Minneapolis
City of Lakes

Minneapolis Police Department Mobile and Body Worn Video Recording Equipment Program Audit

City of Minneapolis – Internal Audit Department
September 19, 2017

Contents Page

Internal Audit Department
350 South 5th Street, Suite 302
Minneapolis, MN 55415-1316
(612) 673-5938

Date: September 19, 2017

To: Audit Committee, Mayor Betsy Hodges, City Council Members, Chief of Police Medaria Arradondo

Re: Minneapolis Police Department Mobile and Body Worn Video Recording Equipment Programs Audit

Findings Summary

Finding 1 – Policy noncompliance

During the review, a number of instances of non-compliance with BWC policy were noted, including:

- Some officers (e.g. SWAT) were not being required to use BWCs, even though policy required their use.
- Some 911 dispatches and use of force events did not have corresponding BWC video in evidence.com. Where video did not exist, there was inconsistent entry of an explanation why in CAD or CAPRS.
- Officers were not consistently running BWC start-up checks, and doing some start-up checks away from precinct.
- Officers were occasionally leaving BWCs powered off until just before activation, preventing pre-event recording from fully functioning.
- Officers transporting individuals to jail frequently deactivated BWCs prior to transferring custody. This was also observed with MV videos.
- Officers were not consistently narrating the reason for BWC deactivation prior to event conclusion.
- Officers were not consistently categorizing BWC videos, including not assigning any categories and assigning incorrect categories.
- Officers were not consistently entering the correct case numbers related to BWC videos.
- Officers were not consistently uploading BWC videos at the end of their shift.
- Supervisors were not conducting reviews of BWC use, and supervisors were not trained on conducting reviews until June 2017.

Finding 2 – Policy completeness and clarity

- The BWC policy focused on MPD's use of the camera equipment and software. A BWC program encompasses more than just equipment and software use, and the State Statute had requirements that went beyond what was included in the MPD policy. The following areas were not completely addressed in policy:
    - Connection of statute-required data classifications to categories used by MPD.
    - Some categories used were not addressed in the policy.
    - Addressing security breach notifications and security safeguards.
    - Addressing notices to data subjects.
    - Addressing authorization to access data, and access procedures.

- Addressing videos classification assignment (public/non-public, etc.)

- In addition to State Statute compliance gaps, certain areas of policy could be clarified, or enhanced to provide more information and guidance:
  - The BWC policy allowed turning off cameras when necessary to discuss issues in private, but did not provide guidance for what a necessary circumstance was.
  - The BWC policy does not address using multiple categories for videos.
  - The BWC program allowed for retention of training videos for only 90 days, when the next shortest period was one year.
  - Additional information on redaction and withholding of subject and offensive information to fully cover compliance with state statutes.
  - Additional information on data retention to fully cover compliance with state statutes.
  - Ability to access data by subjects of the data, and notification to data subjects.

Finding 3 – Body Worn Camera Systems Access

- Multifactor authentication was not required for all users of evidence.com.
- Evidence.com access control procedures were not documented.
- Written approvals were not obtained prior to provisioning user access to evidence.com, as required by state statute.
- There was no periodic access review process.
- One user with administrative access did not need that level of access for their current job.

Finding 4 – Managing Data Requests

- Requests for BWC data from law enforcement and data subjects were not centrally managed and not uniformly documented. To ensure a complete, documented population of all requests exists MPD enhance the data sharing process by routing all data requests through a centralized group, such as the Records Information Unit, and limiting the ability to share data to that group.

Finding 5 – Training

- Written training materials did not cover some aspects of the BWC policy, including specific steps to take when equipment malfunctions, notifying supervisors of video with administrative value and using BWCs in conjunction with MV systems.

Finding 6 – Mobile Video Systems Access

- The vendor contracted by the City to administer its network and servers had administrative access to the server that stores unarchived MV data. While the vendor needed administrative access, the City should monitor the activity of the vendor on this server when access is made.

Background

The Minneapolis Police Department (MPD) used body-worn cameras (BWCs) and mobile video systems in police squad cars (MVs) to capture video and audio data of events.

Body Worn Cameras

- Minnesota had state statutes that include requirements the MPD must comply with as it operates its BWC program, including a required independent biennial audit.
- MPD used BWCs from Axon to capture video and audio data and Axon's cloud-based software, evidence.com, for data management.
- MPD had an established BWC policy and trained staff on how to use BWCs and the evidence.com software. The policy was updated effective July 29, 2017, to clarify and expand when activation of BWCs was required, and throughout the report some data is representative of the 'old' or 'new' policy.
- Officers issued BWCs were to use them during their shifts and approved uniformed off-duty work in line with policy.

Mobile Squad Video

- MV programs did not have specific state statutes governing their operation.
- MPD used a system from the vendor, L3 Mobile Vision, to capture video and audio data, and L3's software to manage data.
- MPD had established MV policies and trained staff on how to use the MV software.
- Officers working in cars equipped with MV systems were to use them during their shifts in line with policy.

I. Body Worn Camera Program Audit Results and Recommendations

A. BWC - Minnesota Statutes

The mobile and body-worn camera programs (programs) are regulated directly by MN State Statutes 13.825 PORTABLE RECORDING SYSTEMS and 626.8473 PORTABLE RECORDING SYSTEMS ADOPTION; WRITTEN POLICY REQUIRED. Further, the programs have additional statutory requirements that the aforementioned statutes refer to, which include MN Statutes (626.553 sub 2, 609.02 sub 7a, 13.82 sub 7 & 17 & 17a, 13.43 sub 2, 13.04 sub 2, 138.17, 13.08, 13.05 sub 5, 13.055) and the US FBI Criminal Justice Information Services (CJIS) Division Security Policy 5.5.

MN Statutes were broken down into 56 unique criteria within the following categories:

- Data classification, redaction, retention, protection and breach notification
- Authorization to access data and access by data subjects
- Sharing among agencies
- Inventory of portable recording system technology
- Use of agency issued portable recording system technology
- Security assessments and biennial audits
- Notification to Bureau of Criminal Apprehension (BCA)
- Portable recording system vendor
- Notice
- Public comment

Of the 56 unique criteria, 16 failed and 40 passed. Of the 40 unique criteria that passed, 17 should be enhanced.

Compliance with State Statutes

Compliance with state statutes is discussed throughout the report. Since the report covers other scope areas, the results of compliance with state statutes are summarized here.

The following were groupings of <u>non-compliance</u> with state statute requirements:

- Policy Gaps
  - Data classification (record type)
  - Security breach notification and security safeguards
  - Notice to data subjects
- Authorization to access data, and access procedures
- Videos classification assignment (public/non-public, etc.)

The following were groupings where <u>controls were compliant, but enhancements to the program are recommended</u>:

- Policy Enhancements
  - Redaction and withholding of subject and offensive information
  - Data retention
  - Access by subjects
  - Notification to data subjects
- Process Enhancements
  - Data requests, sharing and release of information

B. BWC - Equipment and Software

This section addresses the technology aspects of the audit, including features of the platform and devices, external attestations, testing details, and issues identified. The company that supplied body camera technology and services to the City of Minneapolis is Axon Enterprises, formerly TASER. The devices deployed in the field were primarily Axon Body 2, with some Axon Flex and a few older models accounting for a small percentage of deployed devices. Evidence.com was the online cloud platform owned by Axon and was used to view captured data, manage devices and control access to all users. As of 9/1/17, there were 582 users with active body cameras deployed under the City of Minneapolis' instance of evidence.com.

Equipment

Limited testing of the hardware and internal components was performed during the scope of this audit. The Axon Body 2 devices had an on/off switch enables power to the device, and a large center button to activate recording. Per the device configuration, when a camera is recording, an LED indicator recording light is obvious to all parties with visibility to the body camera. The device supports a pre-event buffer which, and as long as the device is powered on, will record up to a two-minute buffer (with or without audio). This allows for events leading up to the activation of a camera to be captured. The pre-event buffer was set to 30 seconds and audio was set to mute (i.e. no audio recorded on the pre-event buffer).

Other features of the Axon Body 2 devices included: the ability for remote activation of a camera (ex. turning on squad car lights, or removing weapon from holster); weather resistance (IP67 certified); non-removable internal storage; GPS support for identifying where an incident occurred; smart phone integration; and battery capacity large enough to provide power to the device for standard usage. Battery capacity was impacted by usage (how frequently the camera is turned on), pre-event buffer (if enabled or not), video quality, and ambient temperature.

Data captured by the devices are stored encrypted at rest (CJIS Compliant, NSA Suite B 256-bit AES encryption) on internal storage. Data is only extracted from the device when inserted into an Axon Docking station, which has a proprietary connection port. Once a camera is docked, a FIPS 140-2 cryptographic software module handles secure key management, data integrity and secure communications (TLS 1.2 implementation with 256-bit connection, RSA 2048 bit key and Perfect Forward Secrecy) from the docked camera to cloud storage. The FIPS 140-2 cryptographic module was validated on 4/6/17 per the National Institute of Standards and Technology (NIST) government website. Body cameras are linked to an evidence.com instance (i.e. City of Minneapolis unique account); when a camera is docked, the data is automatically uploaded, and only accessible by users of the instance linked to the camera, supervisors and administrators.

Software

The evidence.com platform runs on the Microsoft Azure CJIS Compliant Cloud Environment. The application and data are logically isolated from other clients. The evidence.com platform and employees of Axon self-attest compliance with the CJIS Security Policy 5.5 and a CJIS Whitepaper is available on their website. An external SOC2, type II (covering security and availability) attestation for period of 1/1/16 through 9/30/16 was conducted by EY and was reviewed during this audit.

Finding:
- Multifactor authentication was not required for all users.
- Access Control procedures were not documented.
- Written approvals were not obtained prior to provisioning users' access to evidence.com.
- There was no periodic access review process.
- One user with administrative access did not need that level of access for the current job.

Evidence.com is used to access the data collected by the

body cameras, and all system and device configurations. Access to the platform is granted via a user ID and password, multifactor authentication is required for administrators, multifactor authentication is not required for non-administrative roles. Multifactor should be enabled for all user accounts due to the nature of cloud platforms being accessible via the internet. Whitelisting of IP addresses is an available feature of evidence.com not currently utilized that would only allow access to the platform from approved IP addresses.

User Access is provisioned by the Minneapolis PD Business Technology Unit (BTU). Training is required per the MPD BWC Policy prior to being issued a body camera. Formalized Access Control procedures haven't been documented, including a process for periodic access reviews. Written access approvals were not captured for users of the system, which is mandated by state legislation.

Evidence.com features role-based access controls to allow or deny users access to features and functions. The standard role issued to officers limits their access to viewing their captured data and other data that has been shared with them. Supervisors have the ability to view all recorded data as they are responsible for reviewing data captured by officers and ensuring compliance with policy. Administrators have full access to all system functions, with the exception of accessing restricted data. Additional roles exist and were reviewed during the audit for appropriateness. Manual deletion of data is limited to the administrator role, there is a deletion workflow to confirm videos being deleted manually and videos up for deletion based on the record retention schedule. Testing identified one manually deleted file done by a system administrator. The Internal Audit Department recommends that manual deletion be prohibited.

Video redaction, the process of obfuscating portions of the video recordings, is a feature of the evidence.com platform. Redaction is performed by the Records Information Unit (RIU) and access to the redaction section of evidence.com is limited. Redacted videos never alter the original file; a copy is always made to retain the integrity of the original data. All videos and data stored on evidence.com have a SHA2 hash, which is essentially a digital fingerprint to ensure data has not been modified. Any redacted videos will have a different SHA2 has value compared to the original.

Finding:
- All data requests should be routed through the RIU to ensure a complete, documented, population of all requests exists.
- Consider limiting the ability to share data to the RIU.

Sharing of videos is also supported by the platform. Users with the appropriate access rights have the ability to share data to users who request data. Data can be exported to fulfill requests outside of the evidence.com system.

The data retention schedule is determined by assigning a 'Category' to each video. Videos without an assigned category will be retained indefinitely. When data is at the end of the data retention period it is moved into the deletion workflow, where it can be reviewed prior to automated deletion. It was observed during the audit that the data categories configured in the system don't align to data classifications, which is a requirement per the state legislative requirements. From 7/1/16 to 7/28/17, 11% of videos were not assigned a data category, and 5% were not assigned a category from 7/29/17 to 8/23/17. All videos should be assigned a data category and this should be enforced through the supervisor review process.

Finding:
- All videos were not assigned a data category.
- The MPD BWC policy did not have a data classification associated to each data category.
- The retention period for the 'Training' video category was only 90 days, and could be increased to one year.
- Not all configured data categories in evidence.com were documented in the MPD BWC Policy.

Detailed reporting and tamperproof audit logs are available. The reporting allows detailed analysis on usage and compliance to state or department policies.

C. BWC - Policy

MPD's Policy and Procedure Manual is organized by volumes that cover topics such as Department Management, Administrative Procedures, Code of Conduct and the Use of Force, etc. The BWC policy is included in the Administrative Procedures volume under the 4-200 policy series that covers Equipment and Supplies. The initial BWC policy (#4-223) was issued on 6/29/16 and updated on 7/29/16. State statutes governing BWC systems were first effective 8/1/16, with a requirement for the MPD to have a policy by 1/15/17.

MPD's policy contains sections that cover, to varying degrees, the following:

- Officer and supervisor responsibilities
- Activation and deactivation requirements
- Data access, retention and duplication rules
- Critical incident protocol

The BWC policy, as written is primarily focused on MPD's camera and software use, and does not include all aspects of a BWC program. The following is a list of BWC program aspects that we found to be inadequately addressed in the MPD's BWC policy:

Finding:
The MPD BWC Policy was not comprehensive and did not include all aspects of a City-wide BWC program.

- Roles and responsibilities (within MPD and other departments)
- Statutory requirements (addressed in section I)
    - Data classification, retention and access
    - Equipment & system inventory and usage
    - Authorization to access data & sharing among agencies
    - Biennial audit
    - Notifications to BCA
    - Vendor requirements
    - Penalties for violation
- Training, equipment issuance & software access provisioning
- Camera use & related software documentation expectations
- Supervisor responsibilities
- Data request intake and fulfillment
- Data destruction
- Monitoring, oversight, reporting and analysis

As MPD develops the BWC program, additional aspects may be identified that the City should include in the BWC policy.

The review of State Statutes identified gaps in the current BWC Policy that need to be addressed to be in full compliance.

- State Statute lists a number of classifications which should be addressed by policy. Classification of data is nonpublic in most cases, but is public if it documents the discharge of a firearm, if it documents the use of force that results in substantial bodily harm, or if the subject of the data requests that it be made accessible to the public. The BWC policy also does not state that the Tennessen warning does not apply to data.

Finding:
The BWC policy did not address classification of data in line with State Statute requirements.

- The BWC policy does not connect these classifications with how it currently labels videos with various categories. The policy should map state-required classifications to categories.

- In cases of a data breach, the City act in accordance to State Statutes governing data breaches in disclosing the breach, notifying affected individuals and reporting to other agencies. The BWC policy does not address what needs to happen in case of a data breach.
- The BWC policy should include procedures for the secure storage of portable recording system data and the creation of backup copies of the data.
- The BWC policy should include procedures to ensure compliance and address violations of the policy, which must include, at a minimum, supervisory or internal audits and reviews, and the employee discipline standards for unauthorized access to data contained in section 13.09.
- The BWC policy should include circumstances under which a data subject must be given notice of a recording;
- The BWC policy should include the requirement that written authorization is required to access BWC data. The list of individuals with access was updated for terminations, but did not undergo a periodic review.

