Police In-Car Camera Technology Application Controls
March 2018

Lori Brooks Jaquess, City Auditor
Susan Edwards, Assistant City Auditor
Roshan Jayawardene, Internal Auditor

City Auditor's Office

March 26, 2018

Honorable Mayor and Members of the City Council:

The City Auditor's Office has completed the Police In-Car Camera Technology Application Controls audit. The purpose of the audit was to review and evaluate technology application controls and compliance with applicable policies.

Management's response to our audit findings and recommendations, as well as target implementation dates and responsibility, is included following the report.

We would like to thank staff from Arlington Police and Information Technology departments for their full cooperation and assistance during the audit.

Lori Brooks Jaquess

Lori Brooks Jaquess, CPA, CIA, CGAP, CRMA
City Auditor

Attachment

c: Trey Yelverton, City Manager
Jim Parajon, Deputy City Manager
Gilbert Perales, Deputy City Manager
Jennifer Wichmann, Acting Deputy City Manager
Will Johnson, Arlington Police Chief
Dennis John, Chief Information Officer

Police In-Car Camera Technology Application Controls
Table of Contents

Executive Summary

The City Auditor's Office has completed the Police In-Car Camera Application Controls Audit. The performance audit was conducted in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. The audit objectives were to:

- Determine if requests for video evidence are provided within the State of Texas mandated timeframe and videos are available within Arbitrator Software for fulfillment of requests
- Explore methodologies for efficient video upload with minimal impact to other public safety applications, utilizing real time data transfer
- Determine if system security is adequate to meet compliance requirements and efficient operations
- Determine if software includes adequate internal controls to support daily operations and existing policies and procedures

The City Auditor's Office noted the following strengths during review of the Arlington Police in-car camera software:

- Audit trails are operationally adequate
- The system functions as intended with acceptable video quality
- System access is based on job needs

We noted potential opportunities for improvement in the following areas:

- Video copies retained outside of the system
- System log-in capability
- Update of policy and procedures
- Master equipment list
- File naming conventions
- Digital media management software
- Utilization of wi-fi hotspots

Details of audit findings, conclusions and recommendations are included in the following report.

Audit Scope and Methodology

The audit was conducted in accordance with generally accepted government auditing standards. The following methodology was used in completing the audit.

- Reviewed policies and procedures for video operations
- Interviewed APD technology staff and system administrators
- Reviewed use of video equipment and video files with patrol command staff
- Contacted the vendor for system specifics
- Interviewed City IT staff and AT&T technical staff on use of wi-fi methodology for file upload
- Reviewed audit trails for key video files in Arbitrator
- Reviewed security practices and user profiles
- Assessed future video needs for police operations considering new body camera video system
- Reviewed open record fulfillment process for video file requests

Background

The Arlington Police Department (APD) introduced the current in-car camera video system in 2012. It replaced a legacy system that was installed in a limited number of police vehicles. In-car camera video systems are currently installed in most police patrol vehicles. A total of approximately 200 video systems are currently installed in police patrol vehicles. The video equipment and software to manage the equipment is provided to the City by Panasonic. The software is referred to as Arbitrator video management software.

The video system in police vehicles consists of a forward dash mounted camera, rear-view camera or camera for rear passenger area, microphone for the rear passenger area, as well as a microphone attached to the officer's uniform. A Digital Video Recorder (DVR) in each police vehicle retains the video files until they are uploaded to the server. The video system and audio recordings are activated automatically by any of the following:

- Activation of police siren and lights in vehicle
- Vehicle speed more than 80 mph
- Activation of the crash sensor in a police vehicle
- Manual system activation by officer

Program Objectives

The APD has established the following operational objectives for its in-vehicle video and audio recording systems:

- Maximize officer safety
- Maximize the effectiveness of officer reporting, evidence collection, and court testimony through video/audio documentation of events, actions, conditions and statements made during arrests and critical incidents

- Comply with State law requirements regarding Bias-Free Policing
- Efficiently review probable cause for arrest, arrest procedures, officer and suspect interaction, and evidence for investigative purposes
- Protect against false claims of impropriety
- Provide officer training

The Arbitrator video and audio recording system is managed by the APD technology services team. The team includes two system administrators, a database administrator, and a manager.

System Information

The Arbitrator video system is accessed via the mobile data computer (MDC) in police vehicles. The system requires the user to log in to Arbitrator using his/her City's network active directory credentials. Once the system is activated, it records continuously until the DVR recorder is manually stopped by the officer. Once the recording is halted, the system recognizes the video length as a video segment and is saved under the log in credentials used by the officer. Once stopped, users have an opportunity to tag the video as evidence or use other operational criteria for tagging.

The Arbitrator system then automatically uploads the video segment to the Arbitrator server via a real time cellular connection. The video segments can be lengthy, spanning from a few minutes to a segment that lasts for an hour or more. There are two basic video gear models in service currently. These are the Panasonic MK2 and MK3. The MK2 units are older and the resolution of video content is standard. The newer MK3 models offer high definition resolution video images.

Access to Arbitrator software is based on job needs. A patrol officer is given access to view his or her own video segments and the right to name video segments per operational criteria. Police sergeants and command staff are given supervisory access. They can view any videos in the system and make a copy of a video to a DVD disk that is retained outside the system. Video copies on DVD disks are used by command staff to view particular police incidents, such as use of force. Video segments labeled as Internal Affairs can only be viewed by designated investigative personnel and excludes patrol officers, supervisors and command staff. Police administrative staff, such as records personnel, open records staff, police legal staff, and reports staff are also given system access. They can view any video in the system and make copies as necessary. The system can generate reports on common criteria, such as file deletions, copy activity, playback activity and file classification.

Arbitrator software enables users to view the video, use fast forward and backward functionality, and search videos based on selected criteria. A user can locate a video in the system based on the following criteria:

- Officer name
- Time and date
- Police division
- Vehicle number
- Video classification criteria such as evidentiary, traffic, use of force and internal affairs, etc.
- Police unit and shift
- Case file number

Video Retention

Videos are retained in the system per State of Texas record retention criteria and Arlington Police retention criteria. The police department has elected to retain videos for time periods that exceed State requirements. In general, videos are retained as follows:

- Default: 180 days
- Evidence: 65,000 days
- Internal Affairs Division: 65,000 days
- Training: 365 days
- DWI: 365 days
- Open Records: 750 days
- Special Investigations: 65,000 days

Evidence Management

Videos are retained primarily for their evidentiary value and are used in court proceedings by many government agencies. Typically, the evidence is used by Tarrant County. Video evidence is submitted to Tarrant County via a process called Tech Share. It is submitted electronically via a website established by Tarrant County. The APD also receives video evidence from third parties associated with a crime scene being investigated, such as businesses where a crime may have occurred; and video evidence from surveillance cameras and videos submitted by citizens are also received. Third party videos are stored outside of Arbitrator software, mainly in Digital Video Disk (DVD) format.

