data sources the surveillance technology was applied to.

Not Applicable.

(10) A summary of all requests for City Council approval for the use of the surveillance technology item, including whether the City Council approved or rejected the proposal and/or required changes to a proposed Surveillance Use Policy before approval

The City Council previously authorized use of the cameras at the November 1, 2022, city council meeting[1]. The information from that staff reports is still in effect and should be considered for the request of the continued use of the item.

Attachments

1. Use Policy

Attachment 1

1st and F STREET CAMERA USE

[1] https://documents.cityofdavis.org/Media/Default/Documents/PDF/CityCouncil/CouncilMeetings/Agendas/2022/2022-11-01/05A2-Surveillance-Tech-Authorization-B-1st%20and%20F-Cameras.pdf

Surveillance Use Policy

On November 1, 2022, the Davis City Council, in accordance with the Surveillance Technology Ordinance, adopted the following the 1st and F Street Parking Garage Camera Use Policy (26.07.030 Davis Municipal Code)

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.

Cameras are used for security and deterrence at the 1st and F Street Parking Garage site. This site has had a history of break-ins and vandalism.

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

Cameras will be used to monitor city property to both deter criminal activity and aid in the apprehension of criminal offenders, when necessary.

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

The system collects video footage. There is no open-source data.

(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.

Information Services staff are the only staff that have access. Management and the police department are given access if footage is used for criminal investigations or site concerns.

(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.

All downloaded and retained media shall be accessed, maintained, stored and retrieved in a manner that ensures its integrity as secured information, including strict adherence to confidentiality 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 1st and F street server is set to over write data every 30 days. The data will exist for another 90 days on encrypted backup. 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 at the police department 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 City of Davis. Requests for recorded video images from the public or the media shall be processed in the same manner as requests for city 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 city subpoena process. Criminal defendants have access to information pursuant to state and federal laws relating to discovery. Discovery is overseen by the courts.

(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 cameras may be shared with the police department, and other law enforcement agencies who are involved in a joint investigation, or who are conducting their own investigations where the images may show criminal activity. Images can also 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 used as criminal evidence. Images may be shared with Risk Management and any attorneys working on the city's behalf. These are protected as work product, but may be shared and protected pursuant to lawful process.

(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 cameras or use the system shall receive appropriate training. Training should include guidance on the use of cameras, interaction with the Police Department regarding how images can be used for criminal investigations 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.
The use of cameras must be authorized by the City Manager's office. Use of these cameras for criminal investigations is documented in police reports. A staff member is subject to discipline for unauthorized use or misuse of any camera system, which is in direct violation of the provisions of this policy.

The Police Department will conduct an annual review of the 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 Department and other applicable advisory bodies. Any recommendations for training or policy will be promptly addressed.

STAFF REPORT

DATE: June 20, 2023

TO: City Council

FROM: Jason Best, IT Director

SUBJECT: Surveillance Technology – 2023 Annual Surveillance Report for the 1818 Fifth St. Corporation Yard Security Cameras

---

Recommendation

1. Receive Annual Surveillance Report regarding the use of the 1818 5th St. Corporation Yard Security Cameras (26.070.060 (a) Davis Municipal Code (DMC)).
2. Hold a public hearing to consider the continued use of the cameras (26.070.060 (b) DMC).
3. Make a determination that the continued use of the cameras has been balanced with the need to investigate and prevent crimes; protect crime victims and society from those who commit crimes; protect civil rights and civil liberties, including privacy and free expression; and the costs to the city.
4. Approve the continued use of the Security Cameras at 1818 5th St. and the Attached existing use policy.

Fiscal Impact

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

Council Goal(s)

This item is consistent with the Council goal to ensure a safe, healthy, equitable community. It is not tied to a specific task; however, it is part of normal city business activity.

Commission Involvement

Review of the Surveillance Technology is standard operating procedure, with the City Council providing direct authority for approval.