Finding:
BWC policy did not address a number of elements discussed by State Statutes, including security notifications, security safeguards, notices to data subjects, authorizations to access data and access procedures.

The review of State Statutes also identified areas in the BWC policy that could be enhanced to provide clarity and improve compliance.

- The process for redaction and withholding of video subjects, and of offensive information, was not covered in the policy.
- That data destruction was in compliance with state statute was not specifically listed.
- The process for how data can be requested to be retained and accessed by the subject of the data was not covered, and various notification requirements in such cases was not discussed.

Finding:
The BWC policy can be enhanced by including more information on how redaction and withholding of information occurs, that data is destroyed in line with state requirements, and information on the rights of subjects of data and the City's obligation to them.

Other deviations from, or unaddressed topics in the policy include:

- The SWAT teams were not using BWCs. The policy stated BWCs should be worn when reasonably anticipating activation could be required.
- BWC policy stated that supervisors were to review videos, but no records of reviews were available, and training on conducting reviews first occurred in June 2017.
- BWC policy allowed officers to turn off cameras when it was necessary to discuss issues in private, but the policy did not provide details or examples of allowable circumstances.
- Occasionally officers remove a BWC while it is on; policy does not speak to circumstances where it is appropriate to remove cameras.

Finding:
Portions of the BWC Policy discussing use by all officers (e.g. SWAT) and supervisor reviews were not being followed. Other portions of policy were unclear, or provided little guidance to officers. MPD needs to enforce the policy or modify it to encompass these practices, and should provide clearer definitions of when BWCs must be worn, used, and deactivated.

- Certain videos may be related to multiple video categories; the policy and training should address multiple categorization of video, audio, photographs and any other form of information collected through the mobile video recording devices.

Potential problems that may arise based on the policy include off-duty camera use. Officers that are issued cameras are required to use those cameras for approved off-duty work. If during that off-duty work they capture any audio or video regarding use of force by or against the officer or data that may be used in a criminal case, the data shall be uploaded in the same manner as if the data had been collected while on duty. Taking the BWC back to the station for uploading will also charge the camera for the next shift. For all other cases the policy allows the officer to upload the video as soon as practical. If officers that use the cameras for off-duty work don't charge their devices, which take up to ten hours to fully charge, they may not have enough battery power to operate through their next shift.

D. BWC - Training

A training program was established and executed during the roll-out of the cameras to officers. The training covered the use of the cameras and the associated software, evidence.com. Cameras were not provided to officers until they completed the training and attendance records were maintained.

We compared the policy to the training materials to determine how comprehensive the training program was. Training was in line with the BWC policy, but there were three attributes in the policy that weren't covered in the training materials.

- Officers removing themselves from service when experiencing loss of battery power, and notification to supervisor and MPLS Emergency Communications Center of removal from service
- Notification to supervisors of any recorded event believed to be of value for administrative review
- Use of BWC in conjunction with Mobile Video Recording equipment (squad cameras)

Finding:
Written training materials did not cover some aspects of the BWC policy, including specific steps to take when equipment malfunctions, notifying supervisors of video with administrative value and using BWCs in conjunction with MV systems.

As the MPD expands their BWC policy, the resulting changes should be communicated to officers and included in subsequent training programs.

E. BWC – Use and Trends

Startup testing:

At the beginning of a shift, MPD staff picked up their assigned BWC along with their other equipment. Policy required a startup check to be made to make sure the BWC is operational before they begin their work.

We measured whether staff were conducting startup videos using timesheet data and evidence.com records. 44% of days worked did not have a startup video under the old policy. This went down to 24% under the new policy.

Finding:
Some MPD staff were not conducting startup checks. This could result in entering the field with malfunctioning equipment.

We also reviewed startup videos to determine whether they were being conducted at the beginning of a shift. 10% of a sample of startup videos were not conducted at the beginning of a shift under the old policy. This went up slightly to 12% under the new policy. These videos were taken while officers were on the way to a call, or even at the end of a shift.

Finding:
Some MPD staff were conducting startup checks away from their BWC pick up location. This practice makes a startup check obsolete since a failed check would require returning to a pick up location to address a malfunctioning camera.

Activation testing:

MPD staff were required to activate body cameras in line with MPD policy. During the audit the policy changed, under the old policy activation was generally to occur during a policy-defined set of circumstances. Under the new policy, activation was generally to occur prior to a policy-defined set of circumstances. Reasons for failing to activate were required to be documented in CAD or CAPRS by dispatchers or officers.

We reviewed dispatch data and identified calls officers responded to that would require activation. We were unable to locate a BWC recording in 35% of sampled dispatch events under the old policy. This fell to not locating 29% of sampled dispatch events under the new policy. In all cases, no statement was found in CAD or CAPRS documenting why the BWC did not record the event.

Finding:
Some MPD staff were not activating their BWCs when responding to incidents or as required for use of force incidents. Staff that were not activating cameras were also not consistently creating required written explanatory statements.

We reviewed use of force events, which required activation. We were unable to locate a BWC recording in 26% of sampled events under the old policy. 59% of these instances did not have a narrative included in CAD or CAPRS explaining why the BWC was not activated. Use of force events without a recording fell to 7% under the new policy.

We reviewed whether MPD staff activated cameras prior to when an incident began. Under the old policy 16% of sampled videos did not show the start of an incident. This fell to 9% under the new policy. Use of force incidents were part of this data. Looking at use of force specifically under the old policy, 22% of sampled videos did not start prior to the use of force event and 18% were not on during the full chain of events that resulted in use of force. Under the new policy, this fell to 15% not starting prior to the use of force event, and 10% not on during the full chain of events that lead to the use of force.

BWC cameras have a pre-event recording feature that constantly captures 30 seconds of footage, but only if the camera is powered on. We observed some MPD staff keep their camera powered off, and power it on when activating the record feature. This means the full 30 second pre-event recording was not captured. 15% of sampled videos under the old policy did not have a full 30 second pre-recording This increased to 22% under the new policy.

Finding:
Some MPD staff were leaving their cameras powered off, preventing the pre-event recording feature from capturing what occurred prior to the record button getting pressed. Since not all recording begins prior to incident starts, the pre-recording feature can be critical to understanding what occurred.

Usage testing:

We reviewed how often BWCs had a clear view of the incident that was occurring. 6% of sampled videos under the old policy did not capture the incident. This decreased to 3% of sampled videos under the new policy. Use of force incidents were part of this data. Looking at use of force specifically, 16% of sampled videos did not have a clear view of the incident under the old policy. This decreased to 13% under the new policy.

There were various reasons for obscured camera views, though not enough were reviewed to identify patterns. Examples observed included BWC angles not covering the incident, BWC covered by wearer's hands or rain jackets, and BWC accidentally or intentionally detached from person.

Deactivation testing:

MPD staff deactivated the BWC manually and were to do so in line with MPD policy. If deactivation occurred prior to the end of an incident, the wearer must narrate the reason for deactivation.

Finding:
MPD staff were not consistently narrating the reason for deactivating their BWCs when deactivation was done prior to incident conclusion.

We tested how often cameras were deactivated in line with policy. Of sampled videos, 22% of BWCs were deactivated prior to an event ending under the old policy. This went down to 12% under the new policy. Of these events, 71% did not have a narrated reason for deactivation under the old policy. This went down to 50% under the new policy.

We observed a number of instances in which an individual would record multiple videos for a single event, and specifically reviewed a sample of videos taken by the same person and coded to the same case in the same day. In 33% of sampled videos under the old policy, and 35% of sampled videos under the new policy, there was no reason narrated for turning off the camera.

Finding:
MPD staff would occasionally turn off BWCs mid-incident and turn them on later without narrating the reason for deactivation.

The main reason identified for deactivating a camera was the conclusion of an incident - 69% of videos under the old policy and 77% under the new policy. The second most common reason clearly identifiable was to have a conversation with another officer – 9% of videos under the old policy and 9% under the new policy. The policy did not clearly define or provide examples of valid reasons for having a private discussion. This issue was noted as a finding in the BWC-Policy section above. For most of the remaining videos sampled the reason for deactivation is not clear.

In our sample, we observed 16 instances of transportation to jail under the old policy, and 16 under the new policy. In 81% of old policy videos the BWC was turned off while the suspect was still in MPD custody. This decreased to 75% under the new policy.

Finding:
MPD staff transporting individuals to jail frequently deactivated their BWCs prior to completing transport.

Categorization testing and case number testing:

After a video was taken, the BWC user was to categorize it and enter the CAD case number associated with the recorded event. This could be done on the go using City-issued cell phones, on some of the squad car computers, or at the end of a shift using computers at precincts.

We tested the categorization of videos by reviewing a sample of videos under different categories and verifying that the correct category was selected.

We observed that 11% of all videos were not assigned a category under the old policy. This fell to 5% under the new policy. Uncategorized videos were kept indefinitely. The below table summarizes what categories should have been assigned to the sampled uncategorized videos:

Finding:
MPD staff were not categorizing all videos as required. Categorization was required by policy, and was a way of trying to classify videos in line with MN Statute requirements

Category	Old Policy	New Policy
Significant Event	4%	0%
Non-Evidence/General Recording	39%	42%
Arrest/Evidence	27%	34%
Training	1%	0%
Startup	29%	23%
Citation	0%	1%

We observed that videos could be tagged with multiple categories, even though this was not covered in any training or policy materials. Finally, we noted that in some instances the use of multiple categories did not make sense, including 204 videos labeled as both evidence and non-evidence.

Finding:
Use of multiple categories was not addressed in policy or training.

Finding:
Various sets of videos were not consistently correctly categorized as required by policy. This included categories that have clear definitions in the policy, such as use of force, and categories that do not have clear definitions, such as arrest/evidence.

We reviewed a sample of videos categorized as Training, and noted 57% did not appear to be training under the old policy, and 56% under the new policy. Most miscategorized training videos were of officers walking or driving and should have been labeled as non-evidence instead. The training category was the only one with a 90 day retention period; all other categories were retained for a year or more.

Finding:
Many videos categorized as training were miscategorized. Training videos present a higher risk because they have the shortest retention period of 90 days.

We selected a set of non-evidence videos that were associated with cases in CAPRS and reviewed the

videos to make sure these were correctly categorized as non-evidence. Of this targeted sample, 44% were miscategorized under the old policy, and 64% were miscategorized under the new policy. Most should have been classified as arrest/evidence.

We selected a set of use of force videos based on use of force reports, and reviewed the videos to make sure they were correctly categorized as use of force. Of this targeted sample, 14% under the old policy, and 31% under the new policy, were miscategorized and did not include the use of force label. Most were labeled as arrest/evidence.

We reviewed a sample of videos categorized as Startup, and noted 1% did not appear to be startup videos under the old policy, and 3% under the new policy. The miscategorized videos included one video of an officer driving, one arrest, and one warning issuance.

MPD trained BWC users to enter the dispatch or case control number associated with each video as they categorize and upload the data. This field had a specific format that significantly eases a reviewer's ability to locate BWC data associated with a case or dispatch event. We noted 3% of videos that were definitively associated with a case or event were not labeled under the old policy, and 5% under the new policy. Some non-evidence videos also need dispatch or case control numbers, but we could not test how many of these were correctly labeled. We also noted 3% of entered case numbers were incorrectly formatted, making it harder to rely on them to correctly tie videos to dispatch or CAPRS data.

Finding:
MPD staff were not consistently labeling BWC data with dispatch or case numbers. When entries are made, some are incorrectly formatted.

Upload testing:

MPD staff were required to dock their cameras and upload all BWC data at the conclusion of their shift.

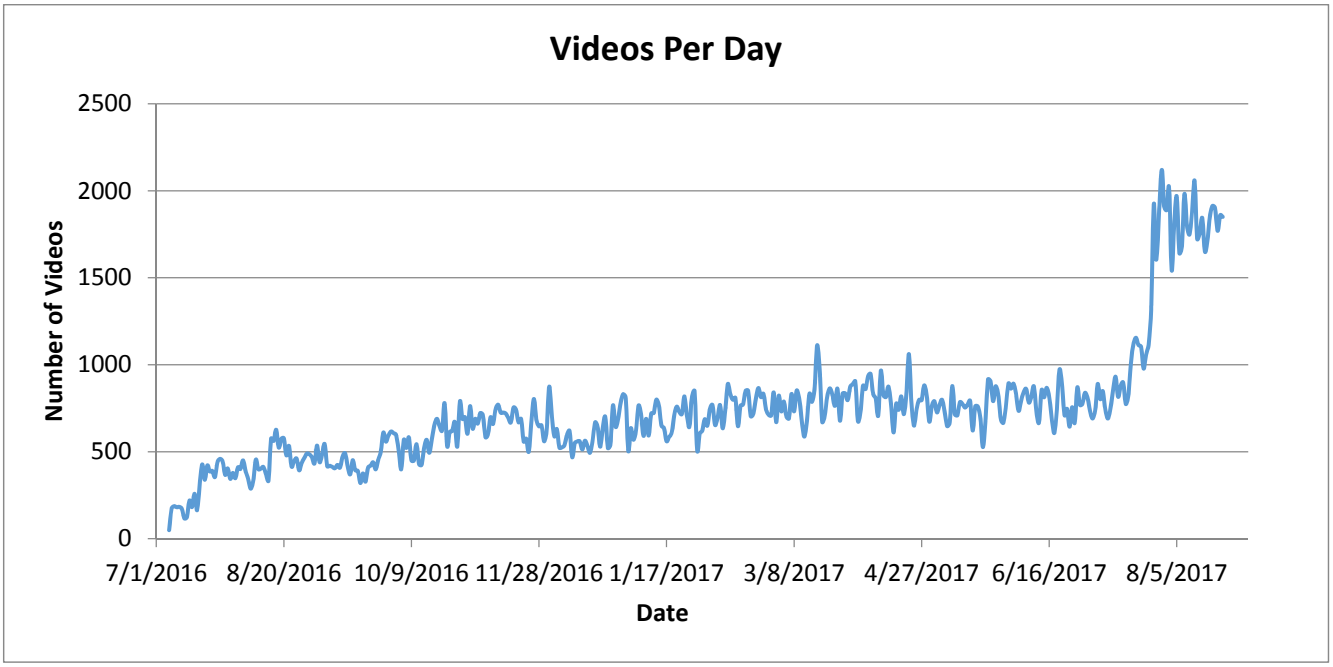
We compared the times each video was taken with the time it was uploaded to evidence.com. Most shifts are 10 hours long, so we expected an average time gap between recording and uploading to be half of a shift, or 5 hours. We observed an average time gap of 18 hours 17 minutes under the old policy. This was reduced to 10 hours 26 minutes under the new policy. We looked at individual average gaps between recording and uploading, and 23% of video owners under the old policy and 12% under the new policy had gaps greater than 30 hours. While the policy requires uploading to occur at the end of a shift, many officers work uniformed off-duty jobs. Officers going directly to their off-duty jobs prevents uploading from occurring at the end of an on duty shift and could skew these results.

