METRO TRANSIT POLICE DEPARTMENT BODY-WORN CAMERA AUDIT REPORT

October 2026

METROPOLITAN COUNCIL

Contents

Highlights 3
Summary of Findings 4
Introduction 9
- Background 9
- Objective 10
- Scope 10
- Methodology 11
- Limitations 12
- Recognition 12

Biennial Review 13
Non-Finding Observations 16
Observations 19
- Section One: Policies and Procedures 19
- Section Two: Footage Review 33
- Section Three: Redaction and Release 42

Conclusions 48
Appendix A: Follow-Up Categories 49
Appendix B: Acronyms 50
Appendix C: Distribution List 51

Highlights

The Body-Worn Camera program has room to improve documentation and oversight.

What We Found

What's Working Well

MTPD Policy 472 contains all required elements. Auditors found no unauthorized access to footage. Arrests were recorded consistently. Department leadership was receptive to feedback and often mentioned willingness to improve.

What Needs Improvement

Auditors found gaps in oversight, administrative controls, and daily procedural compliance.

Department policy is inconsistent with Met Council policy and lacks procedural details. Oversight controls are weak - supervisory review criteria are undefined and are not used to effectively detect training opportunities.

Officers are not always activating, deactivating, or performing pre-shift tests in conformance with policy. Videos were miscategorized or missing case numbers. MTPD lacks periodic BWC refresher training and knowledge checks after policy updates.

Administrative controls require improvement. Redaction and release data was not retained, and one released video included unredacted identifying information. User accounts are not inactivated as quickly as they should be. Hardware inventory is maintained by the vendor.

What We Recommend

MTPD should begin giving periodic refresher training addressing areas of weakness identified in this audit: activation, deactivation, and pre-shift function tests. Staff should write formal procedures, especially for critical areas such as supervisory reviews and redaction and release. MTPD policy and Met Council policy should be brought into alignment with one another. MTPD should conduct regular hardware inventories and improve the account inactivation process to reduce the time from termination to deactivation.

Why We Did This Work

Minnesota State Body-Worn Camera (BWC) law requires an audit every other year for all agencies that use them. Other audits in the past did not include footage review and took a higher-level look at the program. Due to financial, compliance, legal, and reputational risks, auditors decided to do a more in-depth review for this biennial audit.

What We Reviewed

Audit used two scopes. The first covered the entire two-year period since the last biennial audit. More specific testing, not required in the biennial, focused on a shorter period. This review excluded squad car and facility footage and focused only on officer footage, not CSO or TRIP agents.

How We Did This Work

Auditors reviewed stratified samples of footage to ensure compliance with MTPD policies including activation, deactivation, and categorization, among other testing areas. Other video-based tests included sampling shifts to see if officers recorded pre-shift function tests and sampling from a list of dispatch calls to confirm officers activated BWCs when responding to calls.

Auditors also attended BWC training, conducted interviews with staff, reviewed data requests, analyzed other metadata, and compared policy documents.

Summary of Findings

Number	Description	Recommendations	Follow-up Action	Page
Section One: Policies and Procedures				
Observation 1	MTPD BWC policy provides limited operational guidance and lacks formal standard operating procedures (SOPs).	The MTPD should establish and formally approve centralized BWC procedures that translate Policy 472 and applicable statutory requirements into specific operational requirements, including responsibilities, processes, timelines, and key definitions.	Confirmation	*19*
Observation 2	The BWC policy publicly available on MTPD's website was out of date.	The MTPD should implement a policy update process to ensure all publicly available BWC policies and references remain current and consistent.	Confirmation	*21*
Observation 3	MTPD's BWC policy does not align with Metropolitan Council's policy governing the responsibility for the biennial audit.	The MTPD should clarify responsibility for the biennial audit by updating the MTPD policy manual to reference and align with Council Policy RF 6-2.	Confirmation	*22*

Number	Description	Recommendations	Follow-up Action	Page
Observation 3 (cont.)	MTPD's BWC policy does not align with Metropolitan Council's policy governing the responsibility for the biennial audit.	The MTPD should request review from organizational Subject Matter Experts (SMEs) outside of the MTPD in the policy revision and review process (e.g., Office of the General Counsel (OGC) for legal matters or the Data Practices Office (DPO) for retention and release) before policy approval and adoption.	Confirmation	22
Observation 4	MTPD does not provide periodic refresher training as required by Policy 472.	The MTPD should provide BWC refresher training on a periodic basis and to accompany major policy changes and track officer completion.	Confirmation	24
Observation 5	Supervisory review uses inconsistent criteria and is not reported accurately.	The MTPD should establish and maintain documented procedures that define the criteria supervisors must use when reviewing BWC footage, including review expectations, checklist definitions, escalation requirements, and notification responsibilities.	Confirmation	26
Observation 6	The Training Manager does not conduct required quarterly footage reviews.	The Lieutenant of the Training Unit should begin conducting and documenting random quarterly reviews of BWC footage.	Confirmation	28

Number	Description	Recommendations	Follow-up Action	Page
Observation 7	Separated and transferred employee accounts were not inactivated in a timely manner. However, compensating controls prevented unauthorized access.	MTPD administrators and the Local Agency Security Officer (LASO) should work with IS to re-examine the feasibility of using single-sign-on (SSO) for Evidence.com and any other relevant MTPD systems, to reduce the need for manual inactivation. If it is not possible to set up SSO, this team should research other options beyond the payroll reports to reduce the time an account may remain active after an employee terminates or transfers.	Confirmation	29
		MTPD administrators should resume regular and documented reviews of all users at a defined interval, in addition to any as-needed account inactivation.	Confirmation	
Observation 8	An accurate, independent inventory of BWC hardware is not maintained or reconciled at regular intervals.	The MTPD should maintain an inventory of hardware outside of Evidence.com using an appropriate asset management system and perform and document inventories at regular intervals at least annually to ensure accurate and complete inventory.	Confirmation	31

Number	Description	Recommendations	Follow-up Action	Page
Section Two: Footage Review				
Observation 9	Approximately 10% of BWC videos reviewed showed late activation, and approximately 10% showed premature deactivation.	The MTPD should implement regular monitoring of supervisory reviews of BWC footage to identify and address recurring activation and deactivation timing issues.	Confirmation	34
Observation 10	Approximately 16% of BWC videos reviewed were miscategorized, and 11% were missing associated case or incident ID.	The MTPD should create clear definitions of categories for officers to refer to and should clearly define how officers are supposed to use the auto tagging feature in Evidence.com. These definitions should be incorporated into onboarding and periodic refresher training.	Confirmation	36
		The MTPD should implement a control to ensure all footage tagged as evidentiary is associated with a valid case number.	Confirmation	
Observation 11	Pre-shift function tests were performed 29% of the time (17/58) and are not reviewed.	The MTPD should establish a process to monitor PFT completion and compliance, in accordance with policy.	Confirmation	38
Observation 12	In approximately 28% (18/63) of computer-aided dispatch (CAD) calls reviewed with citizen contact, officers did not activate their BWC.	MTPD should strengthen monitoring of activation compliance by implementing periodic reviews of CAD calls to ensure footage exists for all enforcement activities.	Confirmation	40

