**STAFF REPORT**

**DATE:** July 10, 2018

**TO:** City Council

**FROM:** Darren Pytel

**SUBJECT:** Surveillance Technology - Cellebrite Universal Forensic Extraction Device

---

**Recommendation**

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

**Fiscal Impact**

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

**Council Goal(s)**

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

**Background and Analysis**

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

**Surveillance Impact Report**

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

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

The CUFED is a forensic tool used to extract data from mobile phones, smartphones, and personal digital assistants (PDA's). The device itself is not surveillance technology. It simply extracts data from a device. However, because personal data is extracted the use of the device raises constitutional privacy concerns that have been addressed by the United States Supreme Court (use requires search warrant, consent or exigent circumstances).

**(b) If applicable, the location(s) it may be deployed and crime statistics for any location(s);**
The CUFED is used at the police department. Personal technology devices such as smart phones are commonly used to commit crime and are commonly carried by those who commit crimes. These devices contain significant investigative data.

**(c) An assessment identifying any potential impact on civil liberties and civil rights and discussing any plans to safeguard the rights of the public;**
Forensic extractions require a search warrant, written owner consent or exigent circumstances. The devices are commonly used by law enforcement agencies around the world. As with any other forensic device, extracted data must be carefully safeguarded to avoid releasing private information.

**(d) The fiscal costs for the surveillance technology, including initial purchase, personnel and other ongoing costs, and any current or potential sources of funding;**
Initial Purchase Cost
$3,326.40 (already purchased)

Personnel Costs
Operator Certification - $850 – $2,000 (Cost ranges depend on software certification)

Ongoing Costs
None

Potential Sources of Funding
Regular Department Operating Budget

**(e) Whether use or maintenance of the technology will require data gathered by the technology to be handled or stored by a third-party vendor on an ongoing basis;**
Extracted data is stored locally on a police server, or a removable drive. Data reports can be produced in hardcopy form or burned to DVD. There is no third party storage of data.

**(f) A summary of the experience, if any, other governmental entities have had with the proposed technology, including information about the effectiveness, any known adverse information about the technology such as unanticipated costs, failures, civil rights or civil liberties abuses.**
The CUFED is a common tool for extracting data from cell phones, smart phones of PDA's. The device is effective in most cases. In order to extract data from devices, officers must have a search warrant or written consent.

**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.**

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.

**(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 personnel who are trained in its use and with approval of command staff.

**(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 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 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.**
Information gathered as part of a criminal investigation will become evidence and retained as part of the court process.

**(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.

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

**(h) Third Party Data Sharing: If and how other City or non-City entities can access or use the information, including any required justification or legal standard necessary to do so and any obligations imposed on the recipient of the information.**
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 investigation, or who are conducting their own 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 defense attorneys through the discovery process.

**(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.