Background and Analysis

The Davis Municipal Code requires a city department that uses surveillance technology to provide an annual written report for each approved item. More specifically,

> ***Section 26.07.060 Oversight following council approval.***
>
> *(a) By the end of each fiscal year, a city department that uses surveillance technology must present a written annual surveillance report at a regular city council meeting for city council review for each approved surveillance technology item. If the city department is unable to meet the deadline, the department head shall notify the city council in writing of staff's request to extend this period, and the reasons for that request. The city council may grant reasonable extensions to comply with this section.*

(b) Based upon information in the annual surveillance report, the city council will, at a regular city council meeting, balance the need to: investigate and prevent crimes; protect crime victims and society from those who commit crimes; protect civil rights and civil liberties, including privacy and free expression; and the costs to the city and will determine whether to continue to allow the use of the surveillance technology item, cease use, or propose modifications to the corresponding Surveillance Use Policy.

2023 Annual Surveillance Report – 1818 5th St. Corp Yard Camera System

The Annual Surveillance Report will include all of the following:

(1)A general description of how the surveillance technology was used;

The camera equipment was used to investigate missing items, building/vehicle damage and monitor the front door for deliveries and employee access.

(2)A general description of whether and how often data acquired through the use of the surveillance technology item was shared with outside entities, the name of any recipient entity, the type(s) of data disclosed, under what legal standard(s) the information was disclosed, and the justification for the disclosure(s);

No information was shared.

(3)A summary of community complaints or concerns about the surveillance technology item;

No complaints or concerns were submitted to the city.

(4)The results of any internal audits required by the Surveillance Use Policy, any information about violations of the Surveillance Use Policy, and a general description of any actions taken in response;

There were no violations of the Surveillance Use Policy.

(5)Information, including crime statistics, that help the City Council assess whether the surveillance technology has been effective at achieving its identified purposes;

This equipment was used 14 times to determine cause on property damage, locate missing equipment and staff training.

(6)Statistics and information about any related Public Records Act requests;

No PRA requests regarding 1818 5th St. Corporation Yard Security Cameras.

(7)Total annual costs for the surveillance technology, including personnel and other ongoing costs, and what source of funding will fund the technology in the coming year;

Ongoing costs are about $3,500 for storage and backup.

(8)Any requested modifications to the Surveillance Use Policy and a detailed basis for the request;

None

(9)Where applicable, a general breakdown of what physical objects the surveillance technology hardware was installed upon, using general descriptive terms; for surveillance technology software, a general breakdown of what data sources the surveillance technology was applied to;

Not Applicable.

(10) A summary of all requests for City Council approval for the use of the surveillance technology item, including whether the City Council approved or rejected the proposal and/or required changes to a proposed Surveillance Use Policy before approval;

The City Council previously authorized use of the cameras at the July 31, 2018, city council meeting[1]. The information from that staff reports is still in effect and should be considered for the request of the continued use of the item.

Attachments

1. Use Policy

[1] https://documents.cityofdavis.org/Media/Default/Documents/PDF/CityCouncil/CouncilMeetings/Agendas/20180731/04Q-Surveillance-Tech-Corp-Yard-Cameras.pdf

Attachment 1

1818 5th STREET CAMERA USE
Surveillance Use Policy

On October 30, 2018, the Davis City Council, in accordance with the Surveillance Technology Ordinance, adopted the following 1818 5th Street Camera Use Policy (26.07.030 Davis Municipal Code)

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.
Cameras are used for security and deterrence at the 1818 Corporation Yard site. This site has had a history of break-ins and vandalism.

(b) Authorized Use: The uses that are authorized, and the rules and processes required prior to such use.
Cameras will be used to monitor city property to both deter criminal activity and aid in the apprehension of criminal offenders, when necessary.

(c) Data Collection: The information that can be collected by the surveillance technology, including "open source" data.
The system collects video footage. There is no open source data.

(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.
Information Services staff are the only staff that have access. Management and the police department are given access if footage is used for criminal investigations or site concerns.