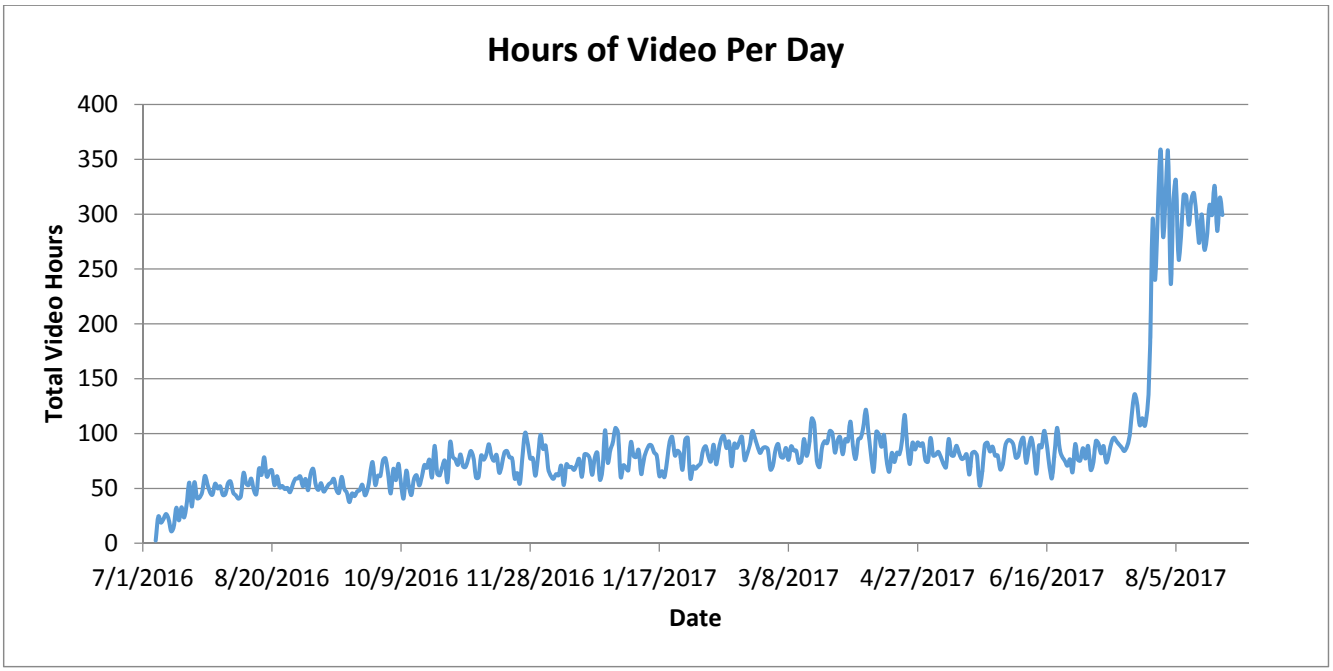
Finding:
MPD staff were not consistently uploading their BWC data at the end of their shifts.

Usage trends:

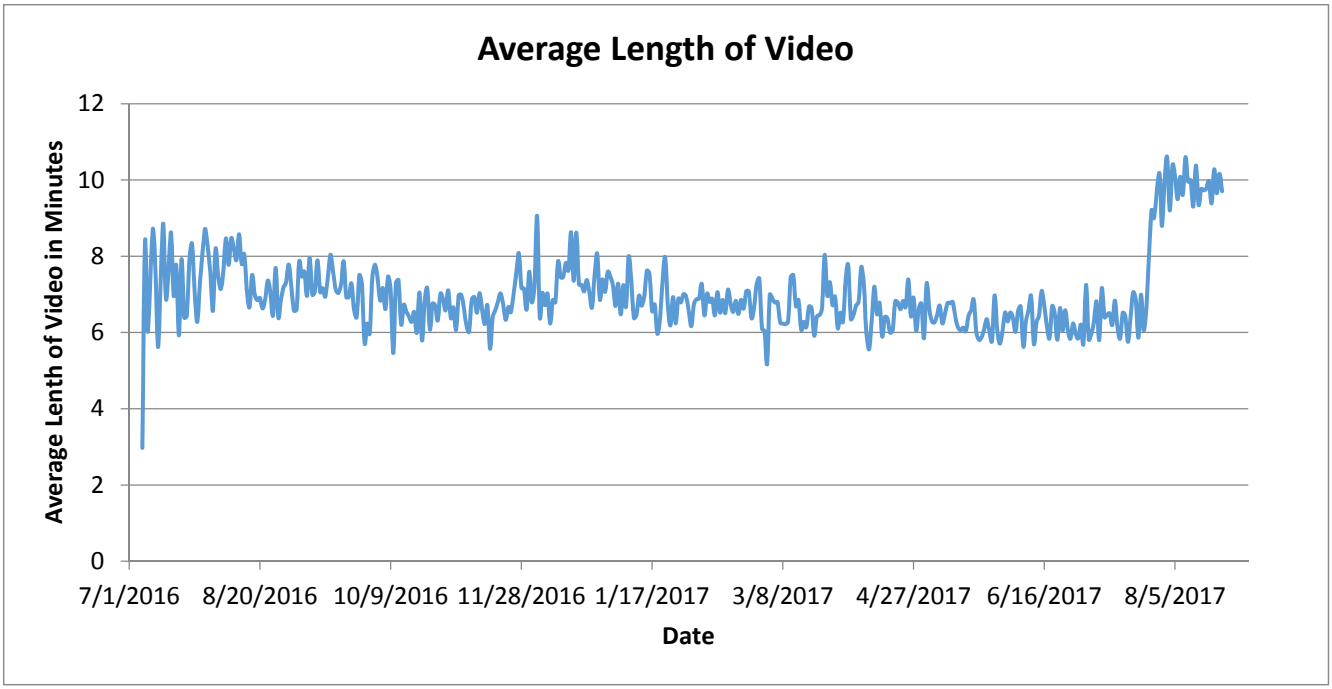
The review focused on three data sets: all videos in evidence.com, CAD dispatch data and time reported by MPD staff in the Workforce Director time reporting system. Where time reporting was used for analysis, the population was narrowed down to staff that have been issued cameras and that are working assignments in which cameras are likely to be regularly used.

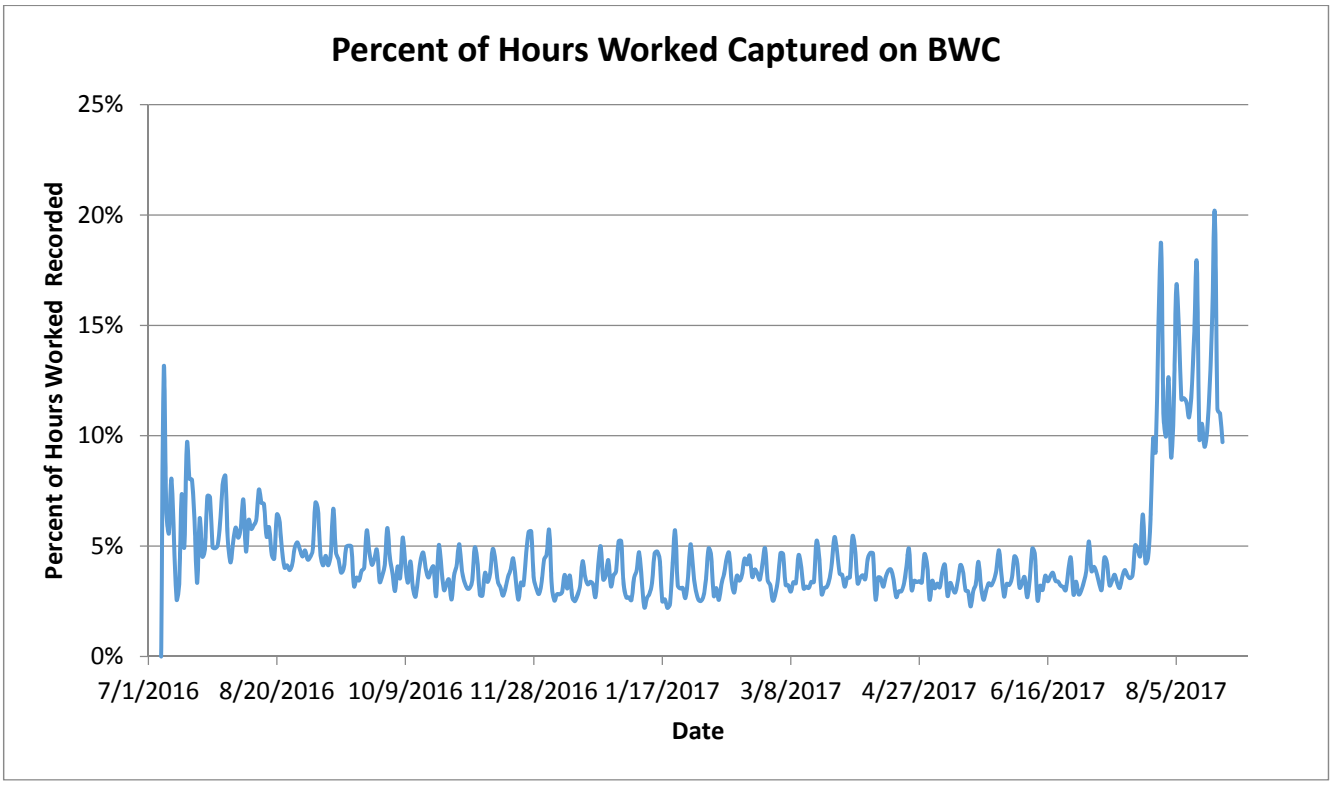
After initial training and BWC assignment, which started with Precinct 1 in July 2016 and ended with Precinct 5 in October 2016, the number of videos and duration of videos per day has stayed more or less constant until the new BWC policy went into effect 7/29/17. The new policy significantly increased the number of videos, and the duration of videos.



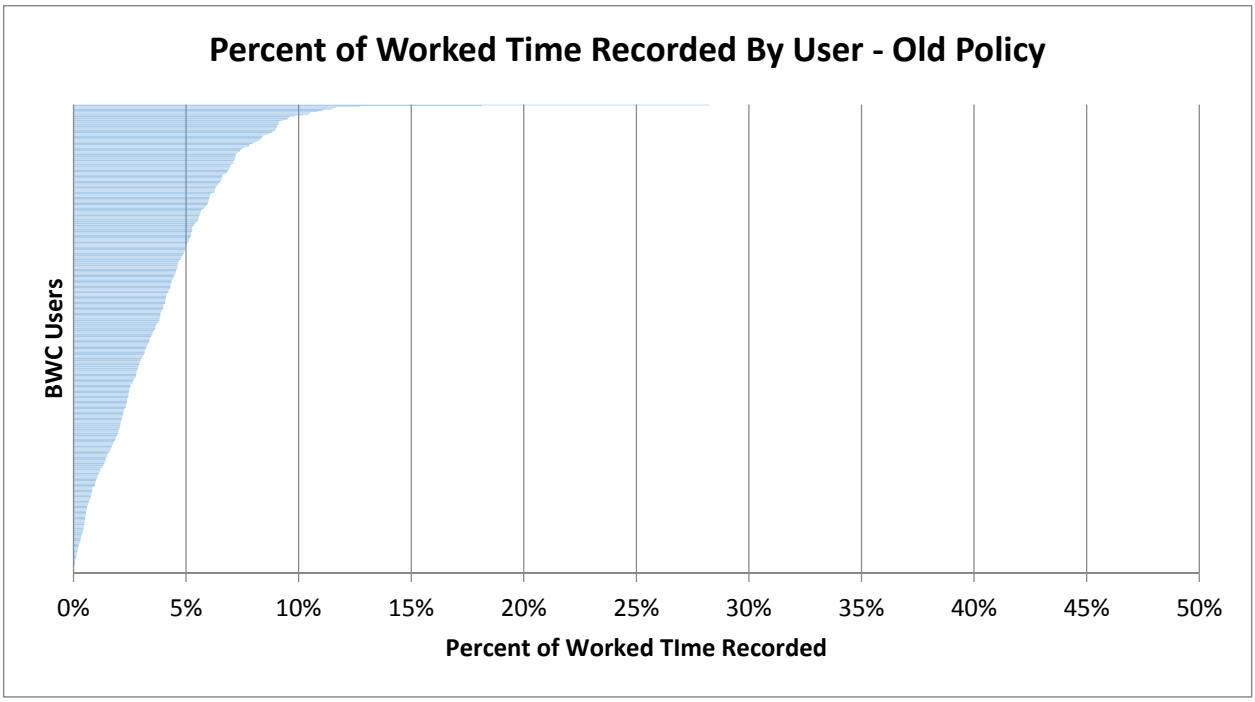


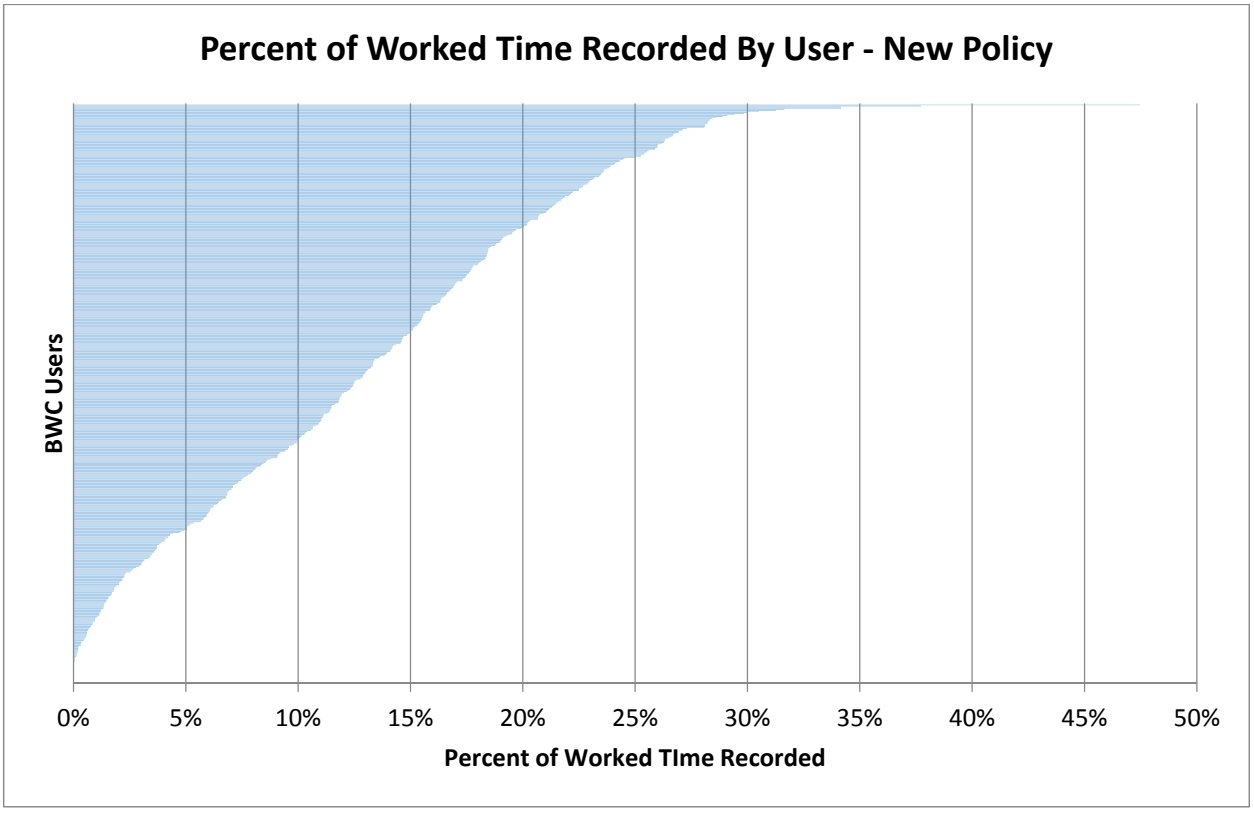
Under the new policy, the average length of videos also went up. A review of what portion of an officer's shift was recorded showed that after initial training use declined, and use increased significantly under the new policy.


