Will Tetsell, City Auditor
Internal Audit Department
350 South 5th Street, Suite 302
Minneapolis, MN 55415-1316
(612) 673-2056

July 23, 2015

Mayor Betsy Hodges, City Council Members and Police Chief Janeé Harteau,

Attached is the City of Minneapolis Internal Audit Department's memorandum of the Police Body Camera Program Consultation. The objective of this consultation, which was requested by the Minneapolis Police Department (MPD), was to collaborate with MPD to identify and understand the considerations involved in the undertaking of a Police Body Camera Program so as to proactively address considerations prior to implementation and execution. The scope of this consultation included program governance and administration, the two brands of body cameras tested in the MPD pilot, and the public data request process for body camera video. A consultation is an advisory service that is agreed upon with the customer and is intended to improve risk management, governance and controls without the auditor assuming management responsibility. As this is a consultation, we typically do not formally follow up on the recommendations included in the report; nevertheless, we will make ourselves available to assist the Police Department as they address the recommendations within the report and other items that may arise.

It is clear that the Pilot Program that evaluated the two brands of body cameras and related applications and storage solutions was well planned and executed, and that configuration and implementation considerations were carefully evaluated. We did not note any material recommendations within the operation of the MPD Pilot Program itself.

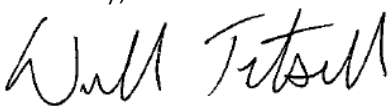
The consultation found that many aspects involved in implementing a police body camera program were considered and either fully- or partially-addressed in the pilot phase. Internal Audit discovered additional considerations that should be addressed to help the City more effectively manage the implementation and execution of the Police Body Camera Program.

During this consultation, Internal Audit was concurrently conducting an audit of the City's Data Governance and Records Information processes, which align and overlap with the Police Body Camera Program. In conducting that work, some items for consideration that relate to the goals and objectives of the Police Body Camera Program came up that we would like to bring to your attention, as well as the attention of decision-makers and stakeholders.

In staying aligned with some of the objectives of the body camera program; enhancing transparency and accountability, the City should evaluate the teams and processes in place to support the redaction, review and distribution of the body camera video footage. Although the front end of the body camera program (capturing,

annotating and storing video data) has been well vetted and tested, we noted that the public disclosure processes are highly manual and require various levels of review, which could impact how efficiently and effectively the Police Records Information Unit is able to keep up with demand while maintaining strong privacy controls. An evaluation of the Police Records Information Unit process should be conducted to validate the ability of the process to adequately manage public video requests, to redact video for private or confidential information, and to timely provide internal and external users a convenient means of viewing the requested video. Since forecasting demand for body camera video is difficult, an extensible process should be established to accommodate various levels of demand.

Sincerely,



Will Tetsell, City Auditor

Internal Audit Department
350 South 5th Street, Suite 302
Minneapolis, MN 55415-1316
(612) 673-2056

Audit Team on the Engagement:
Tim Homstad, Manager, Backbone Consultants
Matt Lagieski, Internal Audit Associate
Will Tetsell, Director Internal Audit

Date: July 23, 2015

To: Mayor Betsy Hodges, City Council Members and Police Chief Janeé Harteau

Re: Police Body Camera Consultation Memorandum

Background

Police departments across the nation have implemented body cameras to help improve police transparency and accountability. In addition, the camera footage could protect officers by providing evidence of false and unsubstantiated claims by the public. The Minneapolis Police Department (MPD) is evaluating the implementation of police body cameras into their police force.

A pilot program that evaluated two products, Taser and VIEVU, began on November 7, 2014. The program was led by the City's MPD Business Technology Unit. The Taser solution tested was a cloud-based offering hosted on Amazon's AWS cloud service. The VIEVU solution tested was a locally-stored offering. The test included three Minneapolis precincts representing different racial and socioeconomic demographics. Each precinct included 12 volunteer officers conducting tests in the field. Evaluation of the two products was concentrated on product review and policy validation. Product review included functional operation of the cameras and infrastructure needed for collecting, transferring, storing and releasing data. Policy evaluation was comprised of two components. First, the functionality and compliance of the policy and its related standard operating procedures provided to the officers for operation of cameras in the field, as well as administrative documentation associated with data collection. The second component was associated with redacting, releasing and distributing data.