Number	Description	Recommendations	Follow-up Action	Page
Section Three: Redaction and Release				
Observation 13	Auditors cannot verify compliance with Minnesota Government Data Practices Act (MGDPA) timely release requirements due to a manually maintained BWC release tracker that is incomplete and inaccurate.	The MTPD should work with DPO to make use of the existing data request portal to improve tracking.	Confirmation	*43*
Observation 14	Request records are incomplete and only retained for six months, which does not align with the Council's records retention schedule.	The MTPD should create an archive to store requests and related documents and communication for six years to align with Council Policy.	Confirmation	*44*
		The MTPD should implement periodic supervisory reviews of release requests to ensure documentation is maintained.	Confirmation	
Observation 15	One instance of identifying information was unredacted from released BWC footage.	The MTPD should work with DPO to establish an SOP that defines what must be redacted.	Confirmation	*46*
		The MTPD should implement a secondary review of BWC footage before release to ensure all required information has been properly redacted.	Confirmation	

Introduction

Background

The Metro Transit Police Department (MTPD) is a rapidly growing department within Metro Transit (MT), a division of the Metropolitan Council (Met Council). In 2025, the MTPD employed 133 sworn officers supported by several civilian staff and Community Service Officers (CSOs). Over the past decade, Body-Worn Cameras (BWCs), also known as portable recording devices, have become common in police departments across the country. The MTPD's BWC program began in September 2020 with 270 Axon Body 3 cameras, unlimited cloud storage for video footage, and camera replacements after 2.5 years. The MTPD renewed its initial $2.28 million contract for $1.73 million in 2025. The MTPD currently maintains 259 BWC devices. The BWC program is supported by Axon's third-party platform Evidence.com, which manages video storage, access controls, audit logs, and data retention.

The decision to adopt BWCs was driven by several purported benefits of BWCs, including accountability and transparency. In January 2020, prior to implementation, as required by statute, the Met Council solicited public comments on the BWC policy. The Met Council's BWC Policy, RF 6-2, cites three primary objectives for the program: to increase trust between police and the communities they serve, to reduce confrontations and complaints against police, and to provide another source of evidence for criminal investigations and prosecution. MTPD Policy 472 is the current departmental policy that guides the BWC program.

In addition to the staff in the MTPD Police Business Systems unit, the BWC program is supported by different administrative groups with core responsibilities including policy administration, information technology and security, and records management. Operational oversight of the BWC program includes supervisory review of recordings, a Use of Force Review Board, and Internal Affairs (IA) investigations.

In 2026, IA established a new position, the Police Accountability Liaison, who supports accountability through community-facing engagement, assistance with complaint intake, and monitoring of accountability-related standards, including accreditation requirements. The Data Practices Office (DPO), housed within the Met Council's Office of General Counsel (OGC), occasionally plays an advisory role for the BWC program.

Many states, including Minnesota, have codified requirements for BWC programs based on best practices. One statutory requirement in Minnesota is a biennial audit report. In 2022 and 2024, Lynn Lembcke Consulting completed the required biennial audit which reviewed compliance with Minnesota Statutes, section 13.825 "Data Practices: Portable Recording Systems"[1] and section 626.8473 "Criminal Procedure; Peace Officers; Privacy of Communications: Portable Recording Systems Adoption; Written Policy Required".[2] These statutes cover compliance requirements, which include classifying data as public, private, or nonpublic; data retention and deletion; limiting data access to data subjects; maintaining inventory; and the requirement to publicly post a BWC policy, among other items. The 2022 audit identified no findings, while the 2024 audit identified one finding related to

---

[1] Minnesota Statutes, section 13.825. *https://www.revisor.mn.gov/statutes/cite/13.825*
[2] Minnesota Statutes, section 626.8473. *https://www.revisor.mn.gov/statutes/cite/626.8473*

MTPD's policy not meeting the minimum requirements of Minnesota Statute, section 626.8473, Subd. 3(b)(3). The statute requires BWC policies to address officers' obligations to use issued recording systems in accordance with agency policy when working under another agency's command.[3] The last biennial audit was performed September 5, 2024, and covered the period August 16, 2022, through August 31, 2024. It was not submitted until January 18, 2025.

During the audit, the MTPD experienced significant turnover and restructuring, resulting in changes to roles and responsibilities. At the initiation of this audit, the Police Business Systems Manager held primary responsibility for the BWC program and reported to the Captain of Support Services, who in turn reported to the Chief of Police. The former Police Business Systems Manager moved to a new role during the audit. The Police Data and Evidence Manager, who reported to the Police Business Systems Manager, was unexpectedly absent on extended leave. Other positions also changed, and the Chief of Police moved from an interim to a permanent position.

Objective

In addition to fulfilling the statutory requirement for a biennial audit, auditors reviewed information technology general controls (ITGCs), compliance with internal Met Council policies, and the extent to which MTPD policy incorporates best practices. The four objectives were to:

1. Review MTPD policies for alignment with best practices and state law.
2. Assess MTPD staff compliance with internal BWC policies and procedures including but not limited to Council Policy RF 6-2 and MTPD Policy 472.
3. Identify and assess ITGC regarding footage access, system security, and data integrity.
4. Determine and assess how BWC footage is systematically reviewed, logged, and monitored internally by the MTPD.

This audit considered the guiding principles from the Met Council, including Imagine 2050 Regional Values of Equity, Accountability, and Stewardship. This audit also supports the Experience strategic priority from the Metro Transit Forward Framework, which commits to "provide a consistently safe, clean, and welcoming experience on our system."[4] This is in line with Metro Transit's 2022 Safety & Security Action Plan, a multi-year strategy to improve rider experience. [5]

Scope

This fulfills the biennial audit requirement by reviewing statutory compliance during the period September 1, 2024, until August 1st, 2026, the end of testing. Review areas include:

Minnesota Statute, section 13.825[6]

- Data Classification

---

[3] Independent Audit Report, January 18, 2025 Lynn Lembcke Consulting *250543.pdf* "the policy includes all minimum requirements of Minn. Stat. § 626.8473, Subd. 3 with the exception of Subd. 3(b)(3)."
[4] Metropolitan Council. (2025). *Regional vision, values, and goals*. Imagine 2050. *https://imagine2050.metrocouncil.org/reference-materials/regional-vision-values-and-goals/*
[5] Metro Transit. (2022). Safety & Security Action Plan. Metropolitan Council. *https://www.metrotransit.org/public-safety*
[6] Minnesota Statutes, section 13.825 *https://www.revisor.mn.gov/statutes/cite/13.825*

- Retention of Data
- Access by Data Subjects
- Inventory of Portable Recording System Technology
- Use of Agency-Issued Portable Recording Systems
- Authorization to Access Data
- Sharing Among Agencies

Minnesota Statute, section 626.8473[7]

- Public Comment
- Portable Recording System Policy

This audit also reviewed camera, video, and system records related to MTPD officer BWC activity in more detail for a more limited period from August 2025 to the end of testing, August 1, 2026.