Average Length of Video
Average Lenth of Video in Minutes
12
10
8
6
4
2
0
7/1/2016
8/20/2016
10/9/2016
11/28/2016
1/17/2017
3/8/2017
4/27/2017
6/16/2017
8/5/2017
Date

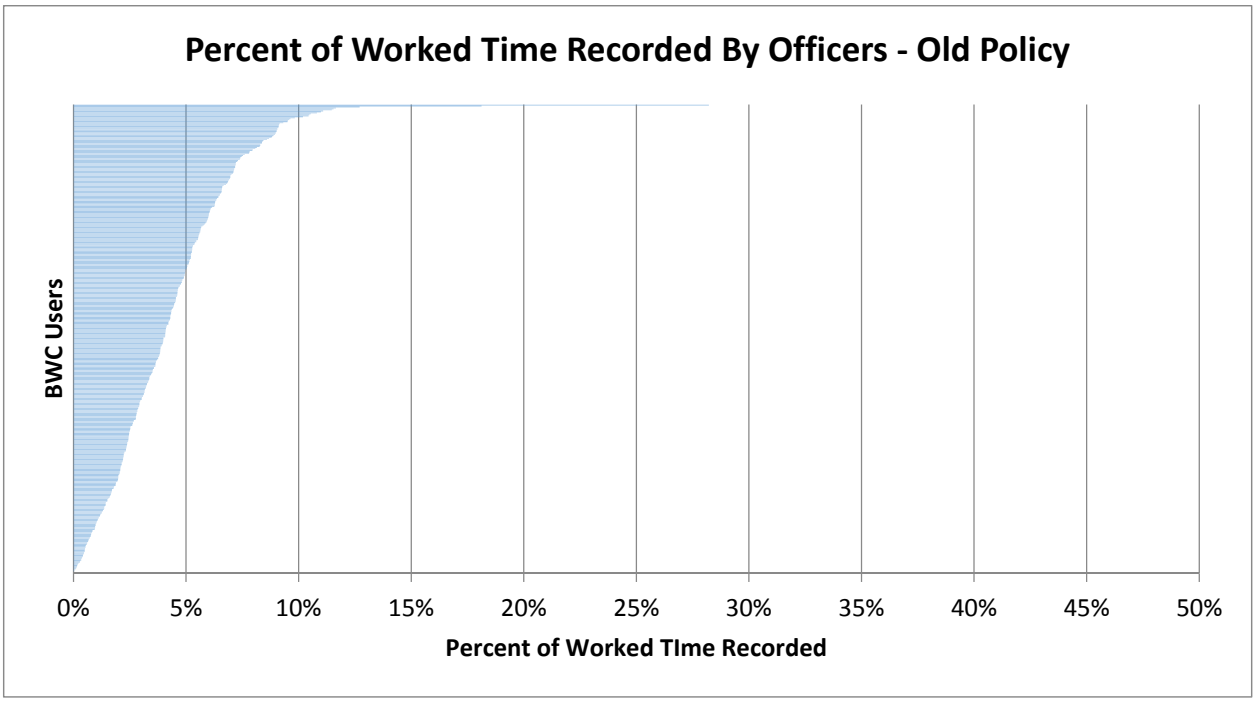

Percent of Hours Worked Captured on BWC
Percent of Hours Worked Recorded
25%
20%
15%
10%
5%
0%
7/1/2016
8/20/2016
10/9/2016
11/28/2016
1/17/2017
3/8/2017
4/27/2017
6/16/2017
8/5/2017
Date

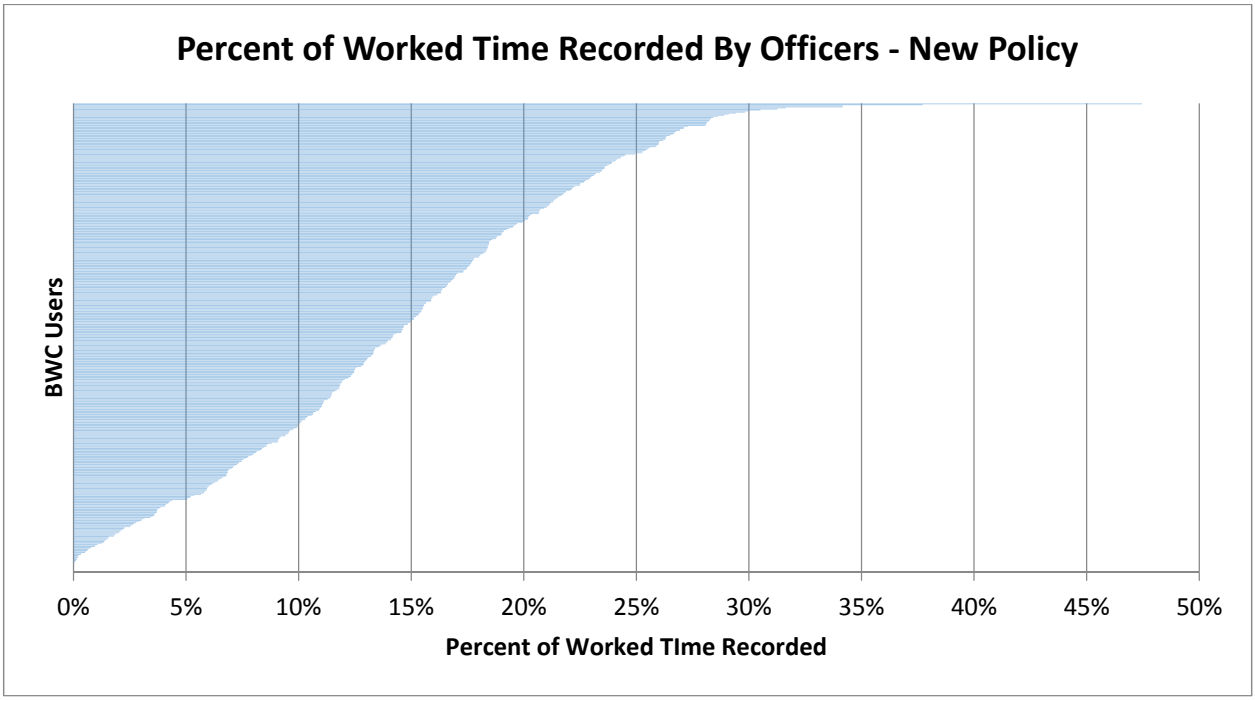
We looked at overall usage by individuals. We used the number of hours that were reported worked in an assignment during which activation would be expected, and determine d what percentage of that individual's worked time was recorded. 27% of users had less than one minute of video per 60 minutes worked under the old policy. This decreased to 15% of users under the new policy.





We observed that officers with a rank of Lieutenant and Sargent were included in the data. These individuals spend less of their work hours responding to recordable events. We conducted the same analysis of percentage of worked time recorded for just Officers. 17% of Officers had less than one minute of video per 60 minutes worked under the old policy. This decreased to 7% of Officers under the new policy.





Appendix B contains a number of charts showing overall BWC use over time, use by precinct, tenure, and shift. It appears that all precincts, shifts, and tenure ranges are using their assigned BWCs.

II. Mobile Video Program Audit Results and Recommendations

A. MV - Technology and Software

The MPD operated its MV system using technology from L3 Mobile Vision, Inc. (L3).

Equipment

Most MPD squad cars were equipped with an MV system. Each system includes a digital video recorder (DVR) mounted in the car, a set of cameras covering the front of the vehicle and the back seat, and a set of microphones to record audio in the car and to be worn by officers. The system also included a wireless transmitter that uploaded the contents of the DVR whenever the car was at a precinct or other place equipped with an access point.

MV systems could be turned on manually, and were also set to turn on automatically whenever the car's police lights were activated. The system was turned off manually. Once a video was captured, the driver would be prompted by the on-board computer to select one of five categories for the video.

Video, audio, and other data from the MV system were stored on a server located in City Hall. The storage system included a back-up system which automatically generated blu-ray discs when enough archivable data was captured. The MPD used discs specifically made for archiving, with a projected lifespan into the hundreds of years. The systems are operated by MPD and City IT staff. However, the City contracts with a vendor to administer the majority of its network operations and servers. Internal audit learned that this vendor has administrative access rights to the server on which the L3 software is located. This access was tied to a general administrative account that is shared by a group of staff at the vendor, and activity was not monitored. There was no reason to suspect any inappropriate access of videos had occurred.

Finding:
The vendor contracted by the City to administer its network and servers had administrative access to the server that stores unarchived MV data. While the vendor needed administrative access, the City should monitor the activity of the vendor on this server when access is made.

Software

The L3 software was accessible only while on the City network, or while connected through a virtual private network (VPN). The access was tied in to the City directory, meaning only individuals with a current City account could be granted access. The software logged video viewing activity, and tied each video to the DVR that recorded it.

The videos were categorized by MV operators on the go, and retention schedules were tied in to these categories. Some categories were set to automatically archive. Because the archiving was done on a disc, once archived there was no way to delete or destroy a video without physically finding and destroying the archive disc. Some categories were set to delete after 90 days. After a video was deleted, the data about that video (e.g. time taken, length) was also deleted within 30 days. Archived videos were also deleted from the system, but could be requested to be added back for temporary viewing.

The software system had very limited report generating capability. Because MPD officers were assigned to different cars on different days, and because partners would both use the same car at the same time, the software system could not associate MV video with a specific officer, and instead linked videos with specific DVR numbers.

B. MV - Policy and Training

MPD had a policy on MV use, included in the Administrative Procedures volume under the 4-200 policy that covered Equipment and Supplies. The policy contained sections that covered:

- Officer and supervisor responsibilities
- Activation and deactivation requirements
- Data access, retention and duplication rules
- Categorization

The provided training materials reasonably addressed the policy, however because the scope of an officer's obligations for the MV system was much smaller than with the BWC system the training was very brief. The training materials covered turning the MV system on and off, categorizing videos, and using the MV microphone.

Internal audit noted a disconnect between the BWC policy and the MV policy and training. Officers who were issued BWCs were allowed to not use the MV microphones, however the MV policy or was never updated to cover this exception, and still states that microphones must be worn.

Finding:
MV policy required officers to wear microphones, even though current practice was to allow BWC-equipped officers to not wear the MV microphones.

C. MV - Use

Officers were to use MV systems to record any stop or contact where a motor vehicle was involved, for domestic abuse incident interviews, and any time a person was transported to any destination in the squad car. The system could be turned on manually, or would turn on automatically when squad car lights were turned on. The system would be deactivated manually, and the vehicle driver would be prompted to immediately categorize the videos.

A more limited review of MV usage was conducted than BWC usage because the system was used in a much narrower set of incidents. Additionally, MPD officers were assigned to different cars on different days, and because partners would both use the same car at the same time, the software system could not associate MV video with a specific officer, and instead linked videos with specific DVR numbers. This made any work to link MV video to individual officers' BWC use, schedules, or dispatch data very difficult.

Our review focused on watching a sample of MV videos for noncompliance with specific aspects of policy.

Categorization

Because of the way MV footage categorization is prompted to the user, there were no videos that were uncategorized. We reviewed a sample of different categories and noted that 18% of videos should have been placed in a different category. The misclassifications ranged from arrest or citation videos being classified as 90-day retention, and videos with no activity that should have been classified as 90-day retention being flagged as arrests.

Activation/Deactivation

We observed that 9% of sampled videos did not capture events that led up to the incident being recorded, and 24% of sampled videos appeared to be deactivated prior to the conclusion of the incident. We specifically noted a subset of the sample included transportation to jail. Of these videos, 61% were stopped as the car was arriving at the jail, but prior to the transported individual being removed from the back seat of the car. The removal from the back seat is a particularly crucial moment, as the officer is actively interacting with the transported subject, and video is particularly critical to document the interaction.

Finding:
MPD staff transporting individuals to jail frequently deactivated their MVs prior to completing transport.

III. Oversight

The MPD did not have an established oversight program to ensure compliance with MV or BWC policy. Both policies stated that supervisors were to periodically review video to ensure proper procedures were being followed; however, there was no established review process or guidance for MV policy. For BWC policy, MPD stated that a set of training sessions for supervisors on how to conduct reviews had just been developed, with the first sessions occurring in June 2017. The training materials that were reviewed provided good instructions on how to conduct reviews, including report generation and what to look for, and established baseline expectations for reviewers. MPD also stated that they were in the process of developing a new program interface to enable supervisors to easily compare hours worked to BWC data.

Finding:
There were no records regarding what kinds of supervisor reviews were being conducted. Though MPD policy included a periodic supervisor review requirement there was no guidance or training on what a review should consist of for MV, and guidance for BWCs was not developed for a year after the policy was put in place.

As stated in the MPD BWC Policy, this program's goal was to enhance accountability and public trust. The policy continues in stating that the policy provides MPD personnel with procedures for the use and management of Body Worn Camera equipment and the resulting data. What the policy and the program lack are how the program is to be governed and by whom.

The MPD BTU conducted a pilot of the equipment and technology, developed and executed a training program and implemented the equipment and technology use across the police department. From that implementation, it's not apparent that any division within the MPD or City focused on the operationalization of the program in pursuit of its original goals of enhancing accountability and public trust.

Acknowledgments

The Internal Audit team, and OPCR staff, would like to acknowledge the effort put forth by the entire Minneapolis Police Department. In particular the Business Technology Unit was very prompt in providing all data requested, and generally being extremely forthcoming with information.

Appendix A: Objective, Scope and Approach

Objective

The objective of the audit was to determine whether mobile and body worn cameras and respective programs were being used and executed in accordance with statutes and policies, and were adequately designed, administered and monitored.

A review of compliance with Minnesota Statutes was part of the Internal Audit Department's Fiscal Year 2017 Annual Audit Plan. The scope was expanded in response to increased interest in the effectiveness of the BWC program.

Scope

The scope of this audit covered from the initial issuance of BWCs to MPD staff in July 2016 through August 2017. The scope included:

- MPD policies on BWC and MV use, and resulting data use.
- MPD training materials.
- Hardware and software used by MPD in its BWC and MV programs.
- Data generated by BWCs and MVs, and generated by MPD staff as they used hardware and software.