(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.
All downloaded and retained media shall be accessed, maintained, stored and retrieved in a manner that ensures its integrity as secured information, including strict adherence to confidentiality 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 1818 Corporation Yard server is set to over write data every 30 days. The data will exist for another 90 days on encrypted backup. 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 at the police department 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 City of Davis. Requests for recorded video images from the public or the media shall be processed in the same manner as requests for city 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 city subpoena process. Criminal defendants have access to information pursuant to state and federal laws relating to discovery. Discovery is overseen by the courts.

(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 cameras may be shared with the police department, and other law enforcement agencies who are involved in a joint investigation, or who are conducting their own investigations where the images may show criminal activity. Images can also 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 used as criminal evidence. Images may be shared with Risk Management and any attorneys working on the city's behalf. These are protected as work product, but may be shared and protected pursuant to lawful process.

(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 cameras or use the system shall receive appropriate training. Training should include guidance on the use of cameras, interaction with the Police Department regarding how images can be used for criminal investigations 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.
The use of cameras must be authorized by the City Manager's office. Use of these cameras for criminal investigations is documented in police reports. A staff member is subject to discipline for unauthorized use or misuse of any camera system, which is in direct violation of the provisions of this policy.

The IS department will conduct an annual review of the 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 IS Department and other applicable advisory bodies. Any recommendations for training or policy will be promptly addressed.

Jason Best
October 2018

STAFF REPORT

DATE: June 20, 2023

TO: City Council

FROM: Deanne Machado, Parks & Community Services Director
Tamiko Kwak, Parks & Community Services Assistant Director

SUBJECT: Surveillance Technology – 2023 Annual Surveillance Report, Davis Community Transit Camera System

---

Recommendation

1. Receive Annual Surveillance Report regarding the use of the Davis Community Transit (DCT) camera system (26.070.060 (a) Davis Municipal Code (DMC)).
2. Hold a public hearing to consider the continued use of the cameras (26.070.060 (b) DMC).
3. Make a determination that the continued use of the cameras has been balanced with the need to investigate and prevent crimes; protect crime victims and society from those who commit crimes; protect civil rights and civil liberties, including privacy and free expression; and the costs to the city.
4. Approve the continued use of the cameras and the existing use policy (Attachment 1).

Fiscal Impact

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

Council Goal(s)

This item is consistent with the Council goal to ensure a safe, healthy, equitable community. It is not tied to a specific task; however, it is part of normal city business activity.

Commission Involvement

Review of the Surveillance Technology is standard operating procedure, with the City Council providing direct authority for approval.

Background and Analysis

The Davis Municipal Code requires a city department that uses surveillance technology to provide an annual written report for each approved item. More specifically,

Section 26.07.060 Oversight following council approval.

(a) By the end of each fiscal year, a city department that uses surveillance technology must present a written annual surveillance report at a regular city council meeting for city council review for each approved surveillance technology item. If the city department is unable to meet the deadline, the department head shall notify the city council in writing of staff's request to extend this period, and the reasons for that request. The city council may grant reasonable extensions to comply with this section.

(b) Based upon information in the annual surveillance report, the city council will, at a regular city council meeting, balance the need to: investigate and prevent crimes; protect crime victims and society from those who commit crimes; protect civil rights and civil liberties, including privacy and free expression; and the costs to the city and will determine whether to continue to allow the use of the surveillance technology item, cease use, or propose modifications to the corresponding Surveillance Use Policy.

2023 Annual Surveillance Report – Davis Community Transit Camera System

The Annual Surveillance Report will include all of the following:

(1) A general description of how the surveillance technology was used;

The cameras have been operational in fiscal year 2022-2023. Footage for this fiscal year was reviewed one time on:

February 22, 2023 - follow up on customer complaint. Additional follow up provided to customer regarding number of bag/items allowed on the bus. No further action needed.

(2) A general description of whether and how often data acquired through the use of the surveillance technology item was shared with outside entities, the name of any recipient entity, the type(s) of data disclosed, under what legal standard(s) the information was disclosed, and the justification for the disclosure(s);

No information was shared.