Minnesota Statutes, section 13.825 defines "portable recording system" 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;” Squad car footage, interrogation footage, and building surveillance footage are not included in this definition and were excluded from the scope. [8]

Community Service Officers (CSOs) and Transit Rider Investment Program (TRIP) agents were not included in the review. TRIP began in Spring 2023 in response to new State laws. TRIP agents are civilian MT employees who can board vehicles, conduct fare checks, lead customer education efforts, and issue administrative citations for non-payment. TRIP agents operate outside the MTPD and did not use BWCs during the period under review.

Methodology

This report was prepared for the MTPD by the Program Evaluation and Audit Department of the Met Council, an independent audit function. This audit was conducted in accordance with IIA (Institute of Internal Auditors) Global Auditing Standards.[9]

Auditors received and reviewed policies, training material, and other supporting documentation. Unlike previous biennial audits, testing included footage review to verify that BWC policies for usage, classification, and retention are being followed. Reports and videos were viewed by auditors directly in Evidence.com. Auditors interviewed administrative staff in addition to five structured qualitative interviews with supervisors. Auditors also observed one training session and observed the redaction and release process.

Various sampling methods were used depending on the objective of the test including random, stratified, and interval sampling. While principles of statistical sampling were used to choose sample size, results are not necessarily intended to be projected to or representative of the population. Due to

---

[7] Minnesota Statutes, section 626.8473 *https://www.revisor.mn.gov/statutes/cite/626.8473*
[8] Minnesota Statutes, section 13.825 *https://www.revisor.mn.gov/statutes/cite/13.825*
[9] The Institute of Internal Auditors. (2024). *Complete global internal audit standards*. *https://www.theiia.org/en/content/standards/complete-global-internal-audit-standards/*

the many specific tests completed in this audit, further detail on methodology is included in the observations section of this report.

Limitations

Portions of the ITGC review were limited to review of certifications rather than first person confirmation. This is because the MTPD primarily relies on BWC security controls provided by a third-party, Axon.

Incomplete and error-prone redaction and release tracking, along with the lack of retained source documents, prevented auditors from confirming that the MTPD responded to public data requests in a timely manner.

Computer-Aided Dispatch (CAD) call sampling was done with random interval sampling because the data was not available in an accessible or readily useful format (PDF only). Data had to be manually entered, and auditors needed to resample due to initially unclear definitions of types of calls, and which instances involved citizen contact. Audit relied on MTPD staff to help determine which labels were likely to relate to citizen contact. The reduced sample size, lack of clear definitions, and interval sampling methodology reduce the generalizability of results.

Recognition

The audit team would like to acknowledge the responsiveness and onsite support provided by MTPD staff. Specifically, we appreciate the time, effort, and collaboration of the Police Business Systems, Internal Affairs and Accountability, and the Professional Standards departments. We would also like to thank the Police Accountability Liaison for their coordination efforts. Many employees expressed their appreciation for audit work and the opportunity to implement recommendations as the department seeks continuous improvement.

Biennial Review

Section Summary

The following section details the required review areas for the biennial audit.[10] Auditors noted no discrepancies in the maintenance of recording system data, data classification, data use, or retention.

Portable Recording System Data

According to Minnesota statute, "[a] law enforcement agency must maintain records showing the date and time portable recording system data were collected and the applicable classification of the data." Auditors reviewed the "Evidence Created Report," which documents when portable recording system data were collected and deleted and how the data were categorized.

Data Classification

According to Minnesota statute, the biennial audit must "determine whether data are appropriately classified." BWC data is presumptively private and thus is classified as private or nonpublic data. Two data releases with redactions were made in 2026 and three were made in 2025 to data subjects. Auditors reviewed all five redacted releases. MTPD staff are instructed to verify the identity of data subjects before the release of footage and to redact non-consenting individuals.

Data Use

According to Minnesota statute, the biennial audit must review "how the data are used". Auditors reviewed MTPD policy, conducted interviews, and reviewed documentation to determine how BWC data is being used. The Evidence.com Sharing Audit Report, Audit Trails, and data request file all document data use.

Officers may view their own footage as needed to classify the footage and write reports. IA receives complaints through multiple channels and may review BWC footage. Supervisors also conduct routine random reviews of BWC footage and escalate potential policy concerns to IA as appropriate. Supervisors may review footage relating to use of force that occurs during their supervising shifts. Investigations involving critical incidents, such as those resulting in death or serious bodily harm, follow a distinct process that includes review by external investigative agencies prior to any internal administrative investigation. Policy requires the Training Manager to conduct quarterly reviews, and the MTPD may use BWC footage for training; however, the MTPD does not currently use footage for this purpose.

Data Retention

According to Minnesota statute, the biennial audit must determine "whether the data are destroyed as required." Auditors confirmed that inventory records, destruction, and deployment records are maintained in Evidence.com. The "Evidence Created Report" generated in Evidence.com includes the date and time evidence was created or deleted. Auditors reviewed audit trails for a sample of released

---

[10] Minnesota Statutes, section 13.825 subdivision 9. *https://www.revisor.mn.gov/statutes/cite/13.825*

footage that document every action taken, and this audit trail is maintained after data has been deleted.

At the conclusion of a BWC recording, officers add metadata tags including categories, to the recording. Supervisors perform random reviews to monitor proper categorization of BWC data. Retention schedule for video exists by category, and deletion is automatically tracked and completed at the end of a video's assigned retention period.

The retention policy meets the minimum statutory retention requirements as "Test/Accidental/Non-evidentiary" is maintained for the minimum of ninety days, deadly force is maintained indefinitely under the "Homicide/CSC/Arson/Death" category, and all other footage is maintained for a minimum of one year (**Table One**).[11]

Table One: Retention Schedule

Category	Retention
Uncategorized	1 year
Academy	1 year
Admin Hold	7 years
Arrest/Cite/Investigation/Evidence	7 years
Call for Service/Citizen Contact	2 years
Critical Incident/OIS	7 years
Firing Logs	7 years
Homicide/CSC/Arson/Death	Until manually deleted
Pending Review	7 years
Test/Accidental/Non-Evidentiary	90 days
Traffic/Accident Investigation	7 years
Use of Force	7 years

Authorization to Access Data

According to statute, the biennial audit must confirm adherence to Minnesota Statutes, section 13.825 subdivision 7, 13.05, subdivision 5, and section 13.055. MTPD's BWC policy governs access to and sharing of BWC data. MTPD personnel are allowed to access BWC data only when there is a business need for doing so. Access to BWC data is captured in the audit trail. User access to BWC data is managed by the assignment of roles and permissions in Evidence.com. Roles and permissions are administered by the Police Business Systems Unit Manager. Permissions are based on staff work assignments. Auditors reviewed user access permissions and found no unauthorized access, however a finding later in this report describes delays in account deactivation after employee termination *(Observation 7)*. Access to Evidence.com is password protected and requires dual authentication. The MTPD disclosed no security breaches.