Approach

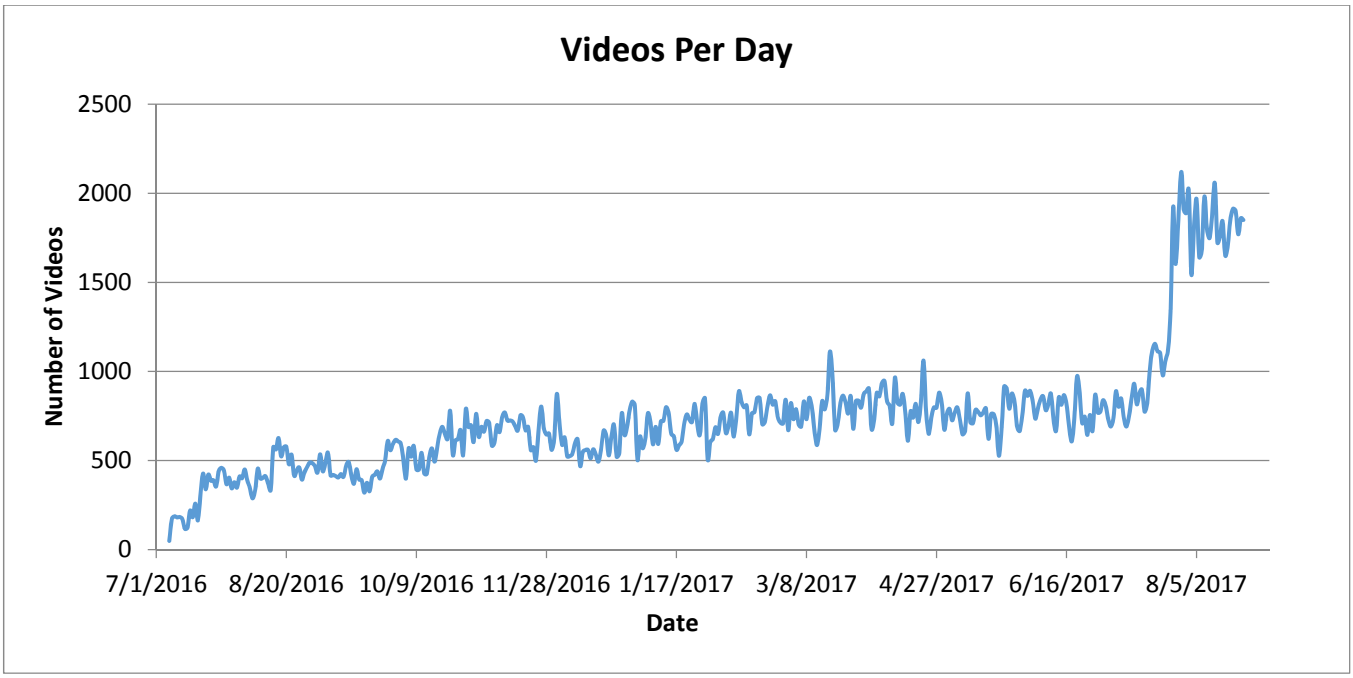
To accomplish audit objectives, Internal Audit:

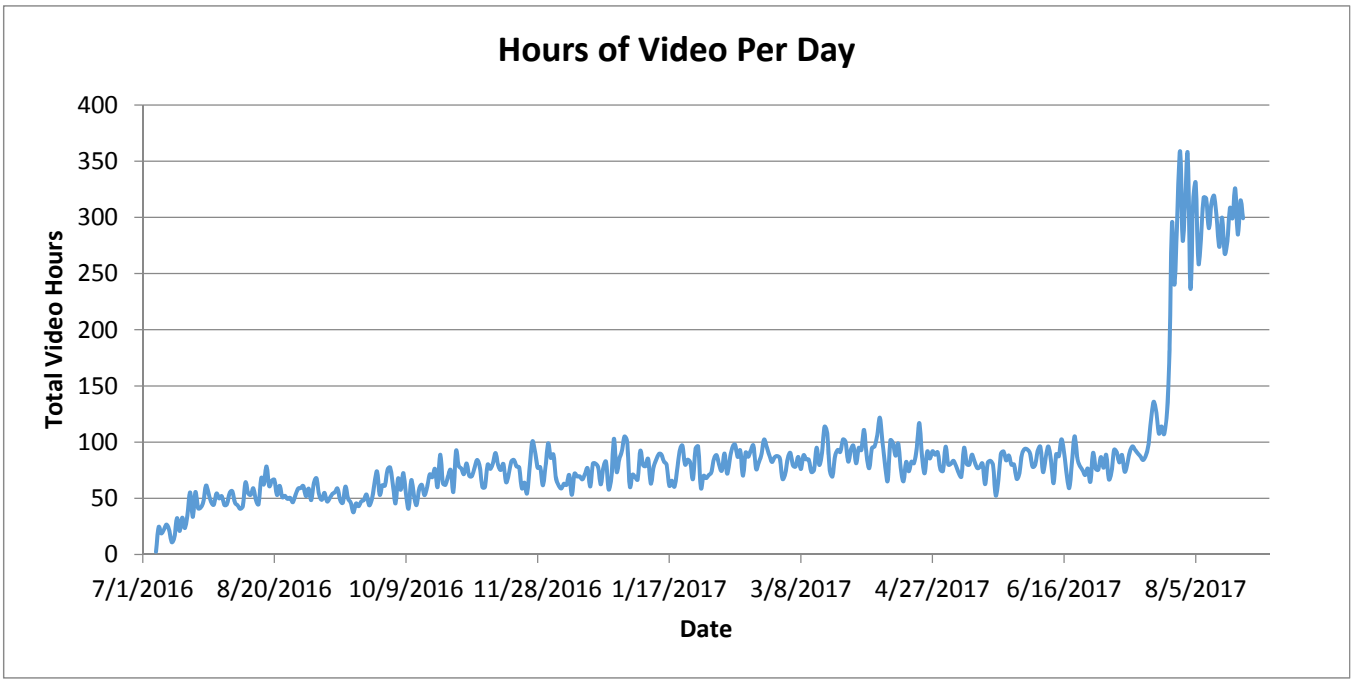
- Reviewed Minnesota statutes.
- Reviewed prior work conducted by OPCR.
- Discussed program functionality with MPD staff.
- Reviewed MPD policy and training materials.
    - Due to policy update during the audit, compliance statistics were determined for new and old policy where applicable.
- Discussed BWC software functionality with Axon representatives.
- Evaluated software access controls and CJIS training records.
- Reviewed BWC videos and MV videos
- Acquired and analyzed data from police dispatch, time reporting, and video storage systems.
- Collaborated with OPCR staff.

Appendix B: Usage Statistics

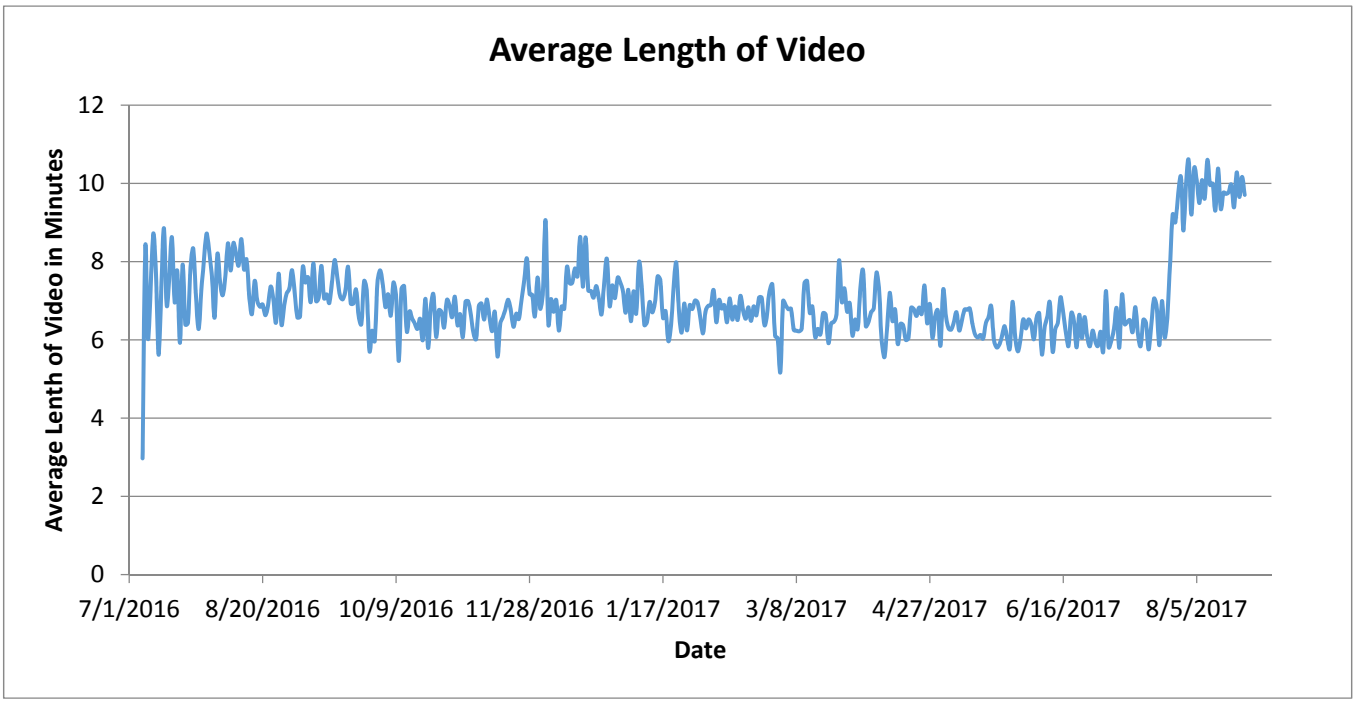
This section contains graphs that show how MPD officers have used BWCs. Data has been narrowed down to cover only officers that have been issued cameras, and to only cover time reported when working assignments in which activation of BWCs is expected to happen.

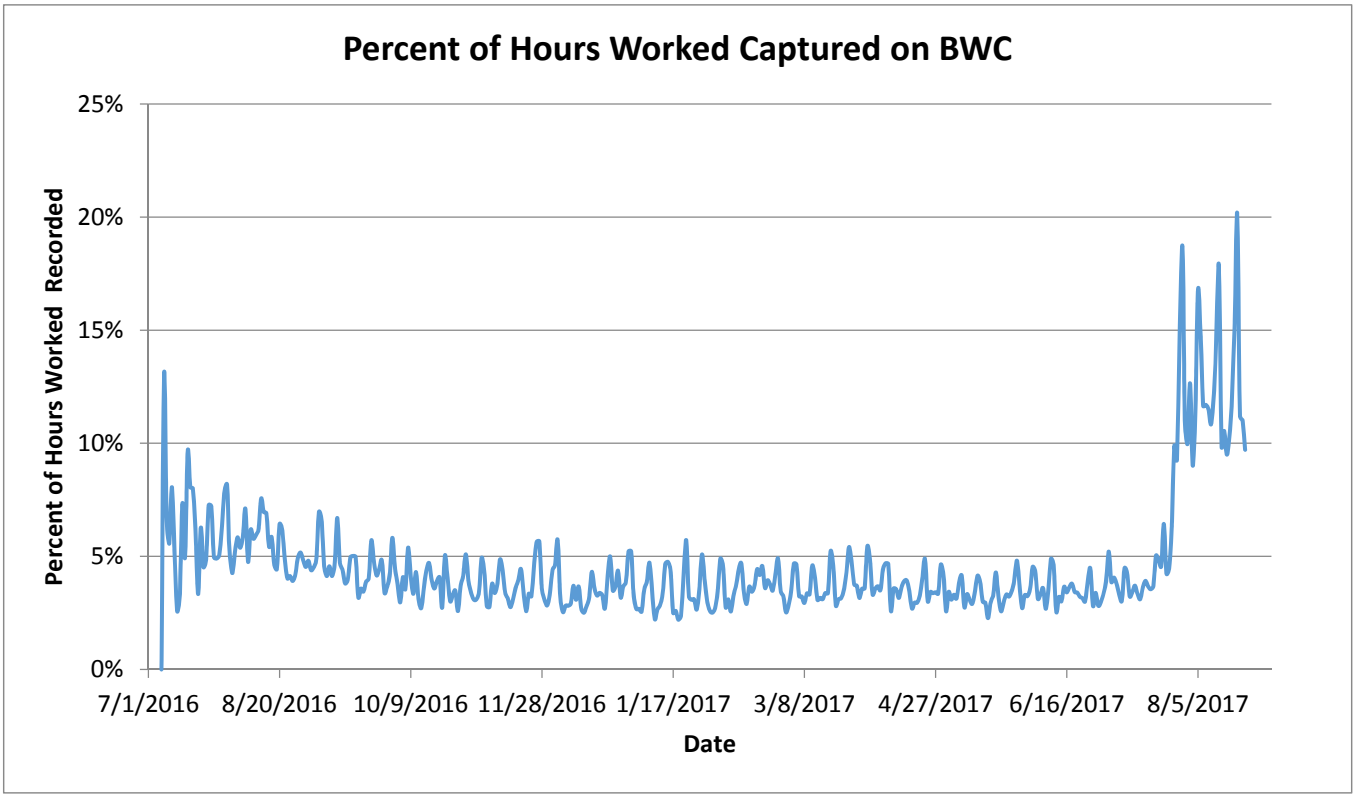
These graphs show the number of videos over time and how much video has been captured.



