Minneapolis Police Department

Biennial Body Worn Camera Audit

Abstract

This document has been drafted to provide an audit of the Minneapolis Police Department's use of Body Worn Cameras (BWC).

WILDCARD®

CYBERSECURITY • WEB DEVELOPMENT • IT SOLUTIONS

Biennial Body Worn Camera Audit

This biennial audit report has been prepared for the Minneapolis Police Department satisfying requirement of Minnesota statute 13.825. The Body Worn Camera Audit focused on the compliance and operational efficiencies of the Minneapolis Police Department.

Wildcard wishes to acknowledge the cooperation and efforts of the Minneapolis Police Department in the execution of the audit. Particularly the Records Information Unit, Business Technology Unit, and the Office of Police Conduct Review. We would also like to thank Internal Audit for facilitating audit activities. of the staff at the agencies included in our audits.

Talin Senner
Chief Executive Officer
Wildcard Corporation
18 November 2019

Executive Summary..... 4

Introduction..... 6

BWC Audit..... 6

Policy..... 6

Data Classification..... 6

Data Maintenance and Destruction..... 7

Public Data Request Handling and Redaction..... 7

Data Access and Security..... 8

BWC Use..... 9

BWC Procurement..... 10

Appendix A: Methodology..... 11

Appendix B: Interview List..... 12

Executive Summary

Objectives - Two audit objectives were identified for the biennial audit of the Body Worn Camera.

- Assess the Minneapolis Police Department (MPD) use of BWC to determine it's compliance with Minnesota statute 13.825.
- Review, examine, and assess MPD policies and procedures for the operation of BWC to determine if there are any potential for improvement to support compliance efforts and operation.

Scope

Wildcard has conducted a biennial audit of the Minneapolis Police Department's use of Body Worn Cameras (BWC). The objective of this engagement is to audit compliance with BWC laws and regulations, and review relevant policies, procedures and security controls, as required by the State of Minnesota Statute 13.825. The audit was an independent review of the MPD's implementation of BWC technology and processes to determine how data is currently classified, used, and destroyed. Wildcard also verified that the system access was appropriate.

The audit was conducted by evaluating the use of the system via observing relevant artifacts, conducting interviews with personnel, and examining the system. Our observations ranged from the time of the conclusion of the previous audit August 1, 2017 to July 31, 2019. We have determined that MPD's operation of BWC technology is in compliance with Minnesota Statute 13.825 and all associated relevant statues.

Wildcard worked with MPD to determine that:

- MPD BWC policy includes provisions for all mandated elements
- Data is appropriately classified
- Data is properly maintained and destroyed
- Public Data is properly sanitized
- Access to data is limited

Areas of Improvement

While MPD is in compliance, Wildcard has identified some areas of improvement. The areas we focused on are capabilities that support compliance activities. Each area of improvement is specified in the following paragraphs along with our recommendations.

1) Access removal for separated personnel.

Wildcard discovered that there is a lag between when personnel are no longer with MPD and when they have had their permissions removed from the BWC portal. Wildcard recommends a process be put in place that expediates the removal of permissions by coordinating efforts between HR and BWC portal operators.

2) Standard Operating Procedures (SOP) for operation of releasing data to external agencies and the public has not been established for RIU personnel.

While working with personnel designated as RIU administrators, Wildcard discovered that there is not a defined SOP in place. BWC operation is governed by state laws and has defined activities that are necessary for proper operation. The implementation of an SOP will facilitate the proper release and sharing of BWC data. The SOP will allow for efficient and consistent operations. The SOP will also facilitate future BWC audits and offer protection from potential liability.

3) Cohesive Handling of failed equipment.

While conducting interviews with MPD supervisors, we noticed that supervisors handled failed equipment differently. Wildcard recommends the implementation of a cohesive strategy for handling of failed equipment.

Introduction

The audit objectives, scope and methodology are described in Appendix A.

BWC Audit

The audit of MPD use of BWC covers the period of August 1, 2017 to July 31, 2019. Wildcard collected artifacts and conducted interviews with BWC operators to determine its compliance with Minnesota statute 13.825. The BWC is defined as a device worn by a peace officer that is capable of both video and audio recording of the officer's activities and interactions with others or collecting digital multimedia evidence as part of an investigation.

General Observation

MPD has put in place formal policies and procedures to operate the BWC system in compliance with Minnesota Statutes. MPD has written policies in place, properly classify data, appropriately sanitize publicly released data, restricted system access, applied appropriate automated data retention controls, and adhere to statutory requirements.

Policy

Observation **-** The MPD has an established policy that addresses the mandates associated with Minnesota Statute 13.825. The policy is defined as 4-223 Body Worn Camera (BWC) and last updated on April 4, 2018.