APD is subject to meeting compliance requirements in addition to video file retention requirements. The Michael Morton act requires government agencies that collect evidence in all forms to provide the evidence to an individual accused of a crime.

Open Record Requests

APD receives many open record requests for video evidence, as well as requests for police reports and 911 call records. The Texas Public Information Act mandates local governmental agencies provide applicable documents and files to the public. Documents applicable to ongoing investigations, however, are exempt from public release. Documents that contain personal information or protected information can be redacted prior to public release. The review of open records requests was limited just to in-car camera video request fulfillment only. Open records fulfillment in general, or evidence other than video, was beyond the scope of the current audit.

For most open record requests for video evidence, all existing videos of a particular crime scene or police activity are requested. These requests may entail in-car camera footage from many officers that responded to the call. In major crime events, 20 of more officers may respond to the call and searching for video evidence in Arbitrator becomes a daunting and time-consuming task. Video open record requests are sent to the police legal team for review, prior to release. If it is determined the video should not be released due to ongoing investigations or it needs to remain protected otherwise, they appeal to the State Attorney General's Office. The Attorney General then decides if video evidence can be withheld from release.

Detailed statistics for open record requests for video evidence is only available for the recent year, beginning in January 2017. Detailed records prior to 2017 had not been maintained by APD staff responsible for fulfilling open record requests. As of June 2017, a total of 3271 open record requests had been received, 200 of which were requests for police in-car camera video evidence.

Audit Results and Findings

APD Mobile Digital Recording Equipment Policy Needs Revision

Policies and procedures are intended to increase efficiency of operations and provide detailed guidance to employees. The APD general orders includes mobile digital video recording equipment policy. These mobile digital video recording equipment policy and procedures need updating to reflect current practices followed by police personnel.

The policy includes an outdated video evidence submission methodology and does not provide detailed instructions on use of vehicles in the event of malfunctioning video equipment. The current policy describes an evidence submission methodology using the Arlington police intranet (portal); however, the current submission method is a process called Tech Share, which is a web based submission method initiated by Tarrant County.

Current practice is that Police vehicles with malfunctioning video equipment are taken out of service, unless an emergency warrants the use of such a vehicle. This practice appears reasonable. This practice is not reflected in the current policies and procedures.

Policies and procedures that are not updated to reflect operations can cause confusion to employees and become ambiguous to interpret.

Recommendation:

1. The City Auditor's Office recommends that the Arlington Police Chief require staff to update current Arbitrator policy and procedures to reflect current video evidence submission methodology and provide detailed guidance on use of vehicles with malfunctioning Arbitrator video equipment.

Some individuals with access to Arbitrator were not known employees or volunteers

A review of a sample of 370 access profiles identified 3 profiles that could not be verified as an active or former employee or volunteer for the Police Department.

The names were compared to the City's Lawson system, which includes records for current and terminated employees, and the names were compared with a list of volunteers maintained by the police department. The names were also compared to the City's IT department records to determine if an active directory account existed for the exceptions. The system administrators did not have any documentation showing access request or approval for the named individuals.

Generally accepted IT security guidelines require that system access be based on job needs and that access requests and approval by management be documented and retained.

Access to Arbitrator is currently sourced from the City's active directory. Based on the active directory, system access profiles are setup in Arbitrator based on job needs. There are 3 main system roles in Arbitrator. These include "PD everyone group," "Supervisory staff," and "video evidence

groups." Users in the Supervisory and video evidence groups (i.e. Police open records request staff and staff who process police records) have access to review any file in the system and copy and upload files from the system. Users in the PD everyone group can view their own videos, but cannot copy files. Access requests are usually sent by the supervisory staff to the system administrators via email, in which they indicate the extent of access to be granted.

System access requests and approvals are not currently retained by the system administrators. Such documentation would likely have indicated the employment status for the 3 exceptions identified, including place of employment, time of employment, and specific job needs related to video evidence in Arbitrator. There are no existing policies and procedures that establish access rules, management approval, and documentation guidelines.

The employees in question were listed as members of the "PD everyone group", which only grants access to video files generated by the user. The system audit trails show neither evidence of these individuals logging on to the system, nor any videos that they created. Ghost access profiles can create a security risk, where video files can be leaked to unauthorized parties, considering the sensitive nature of the video evidence. The accounts were currently disabled.

Recommendation:

2. The City Auditor's Office recommends the Arlington Police Chief develop detailed policy and procedures that address system access requirements.
3. The City Auditor's Office recommends the Arlington Police Chief require system administrative staff maintain documentation of system access requests and management approval.

Generic Accounts in Arbitrator are excessive

Our review of access profiles in Arbitrator identified a total of 23 generic accounts, among the 1,140 active account profiles. These generic profiles have been set up by the system administrative staff. Among these are 3 accounts for interns, 6 accounts for testing, 2 accounts for the police records unit, and 2 accounts titled police scanner unit, among others.

Generic system access profiles are set up for tasks, such as system testing, and to give access to vendors who perform system maintenance. Once the intended tasks are completed, the generic access profiles should be removed from the system.

It appears the generic accounts were set up due to system needs, such as testing; special assignments for police divisions (e.g. records unit); and for training needs. It appears the accounts were intended to be used by more than one individual. The generic accounts in Arbitrator mirror the generic accounts set up by APD for network access, hence the generic access profile in Arbitrator.

The primary risk related to generic accounts is the difficulty in identifying the user of the generic account. A majority of the generic accounts have limited access because they are in the "PD everyone group" profile, as noted earlier. Alternatively, generic accounts under "police records" and "system

administrator" groups have access to video files system-wide, allowing the user a broader range of access. These are at a higher risk of misuse. The risk of misuse can be mitigated by limiting the number of generic accounts which also falls under generally accepted system security guidelines.

Examination of the use of generic accounts by APD for City network access was not performed, as it was considered beyond the scope of the current audit.

Recommendation:

4. The City Auditor's Office recommends the Arlington Police Chief ensure Arbitrator system administrators review current generic system access profiles and limit the number of these accounts, based on job needs.

Former employee access profiles were not deleted from Arbitrator in a timely manner

Access profiles for retired or terminated employees should be deleted timely. Current Arbitrator access profiles include individuals who have retired or been terminated from City employment. A sample of 370 (of 1,140) profiles were selected for audit testing. A total of 69 (19%) exceptions were noted.

An individual's access to Arbitrator software is based on the City's active directory, which grants access to the City network. Credentials, such as active directory password, are used to gain access to Arbitrator, once the access profile is setup within the system. When access to the City network is terminated, the password that is used to gain access to Arbitrator is disabled. However, the access profile in Arbitrator is retained until system administrators manually delete it.