(3) A summary of community complaints or concerns about the surveillance technology item;

No customer complaints or concerns about the surveillance technology were reported in FY 2022-23.

(4) The results of any internal audits required by the Surveillance Use Policy, any information about violations of the Surveillance Use Policy, and a general description of any actions taken in response;

There were no violations of the Surveillance Use Policy.

(5) Information, including crime statistics, that help the City Council assess whether the surveillance technology has been effective at achieving its identified purposes;

No information gathered.

(6) Statistics and information about any related Public Records Act requests;

No PRA requests regarding DCT surveillance technology.

(7) Total annual costs for the surveillance technology, including personnel and other ongoing costs, and what source of funding will fund the technology in the coming year;

Very minimal staff cost, equipment costs are included in the original purchase agreement of the vehicle and built into the future vehicle replacement funds.

(8) Any requested modifications to the Surveillance Use Policy and a detailed basis for the request;

None

(9) Where applicable, a general breakdown of what physical objects the surveillance technology hardware was installed upon, using general descriptive terms; for surveillance technology software, a general breakdown of what data sources the surveillance technology was applied to.

The surveillance technology is wired in all the DCT vehicles. The hard drive is removable with key access. The technology software is through REI video management software (VMS).

(10) A summary of all requests for City Council approval for the use of the surveillance technology item, including whether the City Council approved or rejected the proposal and/or required changes to a proposed Surveillance Use Policy before approval

The City Council previously authorized use of the video component of the DCT Camera Systems at the June 18, 2019, city council meeting. The information is still in effect and should be considered for the request of the continued use of the surveillance technology.

The City Council previously authorized use of the cameras at the June 18, 2019, city council meeting[1]. The information is still in effect and should be considered for the request of the continued use of the item.

Attachments

1. Use Policy – DCT cameras

[1] https://documents.cityofdavis.org/Media/Default/Documents/PDF/CityCouncil/CouncilMeetings/Agendas/20190618/06X-Surveillance-Tech-PCS-Davis-Community-Transit-Audio-Video-Recording.pdf

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 ensure the safety and security of passengers, drivers and community members on the road.

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

The equipment use is authorized to record audio/video footage internally and externally of the vehicle while in operation. The equipment would be accessed only when there is a documented incident or accident. The Paratransit Supervisor and those trained to use the equipment would be authorized to access the equipment.

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

The system collects video/audio footage. There is no open source data.

(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.

Davis Community Transit Coordinator and Supervisor staff are the only staff that have access. Management and the Police Department are given access if footage is used for criminal investigations or risk/liability insurance claims or site concerns.

(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.

All downloaded and retained media shall be accessed, maintained, stored and retrieved in a manner that ensures its integrity as secured information, including strict adherence to confidentiality 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.

Transit industry standard is to maintain files for one week and then write over data unless there is 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 at the Police Department 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 City of Davis. Requests for recorded video images from the public or the media shall be processed in the same manner as requests for city 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 city 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 cameras may be shared with the Police Department, and other law enforcement agencies who are involved in a joint investigation, or who are conducting their own investigations where the images may show criminal activity. Images can also 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 used as criminal evidence.

Images may be shared with Risk Management and any attorneys working on the city's behalf. These are protected as work product, but may be shared and protected pursuant to lawful process.

(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 cameras or use the system shall receive appropriate training. Training should include guidance on the use of cameras, interaction with the Police Department regarding how images can be used for criminal investigations 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.

The use of cameras must be authorized by the City Manager's office. Use of these cameras for criminal investigations is documented in police reports. A staff member is subject to discipline for unauthorized use or misuse of any camera system, which is in direct violation of the provisions of this policy.

The PCS Department will conduct an annual review of the DCT 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 PCS Department and other applicable advisory bodies. Any recommendations for training or policy will be promptly addressed.