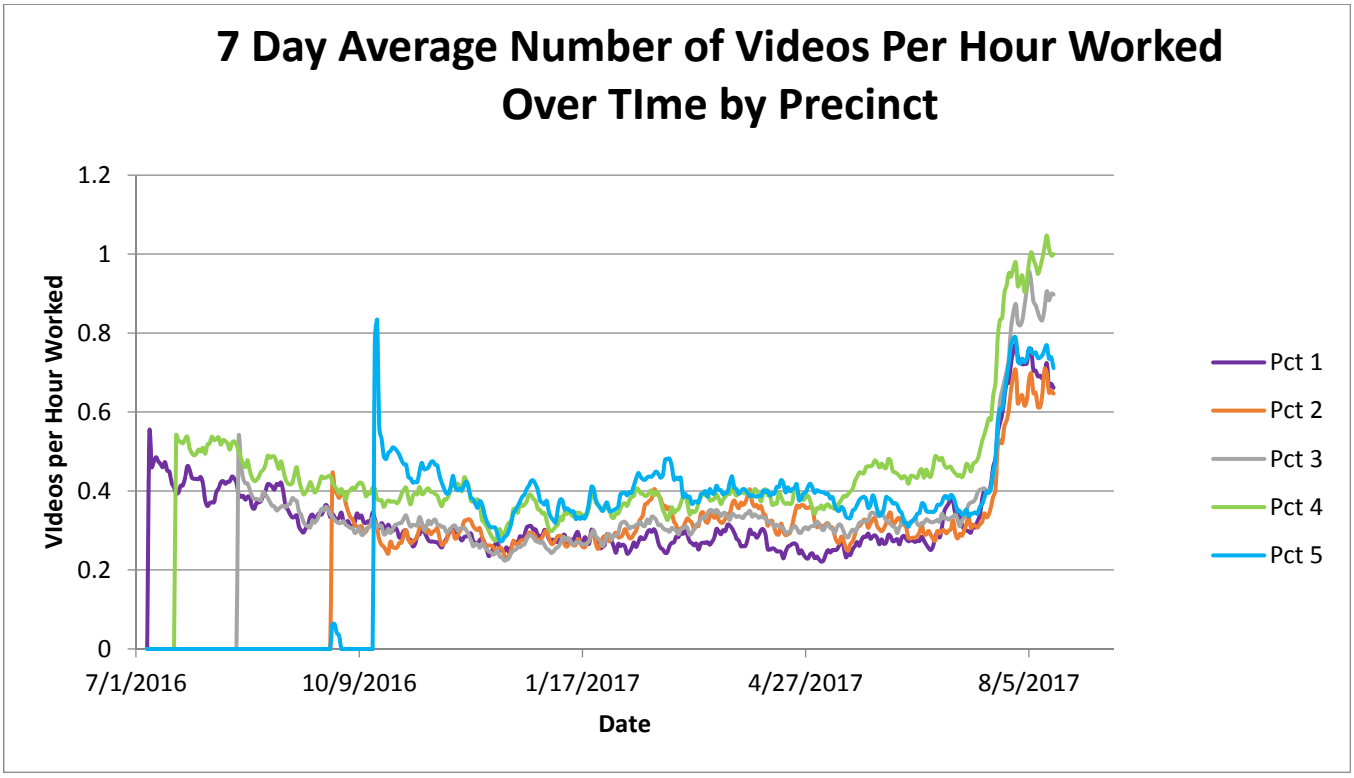


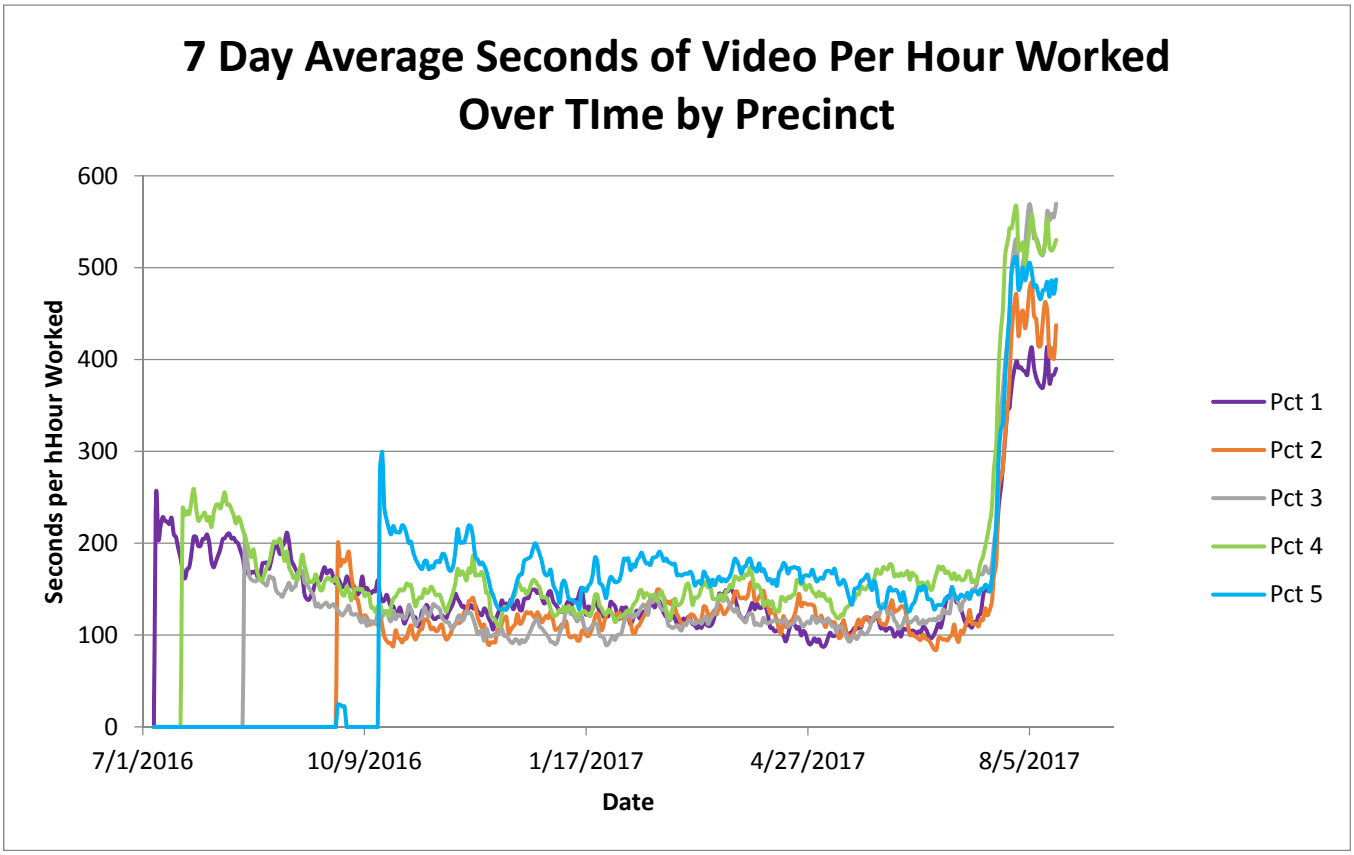
These graphs show the average length of videos over time and how much video has been captured per hour worked.

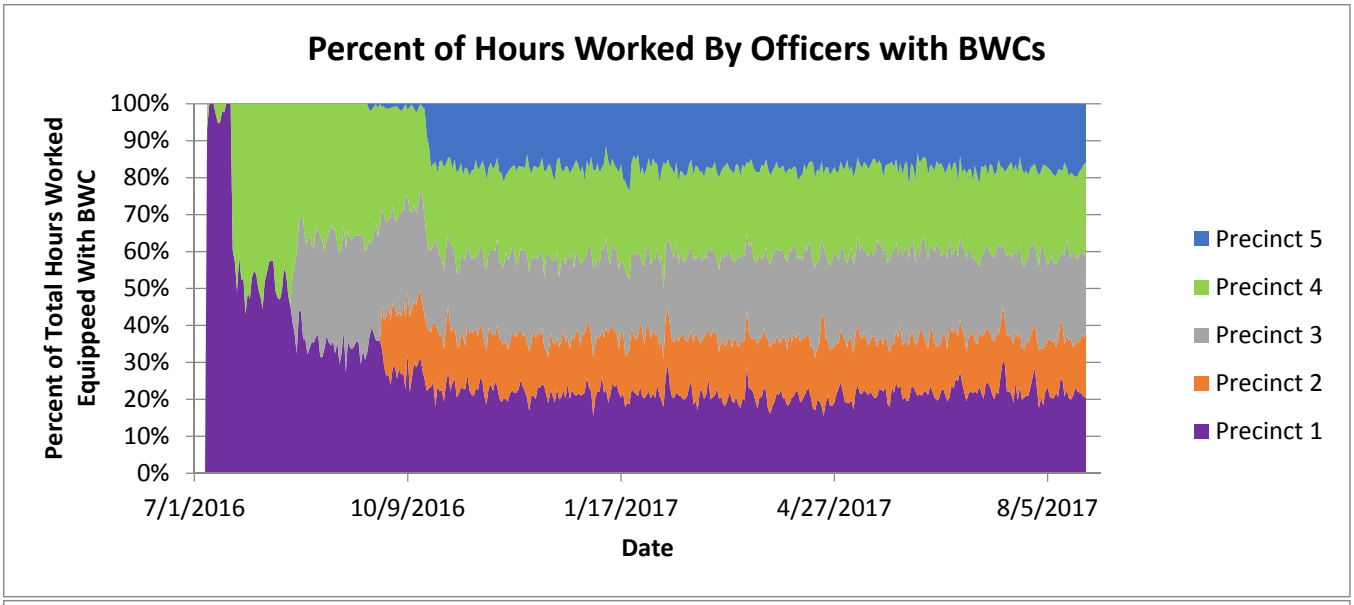


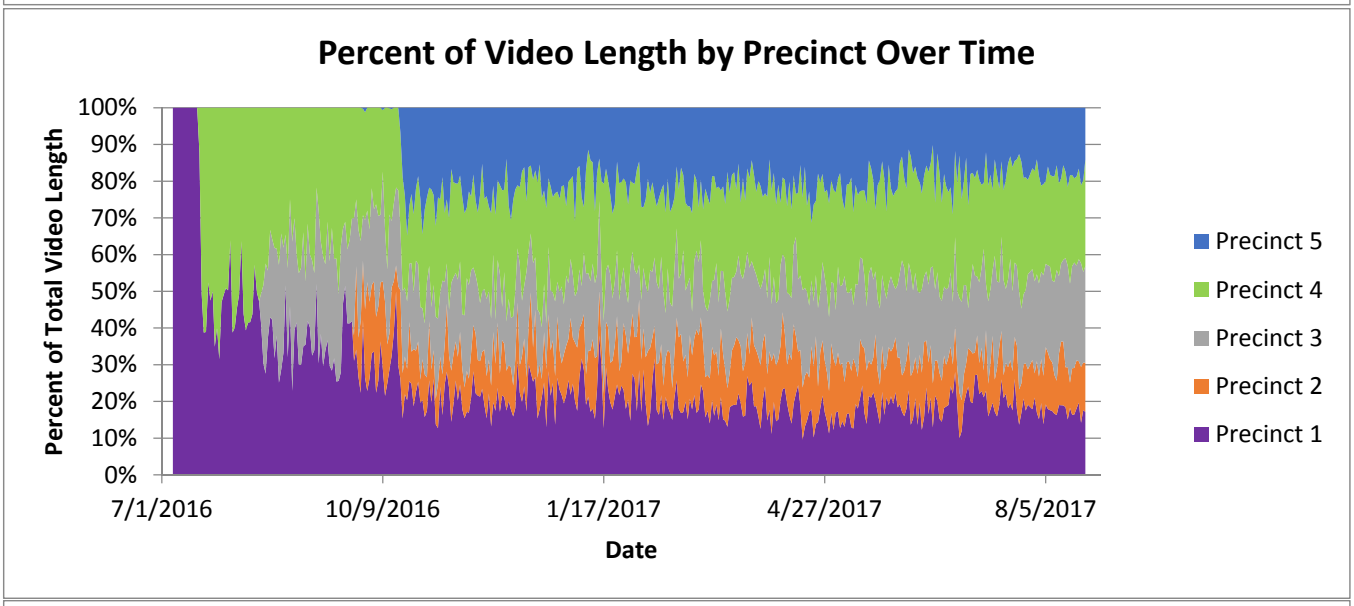


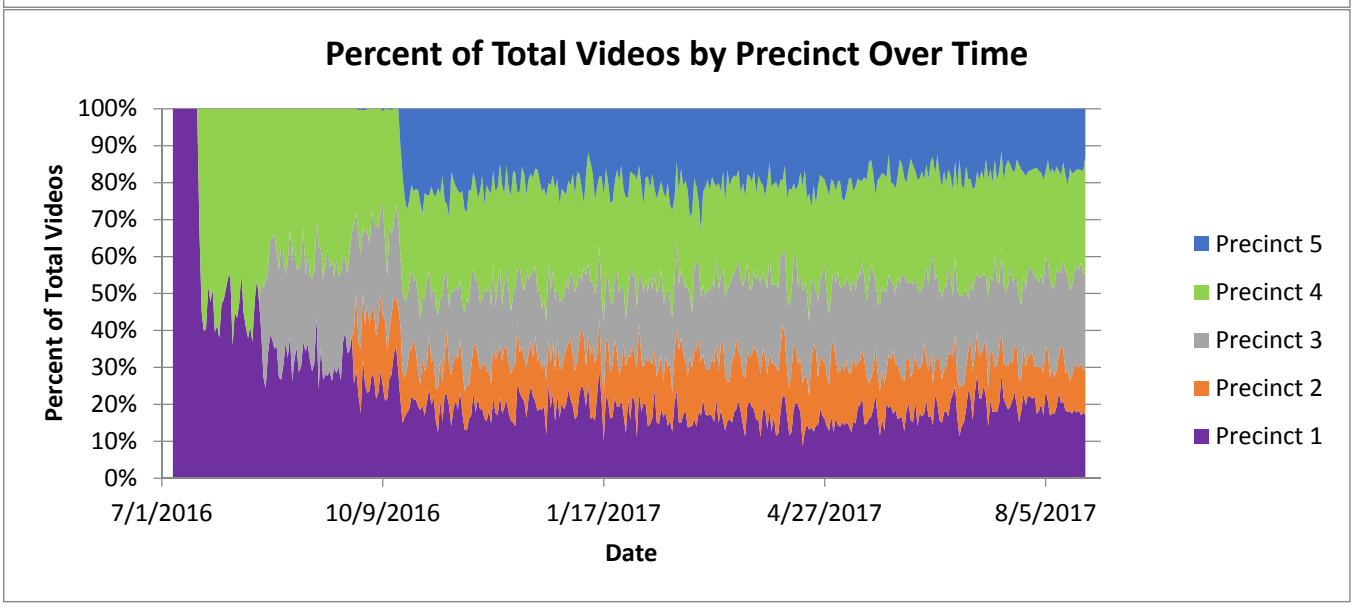
These graphs show hours worked, video length, and number of videos by precinct.