Supervisors usually request system access for an individual via email. The system profile is then created and linked to the city's active directory profile for system access. Notification of promotions and retirements are accomplished via Police Department informal channels, such as emails and internal publications. System administrators use this information to upgrade or terminate system access.

Generally accepted IT Security Practices require termination of system access and deletion of access profiles once employment has been terminated. Ideally, system administrators follow generally accepted system access deactivation to preserve the integrity of the system and data, as required by established policy and procedures.

System access policies are generally reflected in a system policy and procedures manual. Specific guidance on employment termination and system access termination is not included in policy guidelines currently in use. It appears the informal channels for notifying system administration staff of employment terminations and promotions are not used on a regular basis to terminate system access. Some APD system administrators (those administering personnel and payroll matters) receive notifications from the Lawson system when employment is terminated for any reason. However, it is apparent such notifications are not also being sent to the Arbitrator system administrators.

The primary risk of unnecessary former employee access profiles in Arbitrator is unauthorized access. In this case, the risk is mitigated to some extent by deactivating the city network access credentials upon termination of employment. Also, the access for most of the former individuals is limited to viewing video files created by themselves. However, there is some residual risk associated with not terminating network access in a timely manner. Review of network access terminations for former APD employees shows that network access termination is not immediate upon the employee's last day at work. This issue is detailed in a separate finding.

No evidence of unauthorized access or misuse by terminated employees was identified during audit testing.

Recommendation:

5. The City Auditor's Office recommends the Arlington Police Chief require that Arbitrator system administrators terminate software access profiles within a specified time from the date of termination, and coordinate notification of terminations from the Lawson Human Resource system, with assistance from the City's Human Resources Department.

Multiple access profiles for individual employees exist in Arbitrator software

The review of a sample of 370 access profiles in Arbitrator indicated three current employees had more than one access profile. Name changes, presumably due to marriage or divorce, were the reasons for the multiple access profiles.

According to Generally Accepted Information Security Standards, there should be only one system access profile for each individual. This standard is based on data security, data integrity, and ability to trace transactions to one party under one user name.

It appears that the system administrators set up a second user profile upon the employee name change without deletion of the former profile. A process to periodically review system access profiles to ensure validity is not performed by system administrators.

The three exceptions noted included two police officers having access to their own video files, and a civilian investigator with the ability to view any video file in the system, but did not produce video files as part of his/her job duties. No evidence of unauthorized activity was identified during audit test work or by system administrators. Although activity can be traced via audit trails within the system if multiple profiles were used by an employee, limiting profiles is industry best practice that should be followed.

Recommendation:

6. The City Auditor's Office recommends that the Arlington Police Chief require Arbitrator software system administrators eliminate dual profiles when making employee name changes and review access profiles periodically to identify and correct any access profile anomalies.

Network access terminations are not timely

Network access was not consistently terminated timely by the City's IT department.

Network access terminations, performed by disabling the active directory accounts, were not consistently conducted in a timely manner. A sample of 370 access profiles were reviewed. The following 17 exceptions were noted during the review.

Time Lapsed from Termination Date	Number of Exceptions
Still active (terminated 8/31/2015)	1
80+ days	4
40 days – 60 days	2
30 days – 39 days	1
14 days – 29 days	3
3 days – 13 days	6

Generally Accepted Information Technology Security Practices require immediate network access termination for departed employees to protect data and data integrity.

Termination of City network access is completed, via a work order system, by the IT Department. Notification of an employee departure is received as an auto generated email via the Lawson Human Resource enterprise system. Once the notification is received, a work order is created and assigned to a network technician to disable the active directory account.

It appears that delays in completing a network technician's assigned work load is contributing to delayed disabling of the active directory account. Also, it appears a lack of documented departmental policy and guidance is contributing to delays.

As illustrated in the table above, the delay in terminating 10 former employees out of a sample of 17 was in excess of 14 days; and one employee, terminated over 2 years ago, still has network access. The primary risk is a that a former employee will access the city network and departmental files they had access to as an employee and use this information in a malicious manner. Detailed testing to determine if former employees had accessed the City network after termination is beyond the scope of the current audit. However, as a measure of best practices and data security, timely termination of network access to safeguard data integrity is warranted. Regarding Arbitrator software, system administrators have no evidence of data compromise by former employees.

Recommendations:

7. The City Auditor’s Office recommends the Chief Information Officer establish network termination standards based on Citywide data security, and require that network administrators terminate network access for departing city employees within established time intervals.

8. The City Auditor’s Office recommends the Arlington Police Chief, in collaboration with the Information Technology Department, initiate request for additional communication from IT

regarding the status of terminated employees' network deactivation and/or identify methodology for validating that active directory user account has been deactivated.

The Arbitrator software disaster recovery plan requires testing and current data backup should be expanded

The Arbitrator software disaster recovery plan requires testing and documentation. It has not been tested to ensure operability after a disaster. It was noted that only files marked as evidence are backed up. Since files are not always marked as evidence immediately, there could be loss of essential data after system recovery. Data backed up daily should include that which is required operationally, and data needed for state and federal compliance requirements.

A review of the current disaster recovery plan for the Arbitrator software did not indicate the plan has been tested to ensure recoverability and recovery time. Currently, only video files marked as evidence are backed up daily. Some video files are not marked as evidence when they are first produced. Some video files are marked as evidence at a later date by detectives and prosecutors. In the event of a total system loss, currently APD would be unable to recover files not marked as evidence and potentially needed at a future date as evidentiary files.

Generally Accepted Information Technology Practices require that a disaster recovery plan be tested on a routine basis. Recovery time and efficiency of recovery (as needed operationally) should be documented. Disaster recovery plans include redundant hardware, such as servers; obtaining a copy of the application software with vendor assistance; as well as retrieving data that is backed up by the City's Information Technology staff.

Testing of the disaster recovery plan would include complete system restoration. The test would require a coordinated effort between APD system administrators, City Information Technology Department, and the software vendor. There is no evidence of such coordination since system implementation in 2012.

Due to the large volume of video files that are uploaded to the system daily, APD management decided to backup only the Arbitrator files marked as evidence or another operational category. The database size is approaching 80 terra bites of data and is expected to grow in the future.

To determine a software system's operability and recovery time after a disaster and loss of data, it is necessary to perform a routine disaster recovery test. Absent such tests for Arbitrator software, it is not known if system recovery after a disaster will meet operational and compliance needs.

Since the recovery data is limited to files marked as evidence, others that may be needed as evidence at a future date will not be available after recovery. State and Federal evidence retention laws require general video files to be made available for 90 days. In the event of disaster recovery, the City may not be able to comply with requests.

Recommendation:

9. The City Auditor's Office recommends that the Arlington Police Chief require Arbitrator system administrators test and document the current disaster recovery plan to ensure recovery time and the recovered system meets operational needs; and expand backup to 90 days for all Arbitrator video files to meet compliance requirements in the event of recovery after a total system loss.