Procedures included within the police body camera process included:

- Program governance
- Capturing and transferring video
- Categorizing video
- Annotating video
- Transferring video
- Storing video
- Redacting video
- Releasing video

Scope
Internal Audit conducted an evaluation of the processes and technology used in the implementation and management of the Police Body Camera Pilot Program. This evaluation also included program governance, capturing and transferring video, categorizing, annotating and retaining video, and releasing video appropriately. This document will outline the considerations identified based on the MPD Body Camera Program, and recommendations of controls.

Out of Scope
Internal Audit was not involved in vendor selection, requirements gathering, service level agreements, budgets, or selection of cloud versus local storage solutions for the products evaluated during the pilot program. Operational procedures related to police body camera usage, technical testing of security, including but not limited to, vulnerability and penetration testing of the devices, applications or docking stations were not tested during the consultation.

Approach
The assessment approach consisted of independently assessing operational and technical controls, policies and procedures for governance, security and administration, and specific controls for both Taser and VIEVU products, the two vendors selected for evaluation in the pilot program. Information was collected through interviews, observations, and examination of documentation with MPD Business Technology Unit, collaboration with the City Attorney's Office, Police Crime Lab, Information Technology, other City of Minneapolis departments, and industry best practices.

Detailed Summary

Overview of the Taser products
Taser was the first product tested by the City of Minneapolis. The Taser cameras came in two varieties, a chest worn device called the Axon Body, and a smaller camera capable of being worn on the shoulder or sunglasses called the Axon Flex. Both devices offered the same security and controls, and used the same software.

Functionality of both devices was very similar. Recording was started by the officers double tapping a button on the device. This device was constantly recording and retained the previous 30 seconds of footage once an officer double taps the activation button. Upon completion of the officers' shifts, they docked the device in the Taser docking station that would both upload the videos and charge the devices.

Devices would be assigned to each officer and they were required to use only their device. Taser's software solution leveraged software as a service, utilizing Amazon.com's AWS cloud infrastructure and Taser's Evidence.com software. Since Taser's solution was a cloud-hosted platform, all captured videos must be uploaded via the internet.

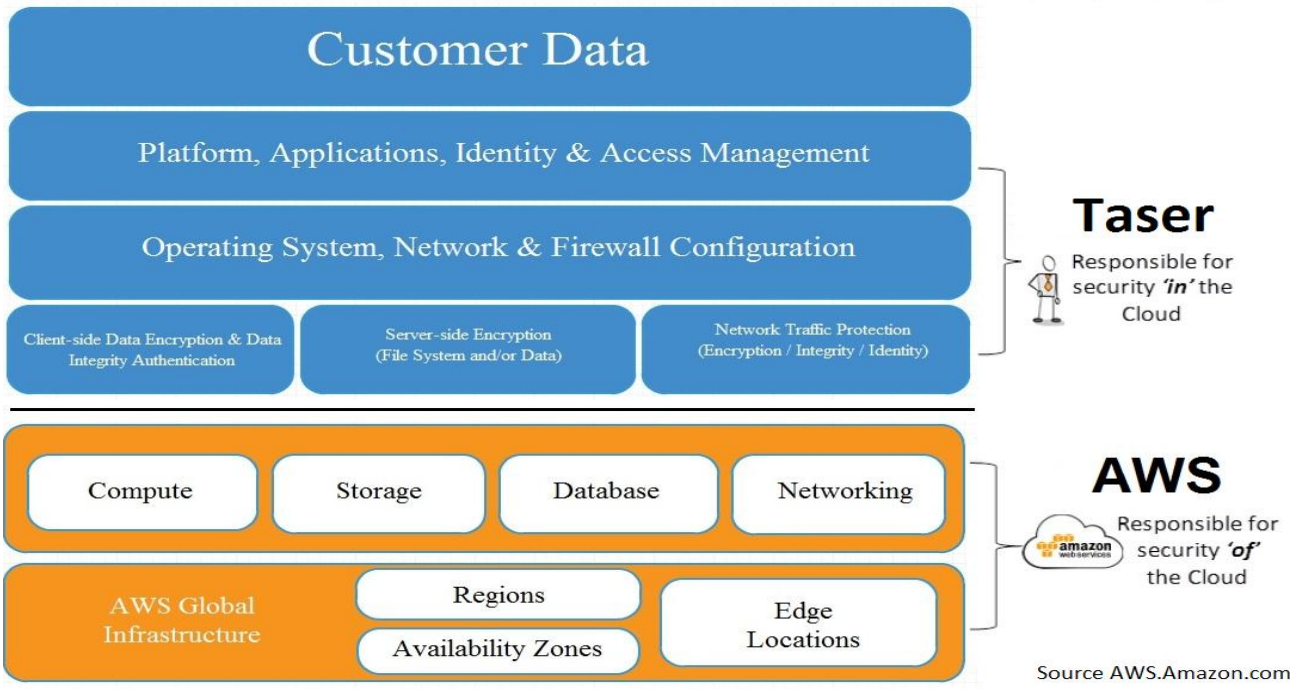
Ernst & Young, a public accounting firm, validated infrastructure controls, security and availability principles for Amazon's AWS platform through a SOC2 report. No review was done on Privacy and Confidentiality principles. Internal Audit was unable to validate the effectiveness of the control environment in place for Evidence.com, as a public report on their control environment was not available at the time of the review. Without the ability to validate the controls in place in the cloud solution, it is unknown how logging at the operating system or virtual machine level is captured, who has access to bypass application controls, or if chain of custody controls could be compromised.