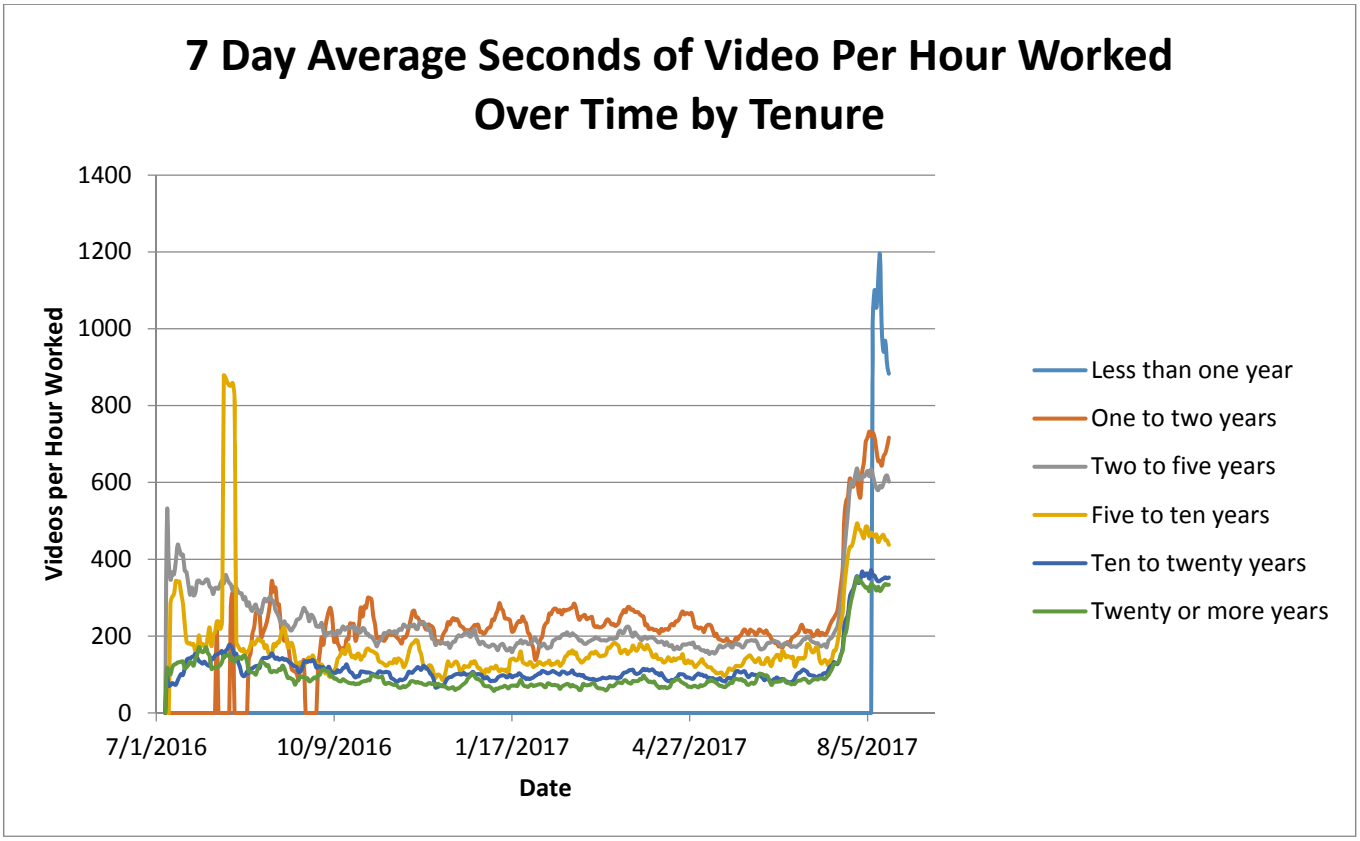


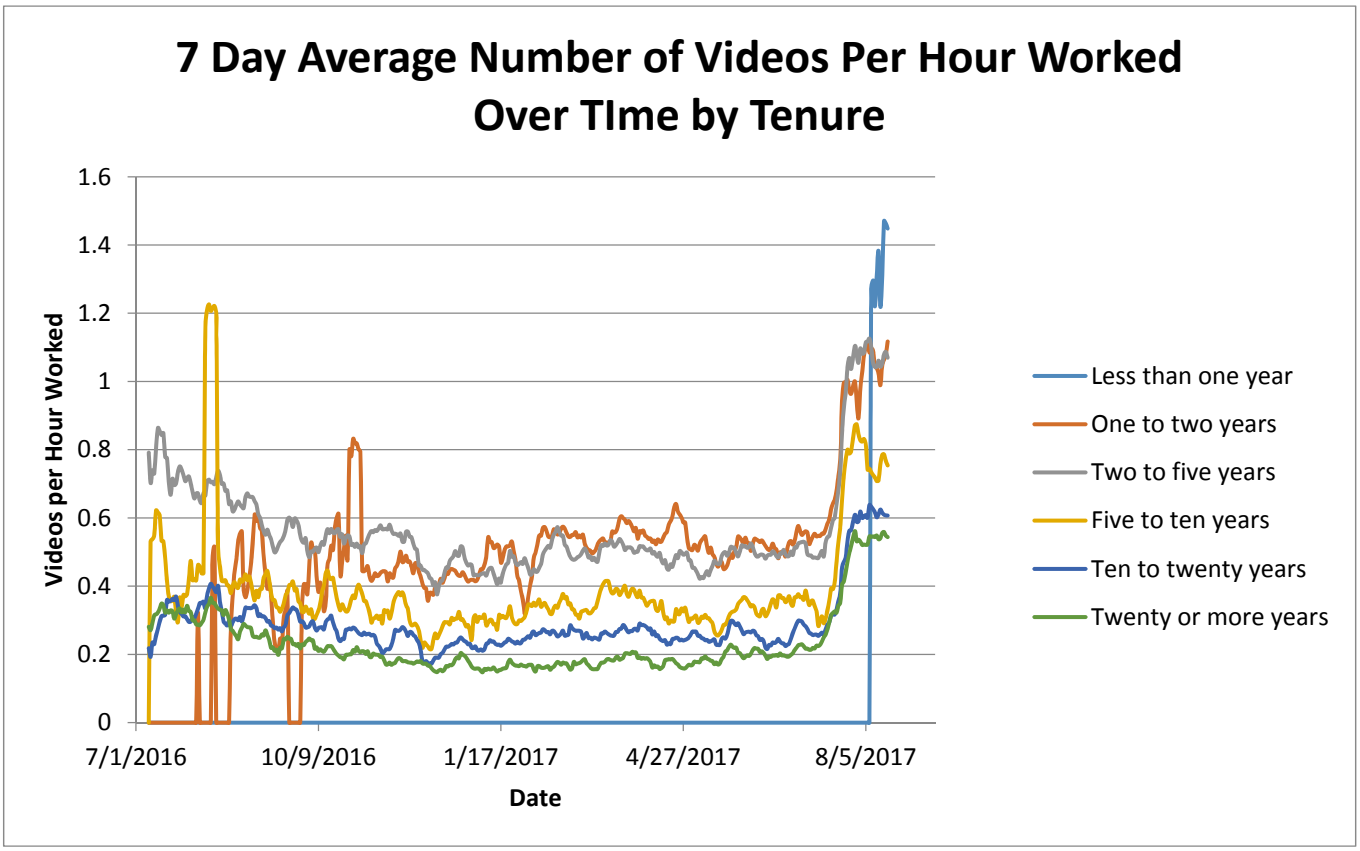

Percent of Hours Worked By Officers with BWCs
Percent of Total Hours Worked Equippeed With BWC
100%
90%
80%
70%
60%
50%
40%
30%
20%
10%
0%
7/1/2016
10/9/2016
1/17/2017
4/27/2017
8/5/2017
Date
Precinct 5
Precinct 4
Precinct 3
Precinct 2
Precinct 1

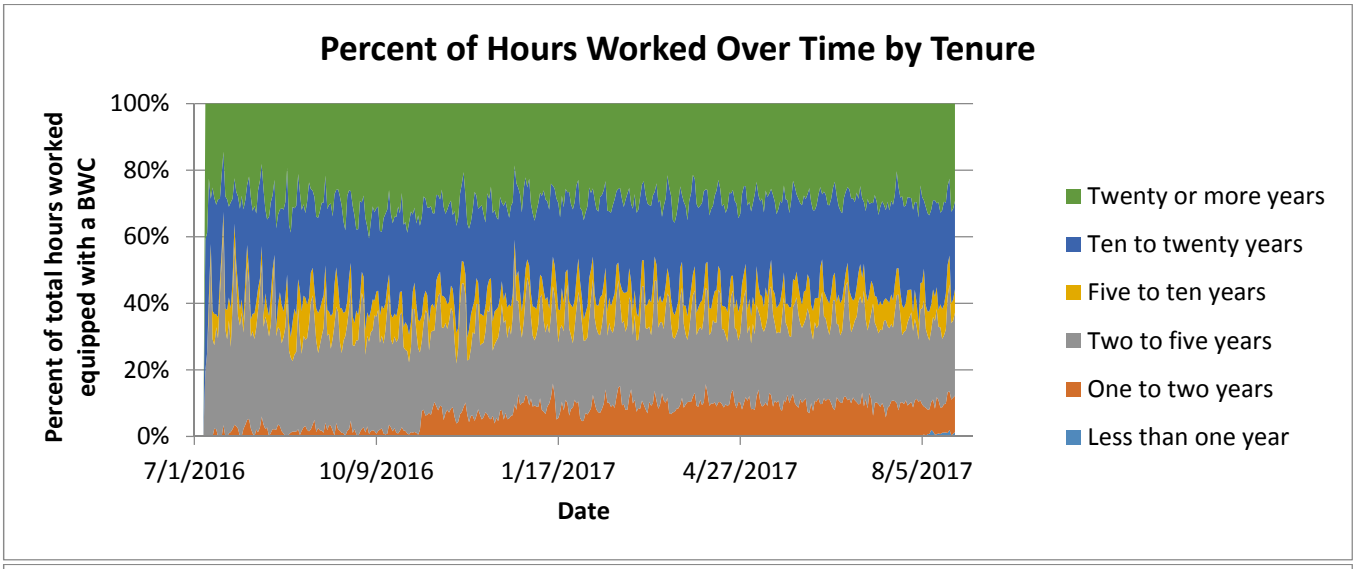

Percent of Video Length by Precinct Over Time
Percent of Total Video Length
100%
90%
80%
70%
60%
50%
40%
30%
20%
10%
0%
7/1/2016
10/9/2016
1/17/2017
4/27/2017
8/5/2017
Date
Precinct 5
Precinct 4
Precinct 3
Precinct 2
Precinct 1

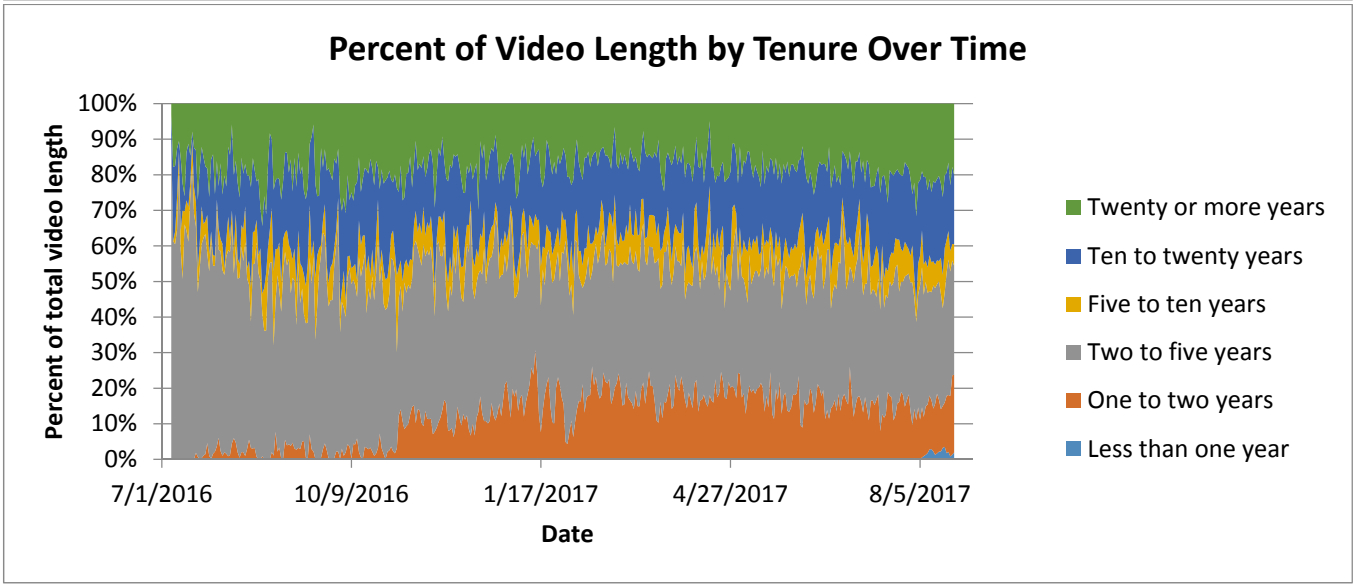

Percent of Total Videos by Precinct Over Time
Percent of Total Videos
100%
90%
80%
70%
60%
50%
40%
30%
20%
10%
0%
7/1/2016
10/9/2016
1/17/2017
4/27/2017
8/5/2017
Date
Precinct 5
Precinct 4
Precinct 3
Precinct 2
Precinct 1

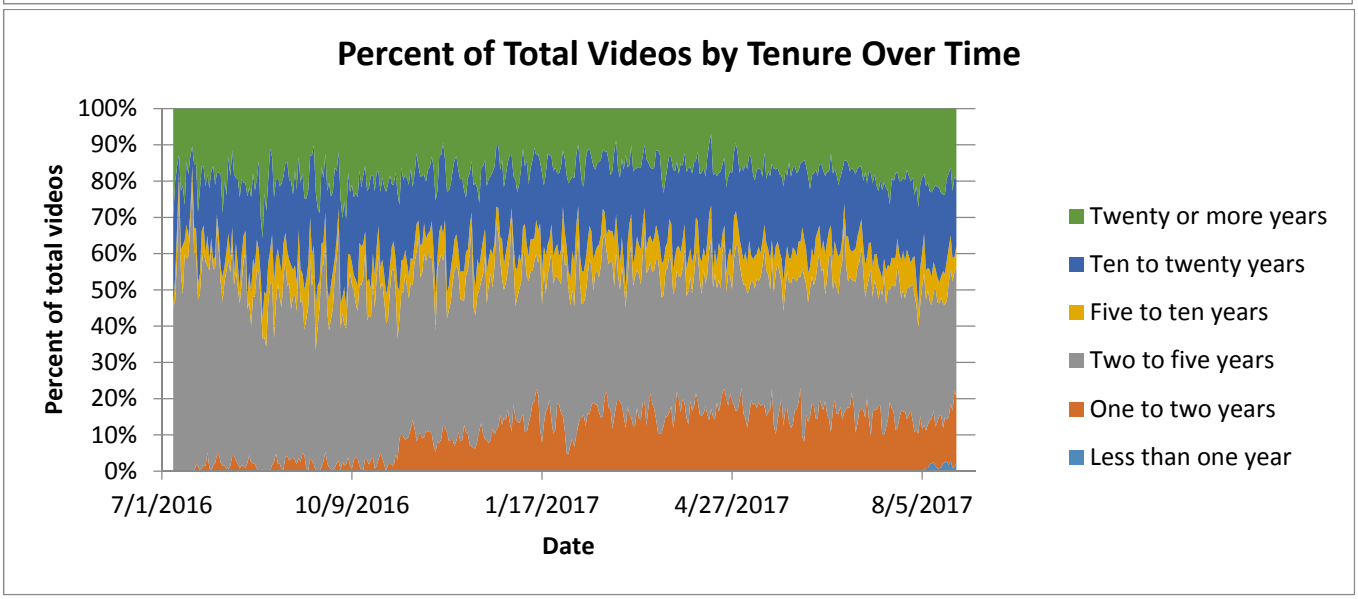
These graphs show hours worked, video length, and number of videos by tenure.