System updates rejected by Arbitrator have not been examined and resolved with assistance from the vendor in a timely manner

A review of Arbitrator reports for various system updates show the following exceptions:

- Approximately 4 video recorder units failed to update the front-end software during January 2015 and June 2017. These updates are automated and sent periodically by the Arbitrator server.
- There were approximately 290 instances of DVD units failing to update firmware between January 2014 and June 2017, with some DVD units failing to update on multiple attempts. Firmware is a software program or set of instructions programmed on a hardware device that provide the necessary instructions for how the device communicates with the other computer hardware.
- There were approximately 250 instances of Arbitrator video recorder units failing to update the recorder settings, with some units failing to update on multiple occasions between January 2014 and June 2017.

System updates are intended to improve performance, correct particular vulnerabilities and increase productivity. System updates are initiated by vendors and performed as part of system maintenance agreements. They are conducted periodically by vendors, based on software needs. System updates are also initiated as part of automated tasks, or auto updates by the server. The exceptions noted were periodic automated updates by the Arbitrator server. Equipment, such as cameras and video recorders are also routinely updated in addition to updates made to the server, front end application, and mobile data computers in police vehicles.

The system administrator identified one digital video recorder unit that failed to update its front-end application, due to an older version of DVR software that was still present in that unit. Detailed analysis of causes of failure will require vendor assistance that has not been sought by system administrators. Vendor assistance is required due to proprietary software code in Arbitrator, as well as analysis tools specific to the application.

The Arbitrator system, used to record video clips in police vehicles, consists of several components. They include servers that run the software and hardware components, such as cameras, video recorders and microphones. Each of these components function in unison to produce a video that meets APD's business needs. Updates are equally applied to all components for them to work in

unison. Any component not updated along with the others, creates a high probability of failure in producing desired video clips.

If the system fails to produce a video clip, due to malfunctioning equipment, it is not recorded as an exception within the system. These failures are only noticed if a video clip is needed for administrative purposes and is not available in the system.

Recommendation:

10. The City Auditor's Office recommends that the Arlington Police Chief require Arbitrator system administrators to monitor system reports and initiate corrective action for software update failures, with vendor assistance in a timely manner.

Wi Fi option for Arbitrator video upload is a better alternative

Arbitrator video files are currently uploaded using wireless technology. Real time video uploads are accomplished through a wireless network that is also used for Police data transmission, such as Computer Aided Dispatch (CAD) and other applications in mobile data terminals. The file is retained in the vehicle digital video recording unit, and the upload process begins once the file is named or when an officer logs off the Arbitrator application.

Arbitrator software and its associated vehicle mounted in-car cameras record police activity on a real-time basis. The videos are stored in the digital video recorder unit. Once the recording is complete in each incident, the system is automated to upload the video files to the Arbitrator server in the data center. The system utilizes existing wireless methodology in the upload process. The live upload process was based on available, viable and reliable methodology when the system was implemented in 2012. The file transfer process must also meet Criminal Justice Information Systems (CJIS) file transfer compliance requirements. This is the reason for use of the live wireless upload, since it consists of required file encryption. The video files contain sensitive personal information, as well as information that needs to be preserved as evidence in legal proceedings, which requires protection protocols.

Arbitrator in-car camera software has been uploading video files in real time using the existing City's mobile network since its inception in 2012. Attempts for alternative methods, such as a dedicated VPN or secondary mobile wireless vendors, failed due to technical limitations in the City network, limitations in Arbitrator software configuration, and cost limitations.

Arbitrator video files are usually large. Video files can range in length from several minutes on a short traffic stop to more than an hour on complex police activity involving a shooting, robbery or lengthy pursuit of suspects. Once the recording activity is manually terminated by the officer upon conclusion of the incident, the system marks it as an individual file, and the upload process begins immediately over the wireless network. These lengthy files have a negative effect on the wireless network. The bandwidth on the network is limited, and it can only transmit a limited amount of data. When lengthy Arbitrator video files upload, it takes up the entire available transmission capacity

and freezes the other wireless network traffic, such as computer aided dispatch. Freezing events result in the officer having to reboot the MDC unit in the vehicle.

The Cities of Dallas and Fort Worth were benchmarked on their best practices for police in-car camera video uploads. The City of Fort Worth currently uses a legacy in-car camera system that requires manual uploading of video files. They are in the process of replacing the in-car camera system. The new system will upload at Wi-Fi hotspots located throughout the City and not utilize its mobile networks for upload activity. The City of Dallas also utilizes Wi-Fi hotspots located throughout its main and sub police stations for in-car camera uploads.

Arlington's Information Technology staff benchmarked smaller Central Texas Cities through a list service to which they subscribe. The cities of College Station and Bryan use Wi-Fi for their police in-car camera videos. The hotspots are located at police stations and other City facilities.

Recommendation:

11. The City Auditor's Office recommends that the Arlington Police Chief utilize Wi-Fi hotspots for Arbitrator in-car camera video file uploads, that can be installed in Police facilities and other key City facilities, to reduce the burden posed by large video file data transfers to the mobile wireless network.

Notification Letter in FOIA software is needed

Per guidance from the Texas State Library and Archives Commission on the Texas Public Information Act, notification should be sent to individuals requesting records, when the city is expected to take longer than 10 days to provide the requested documentation.

A review of FOIA Software, which is used to process open records requests received by the City, indicates that a key notification letter is not currently available in the system. This letter is to inform open record requesters when it is expected to take longer than 10 days to fulfill the request. FOIA software tracks all open records received by the City. It indicates the date of receipt, includes correspondence with requester, shows an audit trail of activity and progress by assigned staff members, and retains documentation, provided as attachments, within the software.

The Texas Public Information Act, chapter 552, gives citizens the right to access governmental records. This law governs the open record request process. The law gives an entity 10 business days to provide the documentation a citizen is seeking. If the process is expected to take longer than 10 business days, the entity should give the requester an expected time frame for providing the documents. The entity must release requested documents, unless authorized by the State Attorney General to not release the documents, based on protection allowed by law. Additionally, the law provides the following processes to benefit citizens requesting information.

- A written estimate for any costs incurred for document search, research and retrieval
- A notification if an Attorney General opinion is sought not to release documents

- Provide certain documents, such as voting records of public officials, without an inclusionary clause

The Attorney General will not consider protection of documents from release, if the request to them is not made within the 10 business day period from receipt of request by citizen. Once it is exceeded, all documents must be provided to the requestor.

Delays in providing documents to requesters are generally due to the time needed to locate documents, redact personal information, or seek Attorney General opinion on protecting documents from release. When documents are requested by the public, the individuals usually ask for any and all documentation pertaining to an incident, such as a police involved activity. Each of these activities may contain large volumes of information, video clips, multiple police reports and even 3rd party provided evidence associated with a particular case. Staff time to sort through the documents is extensive, resulting in delays longer than 10 business days in certain cases. The law does not provide a specific time frame to provide documents. Government agencies may take the time needed to provide citizens with requested documents, providing the proper notifications to requesters are made.