[11] Minnesota Statutes, section 13.825 subdivision 3. Retention of data. *https://www.revisor.mn.gov/statutes/cite/13.825*

Sharing Among Agencies

According to Minnesota statute, the biennial audit must also verify compliance with Minnesota Statutes, section 13.825 subdivision 8. MTPD's BWC policy allows for the sharing of data with other law enforcement agencies for legitimate law enforcement purposes only, for example with prosecutors and other criminal justice entities. Auditors found that nonpublic BWC data is shared with other law enforcement agencies, government entities, or federal agencies in accordance with 13.825 Subd. 8.[12] Law enforcement agencies seeking access to BWC data must submit documented requests in Evidence.com and the MTPD shares BWC data through the Evidence.com secure electronic case-sharing feature. Sharing of BWC data is captured in the audit trail. An Evidence Sharing Audit Report provides documentation of shared data. Auditors sampled and reviewed five Assist Other Agency (AOA) data requests and five discovery requests. All ten releases to other agencies were documented and the agencies receiving the data had been approved in Evidence.com.

---

[12] "Subd. 8.Sharing among agencies. (a) Portable recording system data that are not public may only be shared with or disseminated to another law enforcement agency, a government entity, or a federal agency upon meeting the standards for requesting access to data as provided in subdivision 7.
(b) If data collected by a portable recording system are shared with another state or local law enforcement agency under this subdivision, the agency that receives the data must comply with all data classification, destruction, and security requirements of this section.
(c) Portable recording system data may not be shared with, disseminated to, sold to, or traded with any other individual or entity unless explicitly authorized by this section or other applicable law."

Non-Finding Observations

Section Summary: Auditors reviewed MTPD policy for conformance with additional statutory requirements not required as a part of the biennial audit described in Minnesota Statutes, section 13.825 subdivision 9. Auditors performed a review of ITGCs and reviewed policy against best practices established by the Bureau of Justice Assistance (BJA). These reviews resulted in no formal findings.

MTPD BWC policy conforms with requirements of Minn. Stat. § 626.8473.

Auditors compared MTPD BWC Policy 472 to the requirements of Minnesota Statutes, section 626.8473. The agency's policy includes all minimum requirements of Minnesota Statute, section 626.8473, subdivision 3. The BWC policy is posted on the agency's website in two locations. One posted copy of the policy was of an older version (451) but was updated to the new Policy 472 before the conclusion of the audit.

Lexipol, a third-party platform, maintains the policy manual governing the BWC program. Policies are updated in response to legislative changes, best practices, accreditation standards, and operational needs. The Chief of Police has final approval authority and delegates policy management to the Policy Analyst. Subject matter experts review updates against Minnesota statutes before adoption. The department maintains separate policies for BWC and other video technologies, with public-facing policies posted separately on its website.

MTPD BWC policy meets the scorecard threshold set by the Bureau of Justice Assistance (BJA) with a score of 92%.

The BJA is an organization whose focus is to provide policy development resources, training, and technical assistance for police departments. The BJA produces a scorecard tool for police departments to review their BWC policies. The scorecard's intention is to grade police departments' BWC policies to promote best practices. Auditors used the BJA scorecard to determine if MTPD's Policy 472 meets best practices and standards. The scorecard has 11 categories that cover different parts of a policy (**Table Two**). Within these 11 categories, there are 45 elements. 17 of the 45 elements are mandatory. Policy 472 met 92% of all elements on the scorecard and 100% of the required elements

Of the 11 scorecard categories, five received less than a perfect score: BWC Viewing, Data Transfer/Download, Public Release, Policy Development, and General Issues (**Table Two**). For elements where Policy 472 partially met the best practice described, the auditor gave a score of 0.5. For items where Policy 472 did not meet the best practices described, the auditor gave a score of 0.

Three categories contained partially conforming elements:

1. The *BWC Viewing* category partially conformed with the element requiring policy to specify the authority and conditions for IA review of BWC footage. Policy 472 addresses neither, but Policy 601 contains language that staff may only access footage when there is a business need.
2. The *Data Transfer/Download* category partially conformed with the element that asks if the BWC policy includes specific incident types or categories to properly tag videos. While

Policy 472 has exact specifications for sensitive circumstances or events, it does not include definitions for other types of tags an officer might use (*Observation 10*).

3. The *Public Release* category was partially conforming because one element requires the policy to be publicly available, however the MTPD website had a link to an old version of the policy (*Observation 2*).

Table Two: Breakdown of Score by BJA Scorecard Categories

BJA Scorecard Policy Categories	Possible Score	Agency Score	Did MTPD Meet?
Video Capture-Activation	7	7	Fully Met
Video Capture-Deactivation	2	2	Fully Met
Data Storage/Retention	2	2	Fully Met
BWC Training	1	1	Fully Met
Policy and Program Evaluation	1	1	Fully Met
BWCs and Use of Force	1	1	Fully Met
BWC Viewing	9	8.5	One Element Partially Met
Data Transfer/Download	6	5.5	One Element Partially Met
Public Release	6	5.5	One Element Partially Met
Policy Development	6	5	One Element Not Met
General Issues	4	3	One Element Not Met

Two categories contained an element that did not meet best practices:

1. The *Policy Development* category did not conform because one element requires community engagement in policy development. MTPD lacked documentation regarding conversations or meetings happening between the MTPD and community groups during the development of Policy 451 and 472.
2. The *General Issues* category did not conform with the element requiring clear conditions for the voluntary wearing of cameras. Policy 472 lacks explicit wording on requirements and conditions for required and voluntary wearing of BWC. Although the policy has requirements for BWC activation, it does not describe conditions when wearing a BWC is required versus voluntary.

The MTPD and the vendor's IT general controls for BWC data are adequate.

The MTPD established a reasonable IT control environment through a combination of internal controls and the vendor's security controls as a third-party provider. Auditors directly experienced a number of these controls to complete the work. The vendor was not directly screened by the MTPD, but has contractual commitments related to Criminal Justice Information Services (CJIS) requirements. The vendor was also reviewed by both the Bureau of Criminal Apprehension (BCA) and SourceWell prior to the MTPD selecting them to handle BWC data.