The software used to interact with footage was web based. Users login to Evidence.com to access and manage recorded video. Evidence.com required local administration of the configuration and user provisioning, and granted external parties the ability to view footage. Since the application was hosted externally, users did not need an application (client) installed on their computer to access footage. This could be useful for court litigations and public requests, as a link to a specific video could be used to provide access to view the video, it could however, allow circumvention of redaction and review controls if this functionality is not controlled.

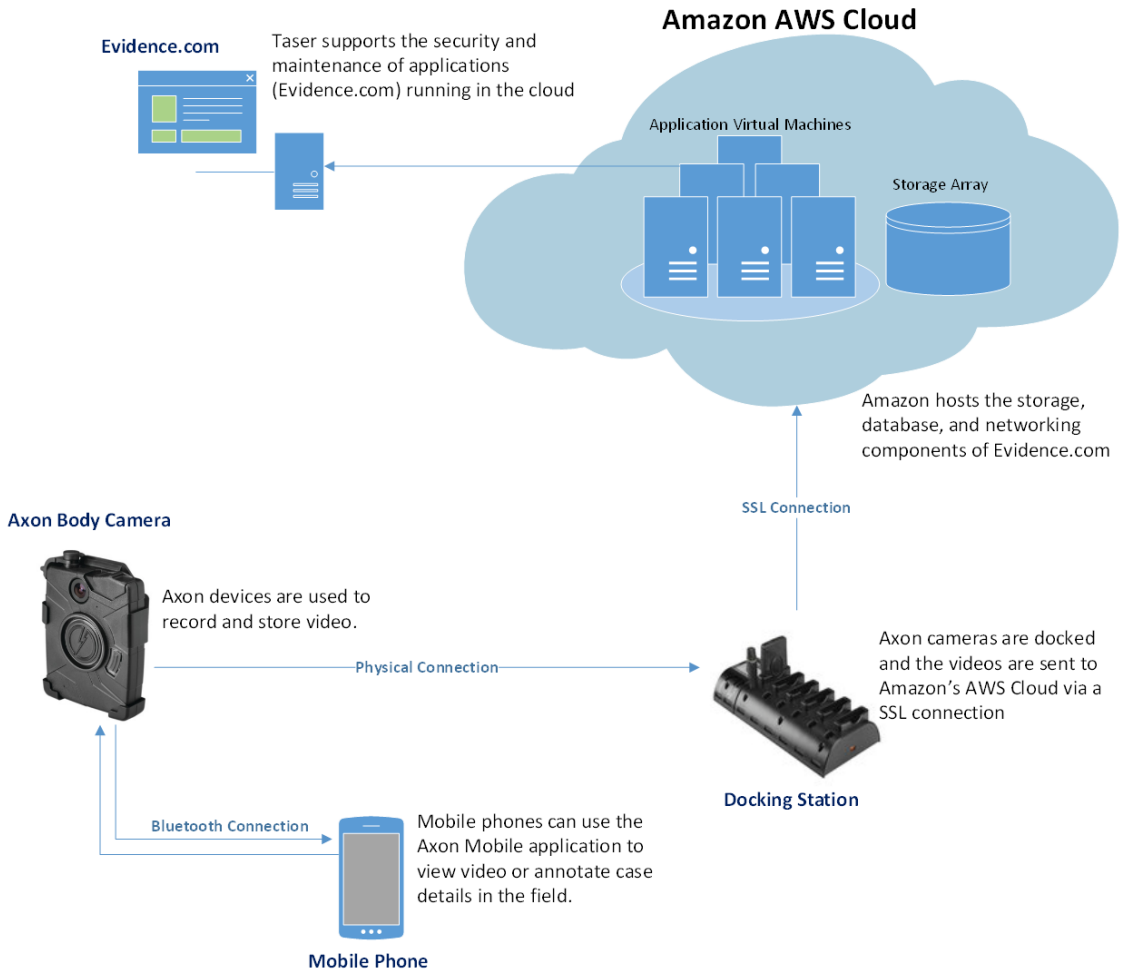
Once videos had been uploaded to Evidence.com, officers were expected to edit the text fields to add details (e.g., case number, category type, etc.) on the video. Completing the text fields in Evidence.com ties footage of incidents to specific case numbers for tracking purposes, and proper classification will trigger record retention durations based on the type of incident that was recorded. Taser cameras also offered Bluetooth connectivity to iOS and Android devices, which allowed officers to annotate videos in the field.