Standardized letter templates for notifications can be stored in the City's FOIA system and be emailed or mailed to a citizen. There can be fillable fields within the letter, where an employee can insert pertinent information for the requestor.

Compliance with the law is mandatory. Notifications to the requestor if more than 10 business days are needed is a good measure of customer service, which may reduce the number of phone inquiries received by the open records staff.

Recommendation:

12. The City Auditors Office recommends that the Arlington Police Chief require the police legal staff, with assistance from FOIA system administrators, to formulate a letter template that can be sent to a citizen when staff believes the search, research and providing of documents will exceed the 10 business day period the State law requires.

Resource assessment for the video redaction unit is warranted

A review of pending open records request cases associated with the APD show some backlogs, attributable to the video redaction process. Total exceptions are minor compared to total amount of open record requests processed for APD. A total of 5 cases are shown as past due from 2016, as well as approximately 10 requests that were currently due, at the time of the review, for the month of July 2017.

Video evidence is reviewed by APD legal staff prior to public release. They are reviewed to identify information needing redaction, such as individual personal information, information pertaining to juveniles, or information related to medical conditions that may be visible in video evidence.

APD legal staff is required to perform the video redactions to ensure compliance. The task, which is time consuming, is assigned to one paralegal, and the redaction software is limited to one stand-alone computer. The request for video evidence through the open records process has recently increased greatly; however, the staffing and the software used to redact videos have remained the same.

Backlogs in video redaction causes delays in providing the requestor with video segments. The impact is primarily customer service related, considering there are no specific established time limits to provide evidence, providing the requestors are informed that fulfillment will take longer than 10 days. Just recently the city introduced body worn cameras for police officers. These videos are expected to cover more police activity than the current in-car camera videos. Each officer responding to an incident is expected to have video footage, and since many officers respond to incidents, the volume of videos is expected to be increase dramatically.

Open records requests by citizens usually include all available evidence associated with an incident. In the future, the city will be required to review a much higher volume of videos. It appears there is a need for more resources in the video redaction unit to review and process the increasing number of requests.

Recommendation:

13. The City Auditors Office recommends that the Arlington Police Chief conduct a resource assessment in the Police Legal Division to ensure there is adequate personnel and redaction software for current and future needs.

Aging evidentiary video files require review to determine if retention is necessary

The Arbitrator system consists of aging video files that are marked as evidence or other criteria, such as use of force and traffic categories. These video files date back to 2012 when the system was first implemented. Considering some of these cases may have already been adjudicated, the retention period set forth by the police department for these video files may have been exceeded. The video files that may have exceeded retention requirements are Class C misdemeanors and Class A and B misdemeanors and state jail felonies. Other classes of video files, such as those related to internal affairs investigations, second and third degree felonies, and first degree capital felonies have retention periods ranging from 10 to 50 years.

The APD, beginning in March 2017, set forth new retention guidelines for videos. These guidelines, based on operational needs, exceed what is required by law in some cases. The retention periods are as follows:

- Class C misdemeanors - 6 months
- Class A & B misdemeanors and state jail felonies - 2 years

Review of video files that fall under class A, B and C misdemeanors requires reconciliation with court adjudication records, in order to determine if its retention period has expired. APD has not performed

the review and reconciliation on aging video evidence files. Files created between 2012 and 2015 are in need of review. An operational process to conduct such reviews is not evident.

Video files are usually large in size, due to length and the resolution of the video. File sizes can range from several megabytes to gigabytes, consuming a large volume of server disk space. Storage is expensive, considering the IT resources that are needed to maintain servers, as well as resources are needed to back up the data. The Arbitrator video system includes approximately 14,000 video files that are marked as evidence between 2012 and 2015. The system does not show file size for these videos, but it is expected to be several terabytes.

Aging video files marked as evidence are expected to increase greatly after the body camera system is implemented. The city will be able to better manage aging video files going forward with an introduction of an operational process to perform reviews/reconciliation on a periodic basis. Data storage costs, as well as data management costs, are expected to decrease as a result.

Recommendation:

14. The City Auditor's Office recommends that the Arlington Police Chief allocate adequate resources to review aging Arbitrator video files for retention compliance periodically, and purge files based on expiration, as established by retention laws and operational policies.

Vendor assistance needs to be expedited to resolve errors in some Arbitrator system equipment

A review of Arbitrator system error notifications indicates an inherited error, common to the older MK2 video recorder units. The system rejects/deletes the IP address of the unit, which results in the failure to automatically upload videos. System administrators have notified Panasonic (Arbitrator vendor) of the error, however the item remains unresolved. Approximately 93 MK2 model units are in use in police vehicles. The failure to upload results in the need for a system administrator to locate the MK2 unit, physically visit the vehicle where it’s attached, and reinstall the system. This process is very time consuming.

Per the maintenance contract with Panasonic, errors are prioritized and resolved based on priority level. The MK2 unit error is classified as a priority, and the vendor has known of the error since February 2017. The vendor has not been able to permanently resolve the issue.

Panasonic cites a corrupt configuration file in the system as the cause, and has notified the system administrator that reinstalling the software is the only resolution to the error. The efforts involved or when there will be a permanent solution is not known.

If a unit fails to upload videos and is not detected, the unit will continue to save video files in its hard drive until its capacity is reached. The possibility exists that the video recorder will run out of space and not record any new video files.

Recommendation:

15. The City Auditor's Office recommends that the Arlington Police Chief require that Arbitrator system administrators seek to expedite a permanent resolution of the MK2 video recording unit issue.

The Arbitrator master equipment file should be updated

The equipment master file in Arbitrator needs to be updated. The system generates notifications to system administrators of video file upload failures. However, the master equipment file includes equipment no longer in service and many notifications are not useful. The system administrators ignore the upload failure notifications due to the errors, and the usefulness of a valuable system control is diminished.

The system includes several controls to enhance operations. The video file upload error notifications are intended to ensure availability of files required for operations. Once a video is completed, it should auto upload via a live cellular connection to the server, making the video available to management and other personnel, such as detectives. The failure notifications are intended to alert the system administrator to troubleshoot the failing unit and manually upload the files, prior to error correction.

Units and equipment are removed from service due to malfunction or destruction (e.g. when a police vehicle is in an accident that could damage equipment attached to the unit). It appears the equipment master list has not been updated to remove out of service units, since the system was implemented.

Since the system routinely generate notices for equipment not in service, the notifications are not utilized by system administrators. They, instead, respond and investigate when management or an officer reports missing video segments in the system. The system administrator must then track down the vehicle in a police substation and manually troubleshoot the unit, as well as retrieve the video segments, due to upload failures. The current process is time consuming.