Analysis **-** After reviewing the policy and comparing its contents to the mandates in Minnesota statute 13.825, all of the requirements for BWC use and personnel are addressed.

Recommendation **-** None

Data Classification

Observation **–** Data collected by BWC automatically has the designation of nonpublic. In order for data to be released to the public a request must be made, and content reviewed by Records Information Unit (RIU).

Analysis **-** Wildcard evaluated a sample of data collected by the BWC system. We also examined the process for sharing data with other agencies and releasing data to the public. The MPD controls that are in place meet requirements of keeping data collected by BWC from public consumption. Shortly after each recorded activity, BWC data is assigned a category which automatically defines its retention characteristics. MPD has also put in place supervisory review processes to evaluate if data is classified correctly. This review process reduces risk that data will be purged from the system inadvertently.

Recommendation **–** None

Data Maintenance and Destruction

Observation – BWC data is stored in a system that limits access to data and automatically manages retention. Data has an automated retention period that ranges from a minimum of 1 year and up to 7 years. MPD has defined a category of significant events which are maintained for at least 7 years and must be manually deleted. Significant events include:

- Critical Incident
- Homicide
- Pursuit involving injuries or significant property damage
- Squad accident involving injuries or significant property damage
- Man-made or natural disaster or act of terrorism
- Any event that an officer or supervisor believes should be brought to the immediate attentoiin of police command staff

MPD has implemented a Quality Assurance program that mandates supervisors review a sample submitted BWC data to validate that data has been properly categorized and has the appropriate retention settings assigned to them.

Analysis - Wildcard worked with the Office of Police Conduct Review (OPCR) to review a sample of data from various categories. We focused on high risk categories that could potentially lead to data related to investigations being deleted. An example is some data that is related to a case involving domestic abuse is accidentally categorized as training data. Training data would have a one year retention instead of the expected seven years. There were 1113 samples of recorded data that were selected randomly. The sample selection was focused on high risk categories. We also focused on data that was created after the updated policy established on April 4, 2018.

Of our sample selection .2% of them were potentially deleted inappropriately. We are not able to validate that this content should not have been deleted. The title assigned to this footage by the officer conflicts with the category types. An example is data with a title labeled domestic violence but is categorized as startup.

Wildcard has validated that the majority of data is not entered into high risk categories inappropriately.

Recommendation – None

Public Data Request Handling and Redaction

Observation – The RIU receives requests via email or walk ins to release BWC data to the public. Requests from outside agencies are typically received via email. The RIU processes these requests by validating that the individual making the request is authorized to receive the data. The RIU then reviews the footage and obfuscates any audio and video that should not be released to the public due to lack of consent or sensitivity of footage. Once the initial footage has been scrubbed it is reviewed by another member of the RIU for quality control. After a quality control check the footage is released.

Analysis - Wildcard conducted interviews with RIU personnel. The RIU walked us through how requests are received and processed. The RIU demonstrated the redaction process in software. The software was able to obfuscate both video and audio and create a new file that preserves the initial copy. That new file is then shared with the requester.

Wildcard observed that the processes employed by the RIU are ad hoc. The processes in place conform to state statutes but they have not been formalized and made repeatable for potential new hires.

Recommendation – While working with personnel designated as RIU administrators, Wildcard discovered that there is not a defined SOP in place. BWC operation is governed by state laws and has defined activities that are necessary for proper operation. The implementation of an SOP will facilitate the proper release and sharing of BWC data. The SOP will allow for efficient and consistent operations. The SOP will also facilitate future BWC audits and offer protection from potential liability.

Wildcard recommends that processes be put in place to validate email requests from outside agencies. Email is insecure by nature that can be manipulated in ways that could trick RIU personnel into releasing data to unauthorized personnel. An additional step should be implemented to verify that requests from government agencies are valid.

Management Response – RIU is developing a SOP and will have it in place by January 1, 2020.

Data Access and Security

Observation – Access to the BWC portal is granted by written permission from Commander of Technology and Support Services Division. MPD has a written access control policy, and written documentation authorizing all users that have access and specifying the purpose of the access. There are roles based access controls in place that limit access to data by the job function assigned to each individual.

There are no current technological controls within the MPD to detect if a breach has occurred within the BWC portal. To compensate, MPD conducts data analysis to determine if there are any anomalies within the system. The data analysis could potentially detect unauthorized access and data exfiltration. Wildcard also observed that while there are measures in place for breach detection, there is no cohesive plan for response to a breach.

Analysis - The roles defined with the portal are fine tuned and restrictive. The number of administrators within the system have been limited to specialized personnel. While interviewing personnel, Wildcard observed that removal of access to the system after personnel have been terminated may take an extended amount of time. Wildcard took a sample of MPD personnel who are no longer with the department over the audit period and collected the termination date. We then compared the termination date with the day the user's access was removed. We determined that it took an average of 38 days to remove access to the sample of users.