Responsibilities within Amazon's cloud

This graphic illustrates the responsibilities of each third-party in Taser's Cloud Storage solution.



Flow of information for Taser cloud solution



Overview of the VIEVU product

The second body camera tested by the City of Minneapolis was a chest mounted camera from VIEVU. This camera was activated by sliding a cover down to expose the camera lens. This device would start recording once the lens has been exposed; it does not capture previous footage like the Taser solution. At the end of the shift, officers must plug the cameras into laptops via a USB cable to upload the footage and charge the device.

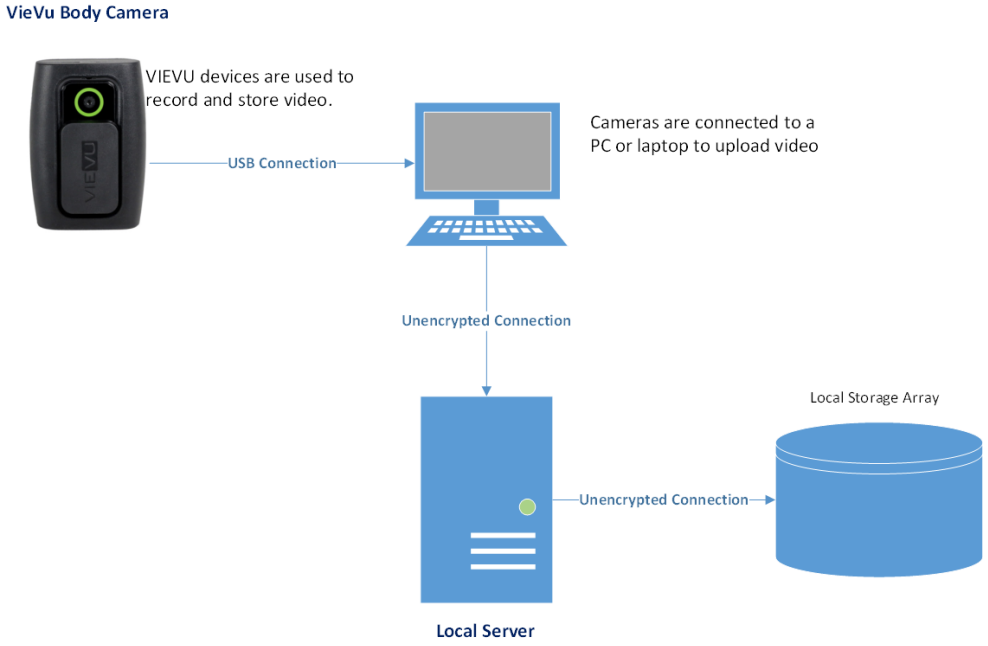
VIEVU offered two software hosting and application options at the time of the pilot program. The first was a local hosted solution where local infrastructure was used to store video files and a client application is used to view footage. The local offering required dedicated storage, redundancy and backup solutions to be in place and managed by the City's IT staff. The second solution was cloud-based storage through an application that leverages Microsoft's Azure cloud network. Local storage was the only option tested during the VIEVU pilot program. The MPD opted to use the local storage offering as it was more popular and metrics would be easier to compare to other agencies.

VIEVU software was a client that must be installed on all devices that were expected to view or manage video files. Once installed, users were required to login to the application to get access. Since a client was required to be installed for the local storage solution, sharing videos via the internet is not a possibility in the current iteration of the software.