STAFF REPORT

DATE: June 20, 2023

TO: City Council

FROM: Stan Gryczko, Director - Public Works Utilities & Operations

SUBJECT: Surveillance Technology: 2022-23 Annual Surveillance Report, Wildlife Trail Cameras

---

Recommendation

1. Receive Annual Surveillance Report regarding the use of the Wildlife Trail Cameras (26.070.060 (a) Davis Municipal Code (DMC)).
2. Hold a public hearing to consider the continued use of Wildlife Trail Cameras (26.070.060 (b) Davis Municipal Code (DMC)).
3. Make a determination that the continued use of the Wildlife Trail Cameras has been balanced with the need to: investigate and prevent crimes; protect crime victims and society from those who commit crimes; protect civil rights and civil liberties, including privacy and free expression; and the costs to the city, and further that the use of the Wildlife Trail Cameras is solely to remotely observe wildlife behavior for research, conservation, and management purposes.
4. Approve the continued use of the Wildlife Trail Cameras and the existing use policy (Attachment 1).

Fiscal Impact

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

Council Goal

Goal 1 - Ensure a Safe, Healthy, Equitable Community.

Background and Analysis

The Davis Municipal Code requires a city department that uses surveillance technology to provide an annual written report for each approved item. The following annual surveillance report is for the Wildlife Trail Cameras.

> ***Section 26.07.060 Oversight following council approval.***
>
> *(a) By the end of each fiscal year, a city department that uses surveillance technology must present a written annual surveillance report at a regular city council meeting for city council review for each approved surveillance technology item. If the city department is unable to meet the deadline, the department head shall notify the city council in writing of staff's request to extend this period, and the reasons for that request. The city council may grant reasonable extensions to comply with this section.*
>
> *(b) Based upon information in the annual surveillance report, the city council will, at a regular city council meeting, balance the need to: investigate and prevent crimes;*

protect crime victims and society from those who commit crimes; protect civil rights and civil liberties, including privacy and free expression; and the costs to the city and will determine whether to continue to allow the use of the surveillance technology item, cease use, or propose modifications to the corresponding Surveillance Use Policy.

FY 2022-23 Annual Surveillance Report – Wildlife Trail Cameras

(1)A general description of how the surveillance technology was used;

- *A wildlife trail camera (1) was deployed from April 10 to April 21, 2023 at the North Davis Meadows Agricultural Buffer to monitor activity at an American kestrel nest box.*
- *A wildlife trail camera (2) was deployed in the Cannery Agricultural Buffer from April 21 to May 15, 2023 to monitor the effectiveness of ground squirrel control equipment.*

(2)A general description of whether and how often data acquired through the use of the surveillance technology item was shared with outside entities, the name of any recipient entity, the type(s) of data disclosed, under what legal standard(s) the information was disclosed, and the justification for the disclosure(s);

- *No information was shared with outside agencies for this surveillance technology.*

(3)A summary of community complaints or concerns about the surveillance technology item;

- *No complaints or concerns were submitted to the Police Department or Public Works Utilities & Operations Department for this surveillance technology.*

(4)The results of any internal audits required by the Surveillance Use Policy, any information about violations of the Surveillance Use Policy, and a general description of any actions taken in response;

- *There were no violations of the Surveillance Use Policy.*

(5)Information, including crime statistics, that help the City Council assess whether the surveillance technology has been effective at achieving its identified purposes;

- *Data collected from camera 1 helped verify use of the kestrel box by non-native European starlings. This nest was removed to make the box available to target species.*
- *Data collected from camera 2 confirmed that the ground squirrel control equipment was functioning, but generally ineffective.*

(6)Statistics and information about any related Public Records Act requests;

- *There have been no PRA requests regarding this surveillance technology.*

(7)Total annual costs for the surveillance technology, including personnel and other ongoing costs, and what source of funding will fund the technology in the coming year;

- *Wildlife Trail Cameras- Costs to deploy the wildlife trail camera and analyze collected data totaled approximately $500 (labor and materials) during this review period. Future costs will continue to be funded via the Urban Wildlife Program within Public Works Utilities & Operations.*

(8)Any requested modifications to the Surveillance Use Policy and a detailed basis for the request;