Minnesota statute requires vendors providing BWC services or storing the data to "protect the data in accordance with the security requirements of the United States Federal Bureau of Investigation CJIS Division Security Policy 5.4 or its successor version." Among others, current CJIS Policy requires:

- Access controls and account management
- Failed login responses
- Limiting and managing remote access, including for mobile devices
- Prohibiting the use of personal mobile devices
- Audit Logging

The MTPD has several internal controls over BWC data, in addition to security controls provided by a third-party. There is a designated Local Agency Security Officer (LASO) who has expertise in information security.

In the section on Use of External Systems (section AC-20), the CJIS standard discusses third parties and states "organizations need assurance that the external systems contain the necessary controls so as not to compromise, damage, or otherwise harm organizational systems. Verification that the required controls have been implemented can be achieved by external, independent assessments, attestations, or other means, depending on the confidence level required by organizations."

The MTPD procured Axon as a vendor through Sourcewell, a State of Minnesota Cooperative Purchasing Venture (CPV). A benefit of using CPVs is that the State can establish a uniform set of terms and conditions and pre-screen vendors for responsiveness and responsibility. Pre-screening responses for this particular contract include a list of several certifications the vendor holds, including in CJIS and other related compliance areas. Additionally, the BCA maintains a list of technology vendors they screen, which includes the BWC vendors.[13]

The contract terms state that Axon "agrees to the [CJIS] Security Addendum." Axon also provides White Papers outlining controls. Their Cloud Services Security paper and CALEA Standard paper include statements on:

- Data encryption in transit and while at rest
- Data storage designed for 99.99999999999999% durability^
- Role-Based Access Control with granular role-based permissions*
- Single-Sign On availability*
- Multi-Factor Authentication*
- Password requirements* and the ability to customize failed login responses^
- Audit Logging*
- Data storage redundancy to support disaster recovery

*Items marked with * in the list above indicate features auditors directly observed while performing testing. Items marked with ^ indicate features auditors did not directly observe, but that were mentioned in conversations or emails with staff.*

[13] Minnesota Department of Public Safety. (n.d.). *Vendor screening program*. Bureau of Criminal Apprehension. https://dps.mn.gov/divisions/bca/bca-divisions/criminal-justice-information-services/vendor-screening-program

Observations

Section One: Policies and Procedures

Methodology:

This section covers a range of tests that auditors performed including reviewing policies against state statutes, assessing how policies are put into practice, and evaluating the surrounding controls such as supervisory review and training.

Auditors interviewed MTPD's policy analyst to determine how the policies are drafted and updated. Auditors then analyzed Minnesota Statutes, section 13.825 and section 626.8473 line by line. Auditors compared each requirement against the MTPD's current Policy Manual, focusing primarily on Policies 472, 601, and 810. Auditors assessed adequacy and applicability of the policy language. Auditors also compared the original BWC Policy 451 with current Policy 472 to note differences between the two versions. Policy 472 was also compared to Met Council Policy RF 6-2 to ensure alignment.

Auditors reviewed the BWC training curriculum to confirm alignment with Policy 472. Auditors spoke with the Training Manager in addition to civilian staff responsible for providing initial setup and training for officers. Auditors attended an academy training session and compared the content against areas required by policy. Auditors also interviewed Captains in operations to understand how training continues in the field after the academy. Finally, auditors reviewed the timeliness of officer acknowledgments of policy.

Auditors randomly selected five supervisors and performed semi-structured qualitative interviews and coded the responses to assess for any inconsistencies. Auditors also reviewed supervisory review metadata in Evidence.com and compared it to summary statistics generated and used by the MTPD.

Auditors also tested controls by mapping roles and responsibilities, reviewing user accounts (including roles, termination logs, and comparing a list of current users to current employees) to evaluate controls over access to footage, and assessed the accuracy of inventory. To access inventory accuracy, auditors pulled a report of all physical hardware from Evidence.com and compared to the latest inventory refresh records. Auditors also observed BWC setup.

Observation 1: MTPD BWC policy provides limited operational guidance and lacks formal standard operating procedures (SOPs).

The two statutes that govern BWC use by police agencies are Minnesota Statutes, section 626.8473 and 13.825.

1) Minnesota Statutes, section 626.8473 mandates that "the chief officer of every state and local law enforcement agency that uses [BWCs] must establish and enforce a written policy governing its use." The statute also lists required items that policies must address.

2) Minnesota Statutes, section 13.825 describes practices that agencies must adhere to when they deploy BWCs. The statute outlines requirements for data practices, inventory, the portable recording system vendor, and biennial audit requirements.

MTPD's current BWC Policy 472 addresses the subdivisions outlined in Minnesota Statutes, sections 13.825 and 626.8473. However, Audit's review identified some areas of the policy that have limited operational guidance, including references to statutory provisions without describing the responsible parties, applicable requirements, or procedures needed to implement them. For example, Policy 472 cites Minnesota Statutes, sections 626.8473, subdivision 3(4), and 13.825, subdivision 2(5b), which require the agency to provide data within five days of a request following a death resulting from a peace officer's use of force. However, the policy does not identify who is entitled to make such a request, namely, the deceased individual's next of kin, the legal representative of the next of kin, or the other parent of the deceased individual's child, nor does it specify the five-day timeframe within which the agency must respond. Similarly, Minnesota Statutes, section 13.825, subdivision 2(g), provides an individual with the right to challenge a decision regarding the release or redaction of data by bringing an action in district court. Neither Policy 472, nor Policy 810, nor the broader MTPD policy manual establishes procedures for responding to this right.

These gaps largely stem from MTPD's reliance on Lexipol, a policy management system used to publish policies and receive updates on best practices and Minnesota regulations. According to the Accreditation Manager and Policy Analyst, who manually reviews and approves policy updates, the MTPD has been moving toward less-detailed policies because Lexipol has shifted away from incorporating procedural guidance into its policies. The Accreditation Manager and Policy Analyst also indicated that incorporating statutes by reference reduces the number of policy updates required because statutory changes do not require corresponding revisions to the policy. While incorporating statutory requirements by reference reduces the need for frequent policy revisions, it may also limit opportunities to formally communicate changes in legal requirements through the department's policy review and acknowledgment process. In Minnesota, the legislature convenes annually, and typically laws without appropriations take effect on August 1st.[14] This timeline makes the claimed advantage of incorporation by reference overstated, since statutory revisions would only need to be incorporated annually.

Written policies and procedures are foundational for any control environment. They ensure continuity during staff changes and ensure consistent application of the policy. Although the MTPD has reduced the level of procedural detail in its policy manual, it has not developed formal SOPs to fill the resulting gaps. Some MTPD staff such as the Principal Administration Specialists have developed their own informal work instructions to guide specific BWC-related activities, but the MTPD has not formally adopted or approved these instructions as department-wide procedures.