VIEVU did not offer video redaction capabilities with the Veripatrol software package used in the pilot program. All VIEVU footage requiring redaction would need to be exported and edited in a third-party application by a qualified video technician.

Officers were expected to annotate all videos captured at the end of their shift. At the time of the review, there was not a mobile device option to annotate in the field. There was the possibility that annotation could be completed on the patrol car's laptop, but this functionality was not tested during the pilot program.

VIEVU Local Storage Solution



Governance and Operations

The pilot programs were managed by the MPD Business Technology Unit, a team comprised of several Police Officers at the City of Minneapolis. At the time of the consultation, a standard operating procedure was available to define expectations for how the cameras were to be used during the pilot programs. While this document did provide a good foundation for the body camera program, lessons learned from the pilot program should be applied to create a formal body camera policy document. This document should define usage, tools used, key contacts and responsibilities for the program. Additional documents should be created to support operating procedures and training. MPD is in the process of further developing these procedures based on learnings from the pilot program.

Since police body camera programs were still developing, it is expected that there will be several changes to legal requirements and how these programs are operated. At the time of the pilot program, several items were being discussed in state legislation that were not likely to receive final decisions until 2016 or later. The Police Records Information Unit along with the MPD should revisit current policies and procedures on a frequent basis as this program evolves and operational efficiencies are noted or legislation changes impact the program. This will be essential to ensure that the program is running optimally by learning best practices as body camera programs mature.

Governance and Operations Recommendations:

- Create and approve a formal policy and procedure prior to the launch of the full body camera program.
- Review policies, best practices and lessons learned on a frequent basis. Any relevant applicable changes should be made as the Body Camera Program matures.

Security Administration

Local security administration was performed by officers within the MPD Business Technology Unit. These officers will be responsible for provisioning users, system configuration and general maintenance on the system. No formal security administration policy or procedure documents were available at the time of the review. A detailed security administration policy should include expectations, roles and responsibilities, processes to provision users, processes to remove access for terminated users and password requirements, amongst others.

Two important controls should be considered if the Taser solution is selected. White-listing IP addresses for administrative functions would require that any administrative tasks originate from within the City of Minneapolis network. System administrators will have full access within the application, including the ability to delete files. Limiting their access to known IP ranges would prevent any unauthorized users from logging in if administrator credentials were compromised.

The second control is to consider implementing two-factor authentication for security administration. Two-factor authentication requires two items before you can log into the system, something you know (password), and something you have (key card, security token). This improves security as it is difficult to compromise both items.

Security Administration Recommendations:

- Create a formal security administration policy that should include but not be limited to the following key components: User Account Administration - Creating Accounts / Changing Account Access / Disabling or Deleting Accounts.
- Implement white-listing IP addresses for security administration.
- Implement two-factor authentication for security administration.
- Create a process to manage terminated users that will identify when users switch roles or leave the department, and when access should be removed immediately.
- Strong password policies should be enforced on all end users and administrators: eight or more characters, combination of letters, numbers, and/or special characters, and cycled every 90 days.
- Conduct periodic user access review to validate all users have appropriate access.
- Hold role owners responsible for approving all users assigned to their respective roles.

User Role Security

Taser and VIEVU products allowed security administrators to grant specific permissions to end users based on what access is appropriate. The two products differed in the implementation of these features. VIEVU allowed specific abilities (read, delete, copy, etc.) to be granted to each user individually. VIEVU did not offer role based security, which makes administering end users more labor intensive. If a policy change required modification of end user access rights, each user would need to be modified individually. This could be time consuming for system administrators.

Taser offered role based security. With this security model, a number of security roles were created (officers, Police Crime Lab, court, etc.) and users were assigned a role. If role changes were required, modification of the permissions associated with that role will automatically impact all end users assigned that role. Role-based security is more manageable than user-based security. Additionally, Taser offered the ability to assign officers into groups, where a supervisor can have access to view the camera footage of their direct reports.

At the time of the review, security rights for both products limited officers to only view videos that they created. A best practice that should be implemented is to separate any administrative functions from users operating body cameras. If an officer operates a body camera and also has system administrator duties, that officer should have two system accounts, one for system administrative functions and one for police body camera work.

User Role Recommendations:

- Prevent security administration roles from creating and uploading video files.
- Align user roles or permissions to job functions, which should be defined in the security administration policy.