Wildcard interviewed some personnel assigned the administrator role in the web portal. Some indicated that they did not fully understand their role in administration of BWC. Those admins rarely logged in or accessed the system.

Recommendation **-**Wildcard recommends a review of the administrators of the system. The MPD should evaluate if those users have appropriate access and have been appropriately trained.

Wildcard recommends the creation of an incident response plan that is implemented throughout all MPD Technology units. The plan should include key stakeholders throughout the city to establish instructions to respond to and recover from an incident.

Wildcard recommends that BWC administrators create a workflow that includes Human Resources to reduce the amount of time separated personnel have access to the BWC web portal. The goal should be to remove access to all of the IT assets at the moment of separation.

Management Response – MPD is working with Information Technology and the City Clerk's office to establish a department wide incident response plan to supplement their detection capabilities. Incident handling is currently institutional knowledge but MPD is actively working to establish more formalized processes. City IT will take the lead on an incident response plan. Once completed, MPD will collaborate with City IT and the Clerk's office to assure we fit within the enterprise-wide plan. Minneapolis City IT anticipates an incident response plan to be in place by the first quarter of 2020.

Removing access of separated personnel is a process that must be manually done in evidence.com. Notification from HR of a person's separation can come 3-4 months early, or it can be immediate. MPD has begun using a calendar notification system to create automated reminders of when a person is separating. This will assure that an administrator is given a timely notice to deactivate access. MPD will work with HR when notification isn't made in a timely manner.

BWC Use

Observation – MPD personnel are only authorized to use MPD issued equipment for recording. In the event of equipment failure, supervisors advise their officers to report the issue to the Technology Unit. The Technology Unit is responsible for servicing the units, replacing units, and putting units into rotation for officer use. The Technology Unit is not available during all shifts worked by MPD personnel. In instances where technology unit personnel are unavailable, supervisors tend to select from three options:

- Pair officer with one with a working camera
- Assign officer the camera of an officer that works a different shift
- Keep the officer in the station until camera is fixed/replaced

Analysis - Wildcard interviewed BWC users and administrators and determined that MPD personnel have been trained to not use any equipment other than issued equipment. MPD policy states that supervisors have discretion in the handling of failed BWC equipment. Due to the latitude provided by policy, supervisors have taken a variety of actions in the handling of failed equipment.

Recommendation - Wildcard recommends that MPD develops a program to provide spare BWC equipment to personnel who work shifts outside of technology unit hours. The additional units would mitigate risks of personnel who may be out in the field without one. It would allow personnel to remain in rotation instead of limited to the office.

Management Response – MPD is currently developing a spare camera program. MPD will provide spare cameras to officers along with training for personnel on how to provision cameras for use. MPD expects the spare cameras and training to be available by January 1, 2020.

BWC Procurement

Observation – The MPD has a procurement process in place that integrates the requirements associated with Statute. There have not been any major procurements by the MPD that fall within the audit period.

Recommendation - None

Appendix A: Methodology

Audit Objectives

Two audit objectives were identified for the biennial audit of the Body Worn Camera (BWC).

- Assess the Minneapolis Police Department (MPD) use of BWC to determine it's compliance with Minnesota statute 13.825.
- Review, examine, and assess MPD policies and procedures for the operation of BWC to determine if there are any potential for improvement to support compliance efforts and operation.

This audit is a biennial audit mandated by state law. Our findings are that MPD operates in compliance with state statutes. The recommendations that are included in this report are supplemental to BWC compliance. To ensure a wide coverage for compliance assurance, interviews were conducted with BWC administrators, system logs and settings were evaluated, policy was reviewed, and training materials were assessed.

The methodology used during the audit has been refined using well known frameworks integrating:

- American Institute of Certified Public Accountant (AICPA)
- Information Systems Audit and Control Association (ISACA)
- Control Objectives of Information Technology (COBIT)
- Infrastructure Library for Information Technology (ITIL)

The audit was conducted in three distinct phases:

- During the Planning phase criteria were developed to support the audit objectives and an audit program was produced to identify the information that will be collected during the audit execution phase.
- During the Execution phase artifacts were collected to evaluate relevant information (interviews, document reading, and log/system evaluation) on the BWC operational functions.
- During the Reporting phase, information analysis is finalized. Findings are presented in draft report and presented to stakeholders for evaluation. Stakeholders have the opportunity to review findings and provide a rebuttal. We then finalize the report and structure working paper files.

Appendix B: Interviewed Roles

- 3 System Administrators
- 30 Supervisors
- 1 Data Analyst
- 2 Record Management Specialist