- *No changes are requested for this surveillance technology.*

(9) Where applicable, a general breakdown of what physical objects the surveillance technology hardware was installed upon, using general descriptive terms; for surveillance technology software, a general breakdown of what data sources the surveillance technology was applied to.
   - *Wildlife trail camera 1 was affixed to the base of an oak tree within the agricultural buffer. The camera was pointed toward the kestrel nest box.*
   - *Camera 2 was affixed to the base of an olive tree pointing toward the rodent control equipment.*
   - *Photo files from this camera deployment were downloaded from the camera onto a city laptop for analysis using Microsoft photo viewing software.*
   - *Photos were deleted after viewing.*

(10) A summary of all requests for City Council approval for the use of the surveillance technology item, including whether the City Council approved or rejected the proposal and/or required changes to a proposed Surveillance Use Policy before approval
   - *The City Council previously re-authorized use of the Wildlife Trail Cameras at the following meetings:*
     - *June 28, 2022*
     - *September 21, 2021*
   - *City Council previously approved a modification that changed record destruction authority from "Director of Public Works" to "Director of Public Works Utilities & Operations" at their June 18, 2019 meeting.*
   - *No other requests have been made.*

The City Council authorized use of the Wildlife Trail Cameras at their October 30, 2018 meeting. The existing use policy approved at the meeting is included in the linked staff report (beginning on page 5)[1]. The information is still in effect and should be considered for the request of the continued use of the items.

Attachments

1. Staff Report & Use Policy - Wildlife Trail Cameras

[1] http://documents.cityofdavis.org/Media/Default/Documents/PDF/CityCouncil/CouncilMeetings/Agendas/20180828/05J-2-Surveillance-Tech-Info-Wildlife-Trail-Cameras.pdf

STAFF REPORT

DATE: June 20, 2023

TO: City Council

FROM: Stan Gryczko, Director - Public Works Utilities & Operations

SUBJECT: Surveillance Technology: 2022-23 Annual Surveillance Report, Wildlife Video Cameras

---

Recommendation

1. Receive Annual Surveillance Report regarding the use of the Wildlife Video Cameras (26.070.060 (a) Davis Municipal Code (DMC)).
2. Hold a public hearing to consider the continued use of Wildlife Video Cameras (26.070.060 (b) Davis Municipal Code (DMC)).
3. Make a determination that the continued use of the Wildlife Video Cameras has been balanced with the need to: investigate and prevent crimes; protect crime victims and society from those who commit crimes; protect civil rights and civil liberties, including privacy and free expression; and the costs to the city, and further that the use of the Wildlife Cameras is solely to remotely observe wildlife behavior for research, conservation, and management purposes.
4. Approve the continued use of the Wildlife Video Cameras and the existing use policy (Attachment 1).

Fiscal Impact

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

Council Goal

Goal 1 - Ensure a Safe, Healthy, Equitable Community.

Background and Analysis

The Davis Municipal Code requires a city department that uses surveillance technology to provide an annual written report for each approved item. The following annual surveillance report is for the Wildlife Video Cameras.

> ***Section 26.07.060 Oversight following council approval.***
>
> *(a) By the end of each fiscal year, a city department that uses surveillance technology must present a written annual surveillance report at a regular city council meeting for city council review for each approved surveillance technology item. If the city department is unable to meet the deadline, the department head shall notify the city council in writing of staff's request to extend this period, and the reasons for that request. The city council may grant reasonable extensions to comply with this section.*
>
> *(b) Based upon information in the annual surveillance report, the city council will, at a regular city council meeting, balance the need to: investigate and prevent crimes;*

protect crime victims and society from those who commit crimes; protect civil rights and civil liberties, including privacy and free expression; and the costs to the city and will determine whether to continue to allow the use of the surveillance technology item, cease use, or propose modifications to the corresponding Surveillance Use Policy.