Device Security

Taser encrypted both data in transit (SSL RSA 2048-bit key, 256- or 128-bit ciphers) as well as data at rest on the servers (256-bit Advanced Encryption Standard). These were industry best practices and sufficient to protect the data being transferred.

Only the local storage solution was evaluated for the VIEVU product. At the time of the review, VIEVU Veripatrol was not encrypting data at rest or data in transit. VIEVU does digitally sign the videos to validate that they are not modified. While this is a good process, digital signatures are not a substitution for data encryption.

Device Security Recommendations:

- Consider solutions to encrypt data at rest and in transit if VIEVU is selected as a vendor.

Networking

The internal network at the City of Minneapolis is a critical component for the body camera program as all body camera footage would be transferred via this network, to the data center and then to the internet if cloud storage is utilized (Taser). It is essential to have sufficient network capacity and throughput to allow all camera footage to be uploaded to the network/cloud, without impacting daily operations at the City.

Estimated data consumption based on Duluth's monthly average is 150 MB per officer per day. Based on this amount, the City could be uploading 75 GB per day (150 MB x 500 cameras). This data will not be a consistent load throughout the day, but will primarily impact the network at three separate intervals throughout the day, aligning with the end of officers' shifts.

All precincts and offices for the City of Minneapolis share the same network, with a speed of 180 mbps. It is important for the City to monitor the network utilization to ensure that daily operations are not impacted by the volume of traffic for these videos as the program expands. The onsite network team should be included in the launch of the full program and will need to closely monitor network health during the first few weeks and assess if the network is performing sufficiently. Two potential remediation efforts for impacted network performance would be implementing quality of service (QOS) prioritization, or increasing the network bandwidth.

Additionally, the pilot program was configured to operate on its own virtual local area network (VLAN). This is a good practice and should be replicated with the expanded program, as it will isolate the body camera network traffic from the general City of Minneapolis network traffic.

Networking Recommendations:

- Implement proactive network monitoring prior to full body camera deployment to ensure the network will be capable of supporting traffic requirements without impacting daily operations at the City.
- VLANs should be implemented to segment the body camera network traffic from the general network traffic at the City.
- Consider implementing QOS to prioritize network traffic.

Public Data Requests

Public data requests are likely going to be the most challenging component of the body camera program. At the time of the review, Minnesota legislation had not formally enacted many of the nebulous expectations related to public data requests. Fulfilling requests is likely to be time consuming and require additional resources. Current law requires all public requests to be fulfilled as soon as departments are able. Current redaction tools are very time consuming, require crime lab technicians to view the footage multiple times, and must go through a review process within the Police Department with support from the City Attorney's Office.

This process is likely the single most public facing component of the program. It is important that the policies, processes and procedures to redact, prioritize and review footage are well documented and available to the public. Due to the manual effort involved to redact footage, it is likely that the City will incur additional labor expenses for employees dedicated to fulfilling these requests. It will be important for the MPD to identify any tools that may be released that could reduce the time or effort to redact video. Additionally, there was one resource in the City Attorney's Office who was responsible for reviewing redacted footage, who had additional responsibilities beyond reviewing redacted footage. If the current process in which footage must be reviewed and approved by legal before being distributed remains, this review process could be a bottleneck for the public data request process.

Public Data Request Recommendations:

- Document and make available internally and to the public a formal public data request process and policy.
- Create a formal monitoring process to track the volume of public data requests, dependencies and bottlenecks in the process.

Video Redactions

Body camera footage released to the public may need to be redacted to preserve the anonymity of citizens or to prevent disclosure of private information. Redacting video was a time consuming and labor intensive process. This process was initiated with a data request, which could be either internal (e.g., case evidence) or external (e.g., public data request). The request was sent to the Police Records Department for prioritization, which takes into account the nature of the request. The process to redact video differs between the two product choices.

Taser had built-in redaction capabilities that help streamline the process. Bulk videos could be batch blurred in their entirety and at multiple levels of opacity, or a technician could blur or black out specific areas within the video file. Any edits made to videos did not impact the original file.

VIEVU did not have redaction capabilities within the Veripatrol software. Video files must be exported and edited within a third party tool by the Police Crime Lab Division. After redaction, the video files must be copied for distribution.

Once redaction has occurred, the City Attorney's Office, as well as the Police Department must review the footage in its entirety to verify the redacted videos are appropriate for public distribution.