A lack of detailed SOPs increases the risk of statutory noncompliance due to increased risk of inconsistent policy adherence. In addition to reputational risks in the community, if the MTPD does not comply with statutory requirements, penalties could be enforced. As outlined in 13.825 subd. 12, "in the case of a willful violation, the government entity shall, in addition, be liable to exemplary damages of not less than $1,000, nor more than $15,000 for each violation." In addition, removal of licenses or temporary restraining orders (pursuant of 214.11) may occur.

---

[14] Minnesota Legislature. (2025, December 22). *Frequently asked questions about the Minnesota Legislature: When do new laws go into effect?* https://www.leg.mn.gov/leg/faq/faq?id=67

Recommendation:

1. The MTPD should establish and formally approve centralized BWC procedures that translate Policy 472 and applicable statutory requirements into specific operational requirements, including responsibilities, processes, timelines, and key definitions.

   Management Response: Agree. MTPD will produce a standard operating procedure for the Body-Worn Camera operations.

   MTPD currently possesses a 13-page policy which consists of sections and subsections on member responsibilities, use, activation, prohibitions, documentation, uploading, tagging, access, retention and key definitions. The department acknowledges that a standard-alone procedure, in addition to the policy, would enhance understanding and provide clear operational guidance.

   Timetable: BWC SOP will be published in Lexipol by end of Q2 year 2027.

   Staff Responsible: Accreditation and Policy Analyst with the support of the Patrol Captains and Police Systems Manager.

   Audit Follow-Up: Confirmation.

Observation 2: The publicly available BWC policy on the MTPD website was out of date.

Minnesota Statute, section 626.8473 subdivision 3. states that "agencies with a written policy must have it posted on the agency's website, if the agency has one." MTPD's policy manual is posted publicly on their website. The MTPD also has a separate page where the BWC policy can be located. Although MTPD's online policy manual reflects the current BWC Policy 472, the BWC webpage directed the public to the outdated Policy 451, which was issued in 2022 and replaced by Policy 472 in late 2025. Before testing ended in July 2026, the MTPD updated their webpage to link the most up-to-date policy, which Audit confirmed by checking the link.

The process for updating MTPD's policies online is both automated and manual. The digital policy manual is updated by the Accreditation and Policy Analyst, who gets policy updates automatically through Lexipol. New policies are given to the Public Safety Senior Communication Specialist, who is responsible for manually updating the website.

If the BWC policy is not updated correctly on the website, staff and members of the public might navigate to the incorrect, outdated policy. Policy 472 and 451 are substantially different from one another, particularly in their expectations for when BWCs should be turned on and when they can be deactivated (*Observation 9* & *Observation 12*). This may lead to confusion and applications of outdated procedures to current law enforcement operations. As a result, staff or members of the public could rely on outdated BWC requirements, increasing the risk of inconsistent practices and noncompliance with current policy and state law.

Recommendations:

1. The MTPD should implement a policy update process to ensure all publicly available BWC policies and references remain current and consistent.

   Management Response: Agree. As noted in the audit report "Before testing ended in July 2026, the MTPD updated their webpage to link the most up-to-date policy, which Audit confirmed by checking the link." MTPD has had internal discussion to ensure policy updates are correctly updated in all public places where they are cross-referenced, including the MTPD webpage.

   Timetable: Completed July 2026.

   Staff Responsible: BWC/Video Supervisor with the support of the Accreditation and Policy Analyst and the Public Safety Senior Communications Specialist.

   Audit Follow-Up: Confirmation.

Observation 3: MTPD's BWC policy does not align with Metropolitan Council's policy governing the responsibility for the biennial audit.

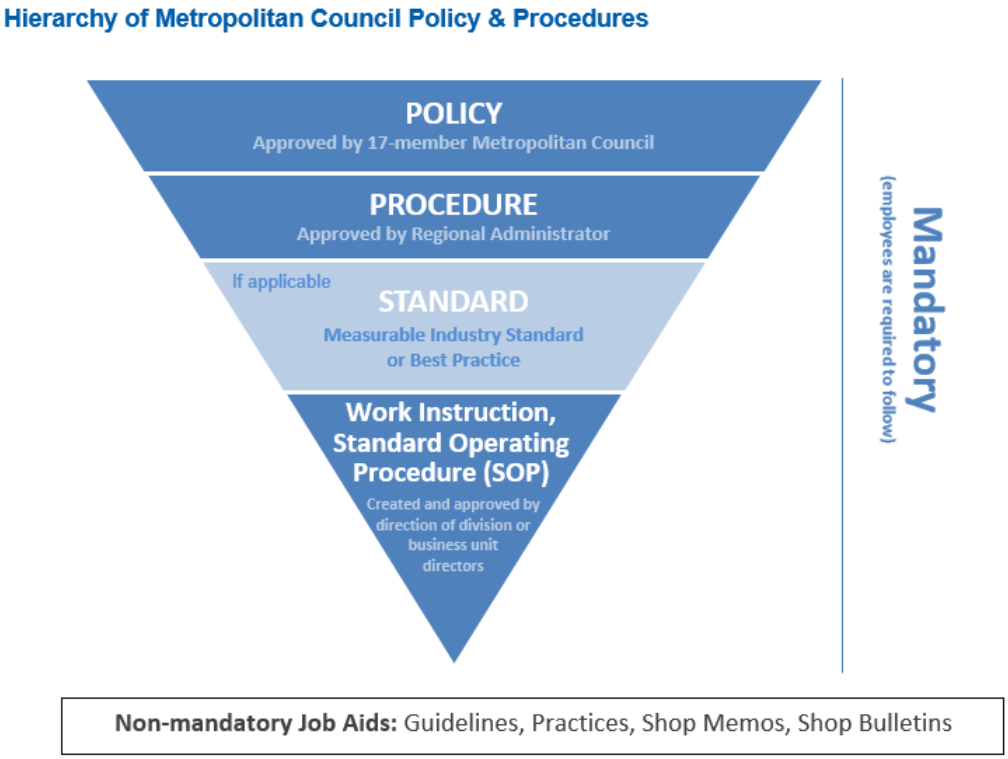
The BWC biennial audit is a core statutory requirement in Minnesota.[15] Currently, Policy 472 states that the Chief of Police is the one to delegate preparation of the biennial audit. However, Council Policy RF 6-2 requires the biennial audit either be completed by "the Council's audit department or another agency as delegated by the audit office." Although the MTPD updated their website to correctly list Policy 472, the Met Council's BWC Policy RF 6-2 still identifies Policy 451 as MTPD's current policy.

Policy RF 6-2 outlines the purpose and scope, the background, and measures for policy implementation. According to Policy RF 6-2, the Chief of Police will appear before the Council as appropriate to provide updates regarding the BWC program and may update the policy at their discretion. While Policy RF 6-2 allows for policy updates, no such updates should directly conflict with the requirements established in Policy RF 6-2. Policy 472 was pushed to subject matter experts within the MTPD to review before distribution to supervisors. There was no formal review process for the new Policy 472, requiring the Office of General Counsel (OGC) to review. According to the Met Council's policy framework, policies are written to "promote mission and values in operational objectives, programs, and activities." Based on the framework (**Figure One**), many MTPD policies are closer to the procedure level.