Recommendation:

16. The City Auditor's Office recommends the Arlington Police Chief require that the Arbitrator system database administrator, in coordination with system administrators, update the equipment master file, to include only equipment currently in use, and use the system notifications as intended.

The number of video copies retained outside Arbitrator is excessive

A large number of videos are copied and stored outside of the Arbitrator system on DVD's. Many are categorized as use of force videos. At the end of a shift, the field officers notify police sergeants of any use of force videos. The sergeant views the video in Arbitrator and makes a DVD copy for police command staff review. A form is completed by the sergeant, regarding justification of the use of force. The process is repeated by command staff, including documenting if use of force is justified. These video copies are then left in command staff "in boxes" with other mail in plain sight. In some instances, more than one officer is involved in use of force. In this event, multiple

videos are copied to disks and given to command staff for review. After review, these video copies are sent to the police training center for long term retention.

APD's existing policy requires review of use of force incidents, including documentation of whether use of force was justified per policy.

Ease of review by command staff appears to be the primary reason for copying videos to DVD's. For example, in some instances where more than one officer is involved in use of force, it may be cumbersome to locate all the separate videos in the system and review them individually. The system allows only supervisors, detectives or APD command staff to copy a video segment from Arbitrator to a DVD. Patrol officers are unable to copy them.

Retaining videos outside the system introduces a risk of exposure to unauthorized parties. The system includes controls to protect the videos, such as audit trails identifying users who accessed them. Video copies in DVD format sitting in plain sight can be copied and distributed, all of which cannot be traced. Although it may be cumbersome to locate and view multiple videos involving one case in Arbitrator, due to the sensitive nature of the content, accessing the videos within the system will protect the integrity and content of the videos.

The use of force form currently used by sergeants and command staff lists the CAD call number, but videos cannot be searched in Arbitrator by the CAD call number. A solution may be to amend the form to include the video file number for each applicable use of force video clip, enabling command staff to access the videos using the file numbers, eliminating the need to create DVD copies.

Additionally, as addressed in a separate section of the audit report, digital media management software may be an ideal solution to managing video evidence.

Recommendation:

17. The City Auditor's Office recommends the Arlington Police Chief, with assistance from field command staff, explore solutions that will promote review of use of force video clips within the Arbitrator system, in lieu of making DVD copies retained outside of the system.

Users are not consistently logging into the Arbitrator system

Most Arbitrator users log in to the system through a MDC (mobile data computer) in police vehicles. Arbitrator uses the City's active directory as the log in method. The same credentials used to log into the city's network are also used for Arbitrator. However, users are not consistently using given credentials to log into Arbitrator. In this event, the system uses the prior user's credentials to name video files. The video file name is system generated based on officer name and current date. The video system is designed to activate, regardless of the officer logging into the system. Common activation criteria include emergency lights, vehicle speed, breaking and microphone activation.

During review, Audit observed videos with the name "Arbitrator." These were instances where the prior user was a system administrator who had performed maintenance on the MDC unit in the police vehicle. Although it is difficult to locate and confirm instances of prior user names in videos stored

in the system, the existence of these prior user file names was confirmed by police field management when officer videos were reviewed by supervisory staff.

Police officers are instructed to log into the Arbitrator system whenever they log in to the MDC unit in the police vehicle. This is stated in the general orders manual, in the section applicable to the Arbitrator video system policy and procedures. As noted, the Arbitrator system uses the network active directory log in credentials, however, a separate log in is necessary.

It appears officers may forget to log into Arbitrator during the log in process for the MDC unit in the vehicle. In some instances, the demand of the job, such as when an officer is dispatched quickly to an incident, could contribute to not logging into the Arbitrator system. It is cumbersome to locate video files when the file is listed under another officer's name. Secondary file location criteria, such as time, day, vehicle number or a police report number needs to be utilized to locate them. In this event, standard file naming conventions are also compromised. An auto log in to the Arbitrator system during the MDC log in process can eliminate the existing condition.

Recommendation:

18. The City Auditor's Office recommends that the Arlington Police Chief require Arbitrator system administrators to seek assistance from the vendor to explore the feasibility of auto log in to the Arbitrator system when an officer logs into the MDC unit in a police vehicle.

The default guest login feature in Arbitrator configuration files needs to be terminated

A default configuration file setting in Arbitrator allows the use of any user name to be used to log into the system. It was noted that a badge number has been used as a user name, thus creating an entry in the officer name master file.

It was noted the officer master file in Arbitrator shows numerical entries, in addition to the standard last name, first initial format. Numerical values as officer names are created when the user ID field is populated with numerical values in lieu of the standard last name, first initial format during the system log in process. The user ID is utilized by the software to create the video file name, which is an automated function. Use of numerical values as a user ID has resulted in video clips with numerical values in lieu of the standard last name within the system.

As noted earlier in this report, the Arbitrator system uses the network active directory credentials for the log in process. Users should utilize the same credentials when logging into either Arbitrator or the City network. The log in credentials are used by the system to name video clips created during an officer's shift.

According to the vendor, Panasonic, the numerical entries are allowed in the user ID field during the system log in process due to a default configuration file setting. The default setting, known as the guest log in feature, allows use of any user name format, such as numerical or alpha and numerical combination. This entry is then written into the officer name master file. It appears officers have used badge numbers in lieu of the last name and first initial format during the log in process.

Inconsistency and using a non-standard ID to log into Arbitrator results in an individual officer having videos under several names, making it cumbersome to search for his/her videos. Searches will need to be completed using other parameters, such as time, vehicle number, or police beat to locate a video clip. The standard file naming conventions are also circumvented.

Recommendation:

19. The City Auditor's Office recommends that the Arlington Police Chief require Arbitrator system administrators to seek vendor assistance to correct the default system configuration setting, known as guest logging methodology, to only accept the standard last name and first initial format for user name.

Some video files used for internal investigations were not classified appropriately

Some video files used in investigations were not marked as "Internal Affairs." The naming of files as internal affairs ensures they are not accessible by any user, other than Internal Affairs Division (IAD) staff, to preserve the integrity of the video.

During a review of Arbitrator video files for file naming consistency, we noted two instances where video files should have been classified as "Internal Affairs" but were not. These involved officer shootings. In one case, there were about 17 files not marked appropriately. At the time of the review, there was a total of approximately 78 video clips in Arbitrator marked as Internal Affairs.

It is necessary that video clips related to an Internal Affairs review be classified as such. If properly classified, the Arbitrator system prevents access to the video evidence to all system users, except IAD staff. This system feature is intended to preserve the integrity of the video evidence and the confidentiality of the investigation. These files are marked as Internal Affairs by police field management or by Internal Affairs staff when the investigative process begins. The system also prevents copying of the video by users, such as supervisors and command staff, who by default have the authority to view and copy videos in the system.