Recommendations:

- Create formal standard operating procedure and training documentation to detail the procedures, tools and expectations related to video redaction.

Data Usage

The large amount of data consumed by the video files coupled with the estimated 500 plus officers that will record videos on a regular basis could equate to a large volume of data required to support this process. Data storage costs are likely going to be one of the largest financial burdens of this program. Using estimates based on the Duluth Police Department data consumption, each officer will consume 150 MB/day, extrapolating this figure to about 75 GB/day.

These estimates could vary depending on final policies or legislation that is passed. Additionally, the current cameras tested were configured to record at standard definition, if future devices or legislation require high-definition footage; data consumption could potentially multiply several times over. Processes to monitor data consumption and trending should be created.

With Taser, storage was directly tied to different pricing tiers, ranging from set amounts with overage fees to unlimited plans. The VIEVU program piloted used local storage, total costs associated with storage, retrieval, redundancy and backups need to be considered. Additionally, with VIEVU, local IT and Management would be responsible for performance and the control environment.

Data Usage Recommendations:

- Develop a process to regularly monitor storage utilization to ensure storage capacity or pricing tiers are optimally managed and to anticipate necessary changes.

Categorizing and Data Retention

Within both applications, users could assign each video an applicable category (e.g., citation, arrest, use of force, etc.) that will determine the length of time the video will be retained for. Categories should be clearly understood and consistently applied when uploading video. It was noted during the pilot program that up to 17% of videos were not categorized. Proper classification of videos is essential for applying the correct record retention schedule. Educating officers on the importance of completing this field, configuring the applications to

require this field or implementing a review process are potential controls that could reduce risk in data categorization and retention.

One potential improvement to the existing categories used during the pilot was to create a category specific to ongoing litigation or court cases. It is a mandate that evidence be retained until the legal process is resolved. If videos were categorized with the standard labels and the retention period lapsed, it could appear to the legal process as disposing of evidence prematurely.

Record retention requirements were following a set schedule of one year, seven years, and in perpetuity, depending on the content captured in the video; non-event police event, police evidence, and significant/critical incidents, respectively. These durations may change in the future as the legislation formulates, but at the time of the pilot program, all video is set to follow this schedule.

Categorizing and Data Retention Recommendations:

- Implement a process or control to verify that all videos are classified and aligned to appropriate record retention schedules per legislation.
- Consider adding additional categories to flag and prevent videos involved with litigations from being disposed of prematurely and create a process to update the category for videos subject to litigation.

Chain of Custody and System Logging

Both solutions had detailed logging capabilities that capture creation, deletion, modification and viewing of footage. This logging was detailed enough to support chain of custody. It should be noted that VIEVU did not offer any redaction capabilities within the application available at the time of the pilot program. If redaction was required on footage captured on the VIEVU device, the footage must be exported and edited in a third-party application. The logs from VIEVU, in addition to the manual logs completed by the crime lab, will be needed to create adequate chain of custody evidence. Taser had built-in video redaction tools that are logged; no external manual logs were needed in addition to the system logs that are created to satisfy any chain of custody requirements.

Alerting was another feature of the Taser solution that was leveraged during the product evaluation. Alerts would be sent to system administrators for various triggers (e.g., account creations, file deletions, password resets, etc.) While this was a good practice and it is encouraged, it will be important to monitor and manage this process as the program scales up. It is important for system administrators to receive a manageable amount of alerts. If the scope of alerting is too broad, significant alerting events may be missed due to the large volume received.

Chain of Custody and System Logging Recommendations:

- Implement a process to ensure that alerts sent to system administrators are relevant and the process is manageable.

Other Recommendations for the roll-out of the Minneapolis Police Body Camera Program:

- Include a right to audit clause within the contract with the selected vendor to allow for further analysis of internal controls within the vendor's organization.
- Obtain Taser internal controls and Evidence.com third-party audit assessment, when available.

- Completion of policy and procedure documentation and creations of an extensible process to manage intake, video redaction, public data requests, and system and user administration.
- If mobile devices will be used in conjunction with body cameras, the considerations of using of personal mobile devices should be understood and evaluated.

Acknowledgements

The City of Minneapolis Internal Audit team would like to acknowledge the time, effort and partnership put forth from the Minneapolis Police Department's Business Technology Unit, City of Minneapolis City Attorney Department, the Police Records Information Unit, and Police Crime Lab. Their collaboration and timely responses were critical in helping us complete a comprehensive review of the Police Body Camera program.