---

[15] Minnesota Statute, section 13.825 subdivision 9. requires law enforcement agencies to "arrange for an independent, biennial audit of the data." The results must be publicly available, unless there is classified data, and the results need to be presented no later than 60 days after the audit.

Figure One: Policy Framework[16]



Met Council policies supersede all other policies and SOPs. All policies are approved by the 17-member Metropolitan Council. In contrast, the MTPD Policy Manual is subject to final review and approval by the Chief of Police or their designee.[17] Despite allowances being made for policy updates in Policy RF 6-2, a division-level policy that directly conflicts with an organization-wide policy adopted by the Met Council would appear inconsistent with the Met Council's role in establishing governing policy. Maintaining a contradictory policy outside the formal approval process and without Met Council sign-off could weaken the Met Council's policy governance and oversight. Further, if MTPD's policies and SOPs do not align with the Met Council's, there will be confusion on roles and responsibilities for the biennial audit.

Recommendations:

1. The MTPD should clarify responsibility for the biennial audit by updating the MTPD policy manual to reference and align with Council Policy RF 6-2.

2. The MTPD should request review from organizational Subject Matter Experts outside of the MTPD in the policy revision and review process (e.g., Office of the General Counsel (OGC) for legal matters or the Data Practices Office (DPO) for retention and release) before policy approval and adoption.

---

[16] "Policy Framework" MetNet. *https://metcmn.sharepoint.com/sites/PoliciesandProcedures/SitePages/Policy-Framework.aspx*
[17] "MTPD Policy Manual" MTPD Website. *https://www.metrotransit.org/transit-police-policy-manual*

Management Response: Agree. MTPD policy does not fully align with the Council's Body-Worn Camera Policy RF-6 in that although it states that a biennial audit will be prepared in accordance with Minn. Stat. 13.825, Subd.9 (MTPD Policy 472.4.1.12), it does not continue that the statutory biennial audit will be, "conducted by the Council's internal audit office or another agency as delegated by the audit office."

MTPD will Consult with the Office of General Counsel to discuss proposed amendments to both the Council and MTPD policies, to achieve alignment with each other and state law. The Accreditation and Policy Analyst will participate in standing monthly meeting as needed with the Office of General Counsel to discuss proposed policy amendments, and meet with the DPO as necessary, regarding proposed updates to policy that may affect MTPD's data practices operations.

Timetable: End of Q2, year 2027.

Staff Responsible: Accreditation and Policy Analyst, General Counsel, Chief of police.

Audit Follow-Up: Confirmation.

Observation 4: The MTPD does not provide periodic refresher training as required by Policy 472.

The MTPD provides BWC training during the academy and field training program before new officers begin work. Although the MTPD requires officers to attend training, it does not document attendance. Additionally, the MTPD does not provide periodic refresher training after officers complete academy training, even though this is required by Policy 472 (**Table Three**). There is no ongoing training provided unless coaching is recommended. Officers instead acknowledge policy updates through Lexipol by checking a box after reviewing the policy. However, the MTPD does not require officers to demonstrate their understanding of the requirements, such as by taking a short quiz. As a result, the MTPD relies primarily on initial training and policy acknowledgments to communicate changes to BWC requirements. Without ongoing training, officers may not consistently understand or apply BWC requirements, which could increase the likelihood of policy violations and inappropriate use of BWC equipment. For instance, refresher training could cover information about video activation and deactivation (*Observation 9*, *Observation 12*), categorization and case number tagging (*Observation 10*), pre-shift function testing (*Observation 11*), and supervisory review expectations (*Observation 5*).

Auditors attended initial academy training. During the academy training, civilian staff demonstrate BWC operations including activation and deactivation, phone synchronization, and footage uploads. Training Unit officers then review Policy 472 with recruits. Auditors observed the training and compared the instruction with Policy 472. The training presentation incorporated policy language; however, auditors identified several instances where the instruction did not fully align with the policy training requirements (**Table Three**). It is important that training materials and verbal instruction reflect current policy so that officers are consistent in their use of BWCs.

Additional policy areas were insufficiently covered, such as Policy 472.6.1 which requires officers to notify citizens that they are being recorded unless specific circumstances apply. The training did not explain those circumstances or explicitly instruct recruits on when they must provide notice. Policy 472.6.2 instructs officers to mute rather than fully deactivate their BWCs under specified

circumstances. Training officers instead instructed recruits not to mute their BWCs and to narrate the reason for deactivation. The training also did not address when officers should reactivate their BWCs. Policy 472.7.1 establishes requirements for tagging BWC footage. Training did not explain the required event categories, including citizen contact and arrest/citation/investigation (*Observation 9*). Training officers instructed recruits to avoid recording sensitive information, such as medical situations and passwords, but did not explain how officers should appropriately tag footage when they record these or other events.

Table Three: MTPD Policy Requirements and Academy Training Comparison

472.10 Policy Language	Presented in Training and Matched the Policy
Proper use of the BWC device and accessories.	Yes
When BWC activation is required, permitted, and prohibited.	Yes
Security procedures for BWC media including appropriate access and use.	Yes
How to respond to an individual's request to stop recording.	Training officers discouraged recruits from using "stealth" mode, in which the recording light on the BWC does not flash. However, officers were not explicitly told to inform citizens of recording.
Proper use of the BWC media systems, including uploading and tagging procedures.	Training did not explain the required event categories, including "citizen contact" and "arrest/citation/investigation." Training officers did instruct recruits to avoid recording sensitive information, such as medical situations and passwords, but did not explain how officers should appropriately tag footage when they record these or other events.

The changes in Policy 472, which did not include procedural items as it previously had in Policy 451, may have led to these discrepancies. In addition, the MTPD has changed its training structure, so both civilian staff and police officers are providing the academy training sessions. Until June 2026, only civilian staff provided technical BWC training at the Academy. Previously, officers would learn BWC requirements such as activation and deactivation during their field training. Following staffing changes within the MTPD and the BWC unit, both civilian staff and sworn officers now provide training at the Academy. Incorporating practical experience with technical expertise during the academy will help to standardize and strengthen the training program.

Recommendation:

1. The MTPD should provide BWC refresher training on a periodic basis and to accompany major policy changes and track officer completion.

   Management Response: Agree. MTPD will create a training course outlining BWC operations of equipment and proficient usage. This training will include a power point and can include presentations from the Training Unit personnel during in-person or virtual sessions, as well as updates delivered during roll call. The training will be authorized and administered as part of an academy for new officers and annual in-service training for sworn officers and CSOs.