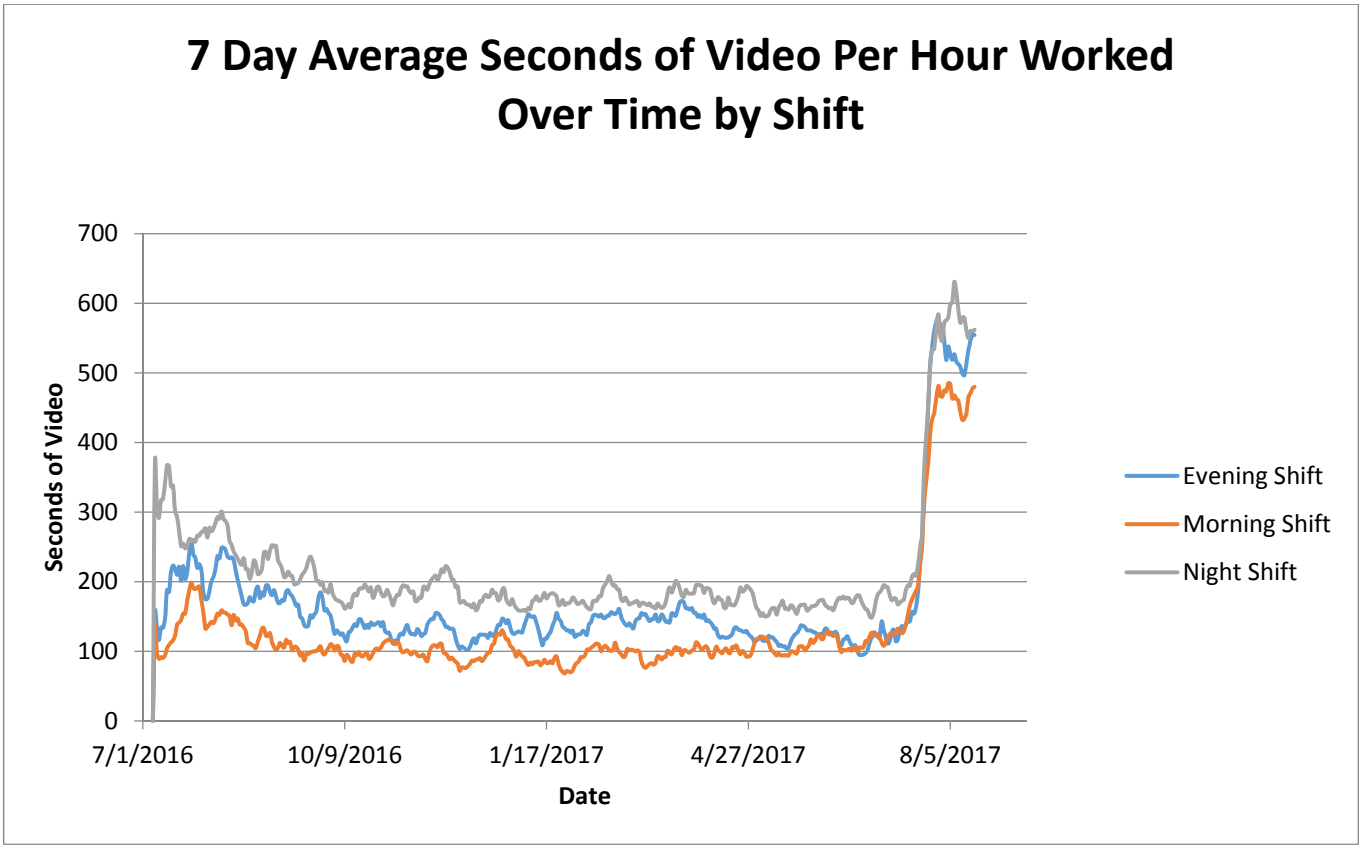


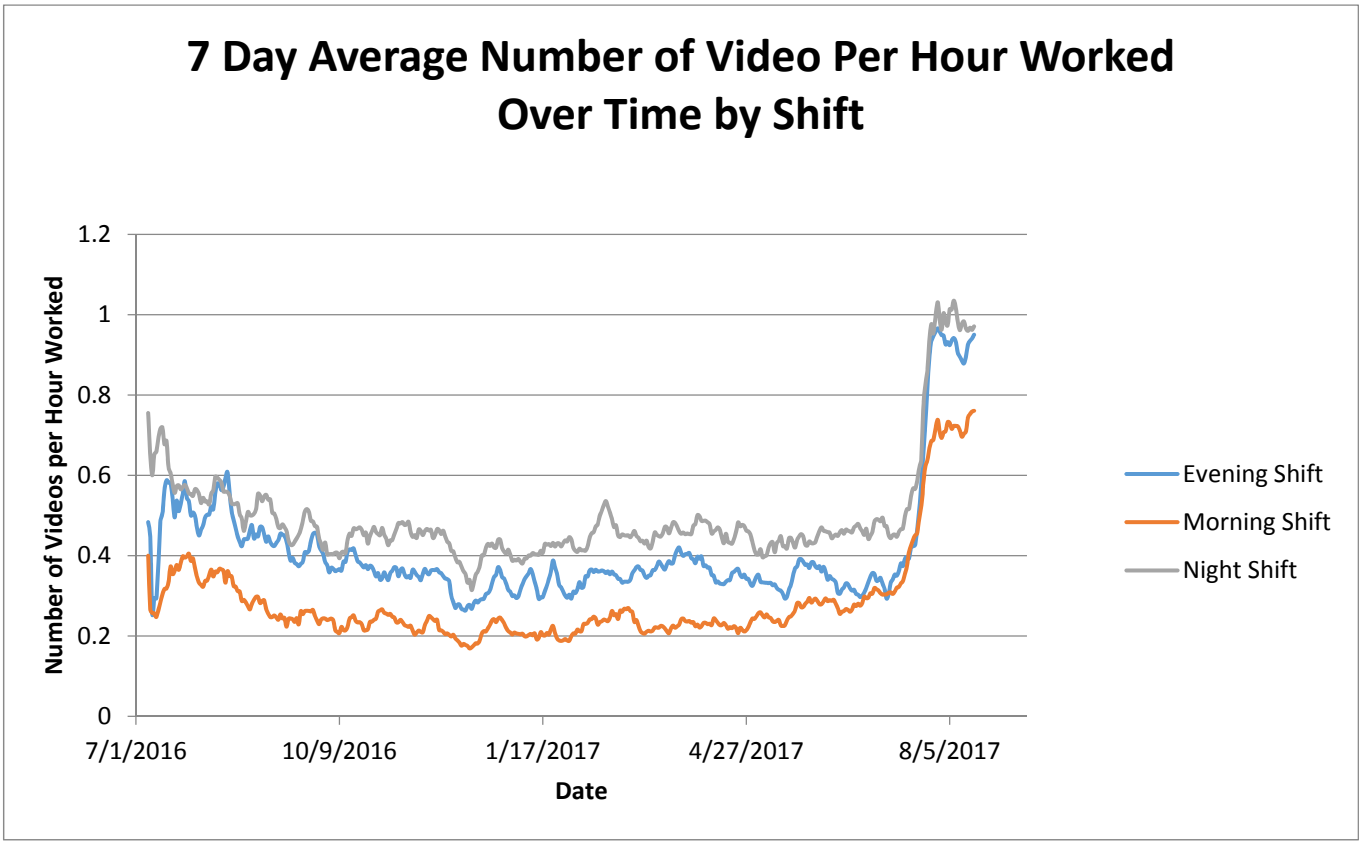

Percent of Hours Worked Over Time by Tenure
Percent of total hours worked equipped with a BWC
100%
80%
60%
40%
20%
0%
7/1/2016
10/9/2016
1/17/2017
4/27/2017
8/5/2017
Date
Twenty or more years
Ten to twenty years
Five to ten years
Two to five years
One to two years
Less than one year

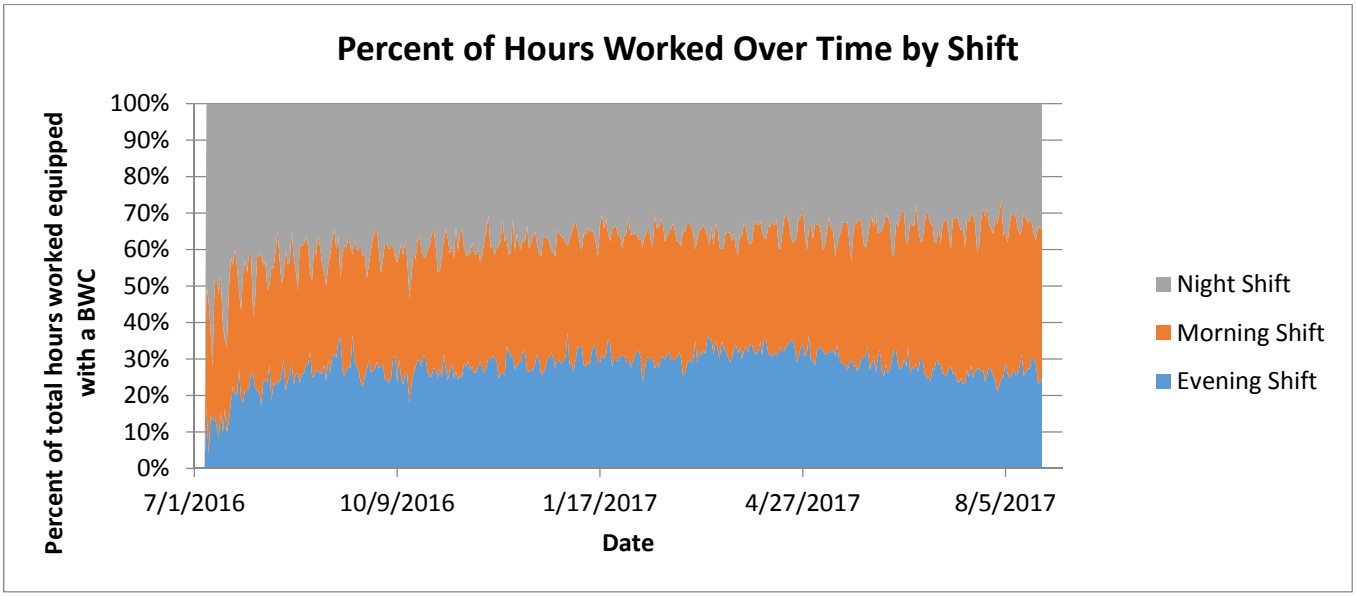

Percent of Video Length by Tenure Over Time
Percent of total video length
100%
90%
80%
70%
60%
50%
40%
30%
20%
10%
0%
7/1/2016
10/9/2016
1/17/2017
4/27/2017
8/5/2017
Date
Twenty or more years
Ten to twenty years
Five to ten years
Two to five years
One to two years
Less than one year

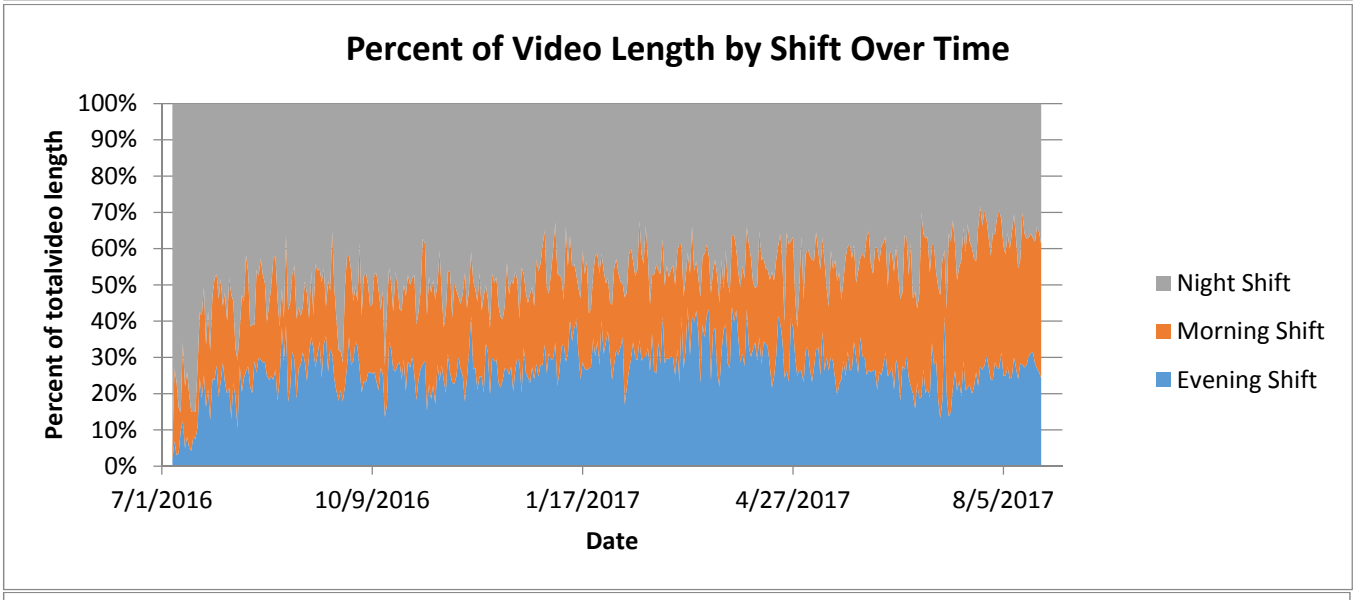

Percent of Total Videos by Tenure Over Time
Percent of total videos
100%
90%
80%
70%
60%
50%
40%
30%
20%
10%
0%
7/1/2016
10/9/2016
1/17/2017
4/27/2017
8/5/2017
Date
Twenty or more years
Ten to twenty years
Five to ten years
Two to five years
One to two years
Less than one year

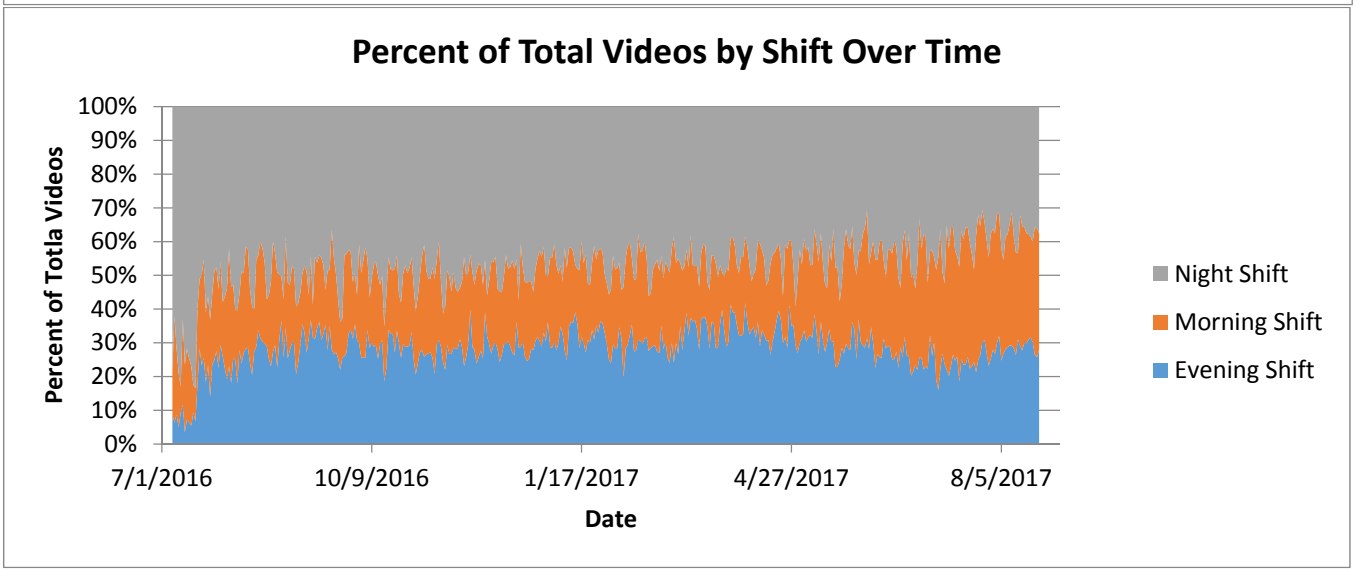
These graphs show hours worked, video length, and number of videos by shift.






Percent of Hours Worked Over Time by Shift
Percent of total hours worked equipped with a BWC
100%
90%
80%
70%
60%
50%
40%
30%
20%
10%
0%
7/1/2016
10/9/2016
1/17/2017
4/27/2017
8/5/2017
Date
Night Shift
Morning Shift
Evening Shift


Percent of Video Length by Shift Over Time
Percent of totalvideo length
100%
90%
80%
70%
60%
50%
40%
30%
20%
10%
0%
7/1/2016
10/9/2016
1/17/2017
4/27/2017
8/5/2017
Date
Night Shift
Morning Shift
Evening Shift


Percent of Total Videos by Shift Over Time
Percent of Totla Videos
100%
90%
80%
70%
60%
50%
40%
30%
20%
10%
0%
7/1/2016
10/9/2016
1/17/2017
4/27/2017
8/5/2017
Date
Night Shift
Morning Shift
Evening Shift