FY 2022-23 Annual Surveillance Report – Wildlife Video Cameras

(1)A general description of how the surveillance technology was used;

- *Wildlife video equipment was not used during this review period.*

(2)A general description of whether and how often data acquired through the use of the surveillance technology item was shared with outside entities, the name of any recipient entity, the type(s) of data disclosed, under what legal standard(s) the information was disclosed, and the justification for the disclosure(s);

- *No information was shared for this surveillance technology.*

(3)A summary of community complaints or concerns about the surveillance technology item;

- *No complaints or concerns were submitted to the Police Department or Public Works Utilities & Operations for this surveillance technology.*

(4)The results of any internal audits required by the Surveillance Use Policy, any information about violations of the Surveillance Use Policy, and a general description of any actions taken in response;

- *There were no violations of the Surveillance Use Policy.*

(5)Information, including crime statistics, that help the City Council assess whether the surveillance technology has been effective at achieving its identified purposes;

- *Wildlife video equipment was not used during this review period.*

(6)Statistics and information about any related Public Records Act requests;

- *There have been no PRA requests regarding this surveillance technology.*

(7)Total annual costs for the surveillance technology, including personnel and other ongoing costs, and what source of funding will fund the technology in the coming year;

- *There were no costs associated with the use of wildlife video cameras during this review period.*

(8)Any requested modifications to the Surveillance Use Policy and a detailed basis for the request;

- *No changes are requested for this surveillance technology.*

(9)Where applicable, a general breakdown of what physical objects the surveillance technology hardware was installed upon, using general descriptive terms; for surveillance technology software, a general breakdown of what data sources the surveillance technology was applied to.

- *Wildlife video equipment was not used during this review period.*

(10) A summary of all requests for City Council approval for the use of the surveillance technology item, including whether the City Council approved or rejected the proposal and/or required changes to a proposed Surveillance Use Policy before approval

- *The City Council previously re-authorized use of the Wildlife Video Cameras at the following meetings:*
  - *June 28, 2022*
  - *September 21, 2021*
- *The City Council previously approved a modification that changed record destruction authority from "Director of Public Works" to "Director of Public Works Utilities & Operations" at their June 18, 2019 meeting.*
- *No other requests have been made.*

The City Council authorized use of the Wildlife Video Cameras at their October 30, 2018 meeting. The existing use policy approved at the meeting is included in the linked staff report (beginning on page 5)[1]. The information is still in effect and should be considered for the request of the continued use of the items.

Attachments

1. Staff Report & Use Policy - Wildlife Video Cameras

[1] http://documents.cityofdavis.org/Media/Default/Documents/PDF/CityCouncil/CouncilMeetings/Agendas/20181030/08J-Surveillance-Technology-Wildlife-Video-Cameras.pdf

STAFF REPORT

DATE: June 20, 2023

TO: City Council

FROM: Stan Gryczko, Director - Public Works Utilities & Operations

SUBJECT: Surveillance Technology: 2022-23 Annual Surveillance Report, Public Works Security Cameras

---

Recommendation

1. Receive Annual Surveillance Report regarding the use of the Public Works Security Cameras (26.070.060 (a) Davis Municipal Code (DMC)).
2. Hold a public hearing to consider the continued use of Public Works Security Cameras (26.070.060 (b) Davis Municipal Code (DMC)).
3. Make a determination that the continued use of the Public Works Security Cameras has been balanced with the need to: investigate and prevent crimes; protect crime victims and society from those who commit crimes; protect civil rights and civil liberties, including privacy and free expression; and the costs to the city.
4. Approve the continued use of the Public Works Security Cameras and the existing use policy (Attachment 1).

Fiscal Impact

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

Council Goal

Goal 1 - Ensure a Safe, Healthy, Equitable Community.

Background and Analysis

The Davis Municipal Code requires a city department that uses surveillance technology to provide an annual written report for each approved item. The following annual surveillance report is for the Public Works Security Cameras.