The exceptions noted during the review appear to be instances of oversight, considering most of the video clips used in investigations were marked appropriately.

Recommendation:

20. The City Auditor's Office recommends the Arlington Police Chief require that Police Field Management and Internal Affairs staff consistently mark video files used for investigative purposes with appropriate Internal Affairs designation.

Digital Media Management Software is necessary

Software, capable of managing video evidence and non-video evidence, using a case number is necessary. The need is even greater with the introduction of body worn camera software.

The APD lacks the ability to manage digital media, such as video and non-video evidence, under a particular case number in an electronic format. The following was observed.

- A large volume of video evidence, associated with use of force by police officers, is copied and stored on DVDs outside of the Arbitrator system. These DVD copies are used by command staff to assess if use of force was justified.
- A large volume of video evidence in a DVD copy format, provided by 3rd parties associated with a crime or incident, is retained manually in file cabinets. The 3rd party evidence includes that provided by grocery stores and private citizens' surveillance videos, resulting from their witness of a crime.
- The current introduction of body camera video software will provide a large volume of video evidence associated with officer activity. This new video evidence will be associated with other video media generated from Arbitrator in-car camera software, as well as evidence provided by 3rd parties. In the absence of digital media management software, this video evidence will be stored separately without the ability to manage them, under a case number, in one medium.

Digital media evidence is intended to be stored electronically. Electronic media, such as Arbitrator software, offers security, audit trails and the tracking of user activity associated with the video files. The City of Arlington receives and utilizes video evidence from 3rd parties, as well as videos stored in varying systems like in-car camera software and body camera software. The ability to gather, store and track evidence by case number, along with needed internal controls such as audit trails, activity logs, and access controls in one medium is desirable.

The new body camera software is in an MP4 video format. The software used is Availweb by Utility Associates of Georgia. The body camera video, along with the in-car camera video and 3rd party supplied videos, will need to be submitted as evidence. Thus, a platform to accommodate the various video sources, based on a case number or other criteria, along with non-video evidence (e.g. police reports), becomes a priority.

The current media software is not capable of storing different video formats and non-video evidence within Arbitrator. Funding for media management software has not been provided to the APD.

Video media is expected to increase greatly after the body camera software is introduced. The APD is at a point where manual storing and cataloguing of evidence will become an impossible task due to

sheer volume. The risk of human error, (e.g. evidence is excluded from manual cataloguing) is high. Requests for open records are also expected to rise with the introduction of body camera software. Meeting open records compliance criteria, along with meeting customer service and response time requirements, will also be challenging under manual evidence storage methods. Alternatively, responding to open records requests will be easier if evidence can be found in one medium.

Recommendation:

21. The City Auditor's Office recommends that the Arlington Police Chief seek necessary resources to obtain digital media management software, needed to effectively manage video media (along with non-video evidence) from varying sources, based on a case number or other criteria, in one medium.

POLICE IN-CAR CAMERA TECHNOLOGY APPLICATION CONTROLS AUDIT
AUDIT RECOMMENDATIONS AND MANAGEMENT'S REPSONSE

	AUDIT RECOMMENDATION	CONCUR/DO NOT CONCUR	MANAGEMENT'S RESPONSE	RESPONSIBLE PARTY	DUE DATE
1.	The City Auditor's Office recommends that the Arlington Police Chief require staff to update current Arbitrator policy and procedures to reflect current video evidence submission methodology and provide detailed guidance on use of vehicles with malfunctioning Arbitrator video equipment.	Concur	APD Command Staff will revise General Orders 209.00 Equipment, Appendix B: Mobile Digital Video Recording Equipment, to provide thorough procedures for submitting video evidence and direction on the use of vehicles with malfunctioning Arbitrator video equipment. The Police Department intends to replace the current Arbitrator video equipment in Fiscal Year 2019 with its body-worn camera vendor's in-car video system to streamline the digital evidence submission processes and reduce the volume of age-related malfunctioning video equipment.	APD Research & Development Manager	7/1/2018
2.	The City Auditor's Office recommends the Arlington Police Chief develop detailed policy and	Concur	The System Administrators of the in-car camera system will develop detailed policy and procedures	APD Research & Development Manager	7/1/2018

	procedures that address system access requirements.		that address system access requirements.		
3.	The City Auditor's Office recommends the Arlington Police Chief require system administrative staff maintain documentation of system access requests and management approval.	Concur	The System Administrators of the in-car camera system will create a formalized process and log for user account creation, modification, and termination requests.	APD Research & Development Manager	4/1/2018
4.	The City Auditor's Office recommends the Arlington Police Chief ensure Arbitrator system administrators review current generic system access profiles and limit the number of these accounts, based on job needs.	Concur	The System Administrators of the in-car camera system will audit and remove nonessential generic user accounts and will keep thorough documentation for generic user accounts that must remain.	APD Research & Development Manager	5/1/2018
5.	The City Auditors Office recommends the Arlington Police Chief require that Arbitrator system administrators terminate software access profiles within a specified time from the date of termination, and coordinate notification of terminations from the Lawson Human Resource system, with assistance from the City's Human Resources Department.	Concur	The System Administrators of the in-car camera system will work with Human Resources to automate termination notifications from Lawson and will establish procedures with checks to ensure in-car camera system user accounts are disabled, and purged if possible, at the appropriate date and time.	APD Research & Development Manager	4/1/2018
6.	The City Auditor's Office recommends that the Arlington Police Chief require Arbitrator software system administrators eliminate dual	Concur	The System Administrators of the in-car camera system will reconcile all user accounts with Lawson, purge unneeded	APD Research & Development Manager	7/1/2018

	profiles when making employee name changes and review access profiles periodically to identify and correct any access profile anomalies.		accounts, and will ensure the new procedures for user account modifications adequately address name change requests.		
7.	The City Auditor's Office recommends the Chief Information Officer establish network termination standards based on Citywide data security and require that network administrators terminate network access for departing city employees within established time intervals.	Concur	A security policy has been published containing expectations for COA IT network disablement and termination corresponding to an employee's departure from the organization.	Chief Information Officer	3/1/2018
8.	The City Auditor's Office recommends the Arlington Police Chief, in collaboration with the Information Technology Department, initiate request for additional communication from IT regarding the status of terminated employees' network deactivation and/or identify methodology for validating that active directory user account has been deactivated.	Concur	The Police Department's System Administrators will validate that terminated Police Department personnel's Active Directory user accounts are disabled at the expected time via the Active Directory Users and Computers console.	APD Research & Development Manager	4/1/2018
9.	The City Auditor's Office recommends that the Arlington Police Chief require Arbitrator system administrators test and document the current disaster recovery plan to ensure recovery time and the recovered system meets operational needs; and expand backup to 90 days	Concur	The Arbitrator System Administrators will work with the IT Department's Server Support Team to further protect the Arbitrator system's data, and to perform a full disaster recovery test if hardware and software allow. Due to the cost of	APD Research & Development Manager IT Supervisor – Server Support	9/1/2018

	for all Arbitrator video files to meet compliance requirements in the event of recovery after a total system loss.		expanding the backup of video files by current and standard practice, the Arbitrator System Administrators will work with the IT Department to seek alternatives. The Police Department intends to replace the Arbitrator video equipment in Fiscal Year 2019 with its body-worn camera vendor's in-car video system that operates as a Software-as-a-Service hosted on the Amazon Web Services secure cloud platform.		
10.	The City Auditor's Office recommends that the Arlington Police Chief require Arbitrator system administrators to monitor system reports and initiate corrective action for software update failures, with vendor assistance in a timely manner.	Concur	The Arbitrator System Administrators will improve its response to system notifications. Most of the software update failure alerts generated by the Arbitrator system are due to the attempts to install updated software on outdated hardware. The Police Department intends to replace the Arbitrator video equipment in Fiscal Year 2019 with its body-worn camera vendor's in-car video system that operates as a Software-as-a-Service and provides updated and compatible hardware throughout the established service agreement.	APD Research & Development Manager	12/31/2018

11.	The City Auditor's Office recommends that the Arlington Police Chief utilize Wi-Fi hotspots for Arbitrator in-car camera video file uploads, that can be installed in Police facilities and other key City facilities, to reduce the burden posed by large video file data transfers to the mobile wireless network.	Concur	The Police Department intends to replace the Arbitrator video equipment in Fiscal Year 2019 with its body-worn camera vendor's in-car video system that utilizes both mobile broadband and Wi-Fi access points in its communication architecture. The IT Department and Police Department have already deployed this infrastructure with the Body-Worn Camera Program. The Police Department does not wish to invest in IT infrastructure for the Arbitrator System it hopes to replace.	APD Research & Development Manager	12/31/2018
12.	The City Auditor's Office Recommends that the Arlington Police Chief require the Police Legal staff, with assistance from FOIA system administrators, to formulate a letter template that can be sent to a citizen when staff believes the search, research and providing of documents will exceed the 10 business day period the State law requires.	Concur	The Police Legal Division reports to the City Attorney's Office, not the Police Department. Per the City Attorney's Office, sending a letter is not a legal requirement and the Police Department is compliant with the Public Information Act. Requestors are most often contacted by staff via phone when there is a delay in processing their request, so more individualized information can be provided, and any questions can be answered. However, FOIA has been updated to automatically notify the requester of the status of their request on the 10th business day. It is our intent to amend the	Police Legal Advisor	2/1/2018

		automated response to include more information related to the expected time frame records will be available based upon the status.		
13. The City Auditor's Office recommends that the Arlington Police Chief conduct a resource assessment in the Police Legal Division to ensure there is adequate personnel and redaction software for current and future needs.	Concur	The Police Legal Division is not part of the Police Department. The City Attorney's Office manages the Police Legal Division. With the rollout of body-worn cameras that is in progress, Police and the City Attorney's Office are assessing if current staffing levels and software are adequate.	Police Legal Advisor, City Attorney's Office APD Management Services Bureau	12/31/2018
14. The City Auditor's Office recommends that the Arlington Police Chief allocate adequate resources to review aging Arbitrator video files for retention compliance periodically, and purge files based on expiration, as established by retention laws and operational policies.	Concur	The Police Department intends to replace the Arbitrator video equipment in Fiscal Year 2019 with its body-worn camera vendor's in-car video system. APD plans to decommission the Arbitrator system after the department has transitioned to the new in-car camera system. Once APD appropriately protects its digital media evidence in an alternate location, the Arbitrator system will be decommissioned and destroyed. The new in-car camera system and body-worn camera system has an improved classification and retention process, and APD will have a recurring process to review video	APD Research & Development Manager	9/27/2019

			files for retention compliance to ensure its keeping evidence as required and expected.		
15.	The City Auditor's Office recommends that the Arlington Police Chief require that Arbitrator system administrators seek to expedite a permanent resolution of the MK2 video recording unit issue.	Concur	The Police Department intends to replace the Arbitrator video equipment in Fiscal Year 2019 with its body-worn camera vendor's in-car video system that operates as a Software-as-a-Service and provides updated and compatible hardware throughout the established service agreement.	APD Research & Development Manager	12/31/2018
16.	The City Auditor's Office recommends the Arlington Police Chief require that the Arbitrator system database administrator, in coordination with system administrators, update the equipment master file, to include only equipment currently in use, and use the system notifications as intended.	Concur	This will be completed.	APD Research & Development Manager	6/1/2018
17.	The City Auditor's Office recommends the Arlington Police Chief, with assistance from field command staff, explore solutions that will promote review of use of force video clips within the Arbitrator system, in lieu of making DVD copies retained outside of the system.	Concur	The Arlington Police Department is updating its process and procedures to handle the volume of digital media evidence generated by in-car cameras and body-worn cameras. The replacement of the Arbitrator System with the solution provided by APD's body-worn camera	APD Research & Development Manager	12/31/18

			system will streamline the review process.		
18.	The City Auditor's Office recommends that the Arlington Police Chief require Arbitrator system administrators to seek assistance from the vendor to explore the feasibility of auto log in to the Arbitrator system when an officer logs into the MDC unit in a police vehicle.	Concur	The Arbitrator system is automatically passing through the Active Directory credentials, but the officer must enter the vehicle's unit number to complete the login process. APD intends to replace the Arbitrator system with its body-worn camera vendor and expects an improved login process with the new system.	APD Research & Development Manager	12/31/2018
19.	The City Auditor's Office recommends that the Arlington Police Chief require Arbitrator system administrators to seek vendor assistance to correct the default system configuration setting, known as guest logging methodology, to only accept the standard last name and first initial format for user name.	Concur	This will be completed.	APD Research & Development Manager	6/1/2018
20.	The City Auditor's Office recommends the Arlington Police Chief require that Police Field Management and Internal Affairs staff consistently mark video files used for investigative purposes with appropriate Internal Affairs designation.	Concur	This will be completed.	APD Internal Affairs	7/1/2018

21.	The City Auditor's Office recommends that the Arlington Police Chief seek necessary resources to obtain digital media management software, needed to effectively manage video media (along with non-video evidence) from varying sources, based on a case number or other criteria, in one medium.	Concur	The Police Department intends to replace the Arbitrator System with the in-car camera solution provided by its body-worn camera vendor. The vendor markets their platform as a digital evidence management system and includes case management features. The department is working toward using this solution as its digital media management software and will determine if there are any gaps.	Assistant Chief of Support Operations APD Research & Development Manager Commander of Internal Affairs Division	12/31/18