> ***Section 26.07.060 Oversight following council approval.***
>
> *(a) By the end of each fiscal year, a city department that uses surveillance technology must present a written annual surveillance report at a regular city council meeting for city council review for each approved surveillance technology item. If the city department is unable to meet the deadline, the department head shall notify the city council in writing of staff's request to extend this period, and the reasons for that request. The city council may grant reasonable extensions to comply with this section.*
>
> *(b) Based upon information in the annual surveillance report, the City Council will, at a regular City Council meeting, balance the need to: investigate and prevent crimes; protect crime victims and society from those who commit crimes; protect civil rights and civil liberties, including privacy and free expression; and the costs to the city and will*

determine whether to continue to allow the use of the surveillance technology item, cease use, or propose modifications to the corresponding Surveillance Use Policy.

FY 2022-23 Annual Surveillance Report – Public Works Security Cameras

(1)A general description of how the surveillance technology was used; The technology was used for Public Works, which include corporation yard, water wells, water tanks and pump stations, wastewater lift stations, and stormwater pump stations DVRs and cameras;

- *We are restoring remote view functionality by replacing old cameras and making network upgrade. We are adding local storage to the sites. We are coordinating all our surveillance systems work through the IS department. The equipment is used to monitor critical infrastructure and locations with chemical / fuel storage.*

(2)A general description of whether and how often data acquired through the use of the surveillance technology item was shared with outside entities, the name of any recipient entity, the type(s) of data disclosed, under what legal standard(s) the information was disclosed, and the justification for the disclosure(s);

- *No information was shared with these surveillance technologies.*

(3)A summary of community complaints or concerns about the surveillance technology item;

- *No complaints or concerns were submitted to the Police Department or Public Works Utilities & Operations for this surveillance technology.*

(4)The results of any internal audits required by the Surveillance Use Policy, any information about violations of the Surveillance Use Policy, and a general description of any actions taken in response;

- *There were no violations of the Surveillance Use Policy.*

(5)Information, including crime statistics, that help the City Council assess whether the surveillance technology has been effective at achieving its identified purposes;

- *Wells, Tanks, Pumps and Lift Station Cameras - We are replacing equipment to restore prior functionality.*

(6)Statistics and information about any related Public Records Act requests;

- *There have been no PRA requests regarding this surveillance technology.*

(7)Total annual costs for the surveillance technology, including personnel and other ongoing costs, and what source of funding will fund the technology in the coming year;

- *Wells, Tanks, Pumps and Lift Station Cameras – Replacement of old non-functional equipment is being funded from the annual operations and maintenance budget.*
- *Funding for each site is based on the enterprise fund supporting the infrastructure being monitored. No additional budget is necessary for these improvements.*

(8)Any requested modifications to the Surveillance Use Policy and a detailed basis for the request;

- *No changes requested.*

(9)Where applicable, a general breakdown of what physical objects the surveillance technology hardware was installed upon, using general descriptive terms; for surveillance technology

software, a general breakdown of what data sources the surveillance technology was applied to.

- *Wells, Tanks, Pumps and Lift Station Cameras - City light standards on city sites. Areas outside the site were a person could be identified are masked.*
- *Yard Cameras – City light standards etc. and the Corp yard site.*

(10) A summary of all requests for City Council approval for the use of the surveillance technology item, including whether the City Council approved or rejected the proposal and/or required changes to a proposed Surveillance Use Policy before approval

- *The City Council previously re-authorized use of the Public Works Video Cameras at the following meetings:*
  - *June 28, 2022*
  - *September 21, 2021*
- *The City Council previously approved a modification that changed record destruction authority from "Director of Public Works" to "Director of Public Works Utilities & Operations" at their June 18, 2019 meeting.*
- *No other requests have been made.*

The City Council authorized use of the Public Works Cameras at their October 30, 2018 meeting. The existing use policy approved at the meeting is included in the linked staff report (beginning on page 5)[1]. The information is still in effect and should be considered for the request of the continued use of the items.

Attachments

1. Staff Report & Use Policy – Public Works Corporation Yard Cameras

[1] https://documents.cityofdavis.org/Media/Default/Documents/PDF/CityCouncil/CouncilMeetings/Agendas/20181030/08G-Surveillance-Technology-PW-Security-Cameras.pdf