To ensure understanding and accountability between annual in-service trainings, an LOD will be created and distributed via the Learning and Development portal for all Sworn and CSOs annually.

Timetable: BWC LOD will be established by end of Q4 year 2026. In-service completed by end of Q3, year 2027.

Staff Responsible: Captain of Training Unit with the assistance of BWC/Video and support staff.

Audit Follow-Up: Confirmation.

Observation 5: Supervisory review uses inconsistent criteria and is not reported accurately

Supervisory review of BWC footage is performed using inconsistent criteria across reviewers, resulting in reporting that does not accurately reflect actual performance or outcomes. Further, the resulting data is not aggregated or shared in a useful manner, which reduces the value of the supervisory review itself.

Supervisors have informal guidance to review 40 BWC footage videos each month. For each review, supervisors complete a checklist that includes the following checkboxes:

- ✓ Activated Correctly
- ✓ Clear View/Audio
- ✓ Missing ID and/or Category
- ✓ Ended Correctly
- ✓ Correctly Classified
- ✓ Great Performance
- ✓ Late Activation
- ✓ ID and Category Listed
- ✓ No Concern Identified

Although the five supervisors interviewed were consistent in describing the quantity and types of videos they reviewed, they had differing definitions for the checkboxes. For instance, one supervisor described the checkbox for “clear view/audio” as no obstruction, whether intentional or unintentional, while four of the others only considered *intentionally* blocking or muting the BWC as noteworthy. Similarly, one supervisor said officers have discretion about whether their BWCs are activated while a suspect is being transported in a squad car, while four others stated that the BWC must stay on until the suspect transfers custody at the jail.

There is also confusion about the “Refer to Supervisor” function in Evidence.com, specifically about whether to remove the officer being reviewed from the line of notification when a video is flagged for referral. Some supervisors said they were unsure if Evidence.com automatically notifies officers, while others said the reviewee officer would be automatically notified unless reviewers manually redirect the notification to the officer’s supervisor. For the other checkbox fields, some supervisors expressed interest in work instructions and definitions for each field, stating that none are currently documented.

Supervisors’ varying interpretations of each item in the checkbox reduces the value of the supervisory review data. Further, because each supervisor is reviewing footage from officers who do not necessarily report to them, they may not be consistently informed of issues with their direct reports.

Supervisors mentioned looking for patterns of behavior when managing officer performance; however, this relies on other supervisors noting and sharing feedback in a consistent and useful manner.

MTPD administration generates a summary of how many videos each supervisor has reviewed in the Evidence.com module each month, with the expectation each supervisor has reviewed 40 videos.[18] MTPD staff provided auditors with these summary statistics within the audit scope (August 2025 – May 2026) and the raw metadata logs from Evidence.com of each supervisory review completed. In comparing the summary statistics and the raw metadata, auditors found the MTPD is not accurately reporting the number of supervisory reviews completed by each supervisor. Of the 167 monthly records reviewed, 24% were inaccurate. Approximately half of the inaccurate monthly records overreported the number of supervisory reviews completed, and the other half were underreported.

Auditors have been unable to determine the root cause of supervisory review statistics not matching raw metadata from Evidence.com. MTPD staff have not provided an explanation of the procedure they use to compile the summary statistics, nor the source of data they are using to do so. Supervisory review is a control for ensuring officer compliance with BWC policies and to monitor officer performance. Without reliable data, the MTPD cannot ensure the strength of this control.

Recommendation:

1. The MTPD should establish and maintain documented procedures that define the criteria supervisors must use when reviewing BWC footage, including review expectations, checklist definitions, escalation requirements, and notification responsibilities.

   Management Response: Agree. MTPD will produce Standard Operating Procedures (SOPs) that will establish clear expectations for supervisory reviews, documentation, follow-up, escalation, and corrective action. SOPs will also address the following areas:

   - BWC activation and deactivation
   - BWC categorization
   - BWC Pre-Shift Function Testing

   Timetable: Approved SOPs will be published in Lexipol by end of Q2, year 2027.

   Staff Responsible: Production of the SOP will include Patrol Captain, BWC Manager, and Accreditation and Policy Analyst.

   Audit Follow-Up: Confirmation.

Observation 6: The Training Manager does not conduct required quarterly footage reviews

The Lieutenant of the Training Unit, acting in the role of Training Manager, does not conduct quarterly random reviews of BWC footage as required by MTPD policy. In an interview, the Lieutenant told auditors their department was not involved in footage review. Footage review metadata logs also

[18] The MTPD has been unable to provide auditors with the source of the data they use to generate the monthly summaries.

confirm that the Lieutenant of the Training Unit did not conduct random footage reviews during the audit period.

MTPD Policy 472.8.1 specifically states “The Training Manager should conduct a quarterly review of a random sampling of BWC media to evaluate department performance and effectiveness and to identify specific areas where additional training or changes to protocols would be beneficial.”

The MTPD does not have a procedure or work instruction that documents how the Training Manager should conduct these quarterly reviews. The Lieutenant was also unaware of the requirement. Without conducting the required quarterly reviews, the Training Manager cannot fully achieve the policy’s objectives of evaluating department performance and identifying opportunities for additional training or changes to protocols.

Recommendation:

1. The Lieutenant of the Training Unit should begin conducting and documenting random quarterly reviews of BWC footage.

   Management Response: Agree. The MTPD BWC policy 471.8.1.6 states that the Training Manager is permitted to access and view BWC video for “training purposes”. Currently our Training Manager also serves as the Use of Force Board Chair. In policy MTPD policy 302.3.1 it states the Use of Force Board Chair is only supposed to access BWC video for case review at the recommendation of Internal Affairs. With the help of the auditors, MTPD recognized that the terms within policy 471.8.1.6 create a conflict of interest with MTPD policy 302.3.1. MTPD Management will form a workgroup to identify best practices in this area and propose a future policy update.

   Additionally, MTPD does have the supervisor review process which assists with the BWC monitoring process for discrepancies in training and operational issues. Clear direction through a newly established SOP for Supervisor Reviews referenced in observation 5 will enhance protocols for reporting additional training that is needed.

   Timetable: End of Q2 year 2027.

   Staff Responsible: Internal Affairs with support from the Training Unit and Accreditation and Policy Analyst.

   Audit Follow-Up: Confirmation.

Observation 7: Separated and transferred employee accounts were not inactivated in a timely manner. However, compensating controls prevented unauthorized access.

According to the CJIS Security Policy, Law Enforcement Agencies should “disable system access within twenty-four (24) hours” of an employee’s termination or transfer to a new role where that access is no longer needed. The policy also states that access control policies and procedures should exist, and to “notify account managers and system/network administrators within one day when… users are terminated or transferred”. Section AC-2 also states that accounts should be reviewed “at least annually,” and this process should be aligned “with personnel termination and transfer

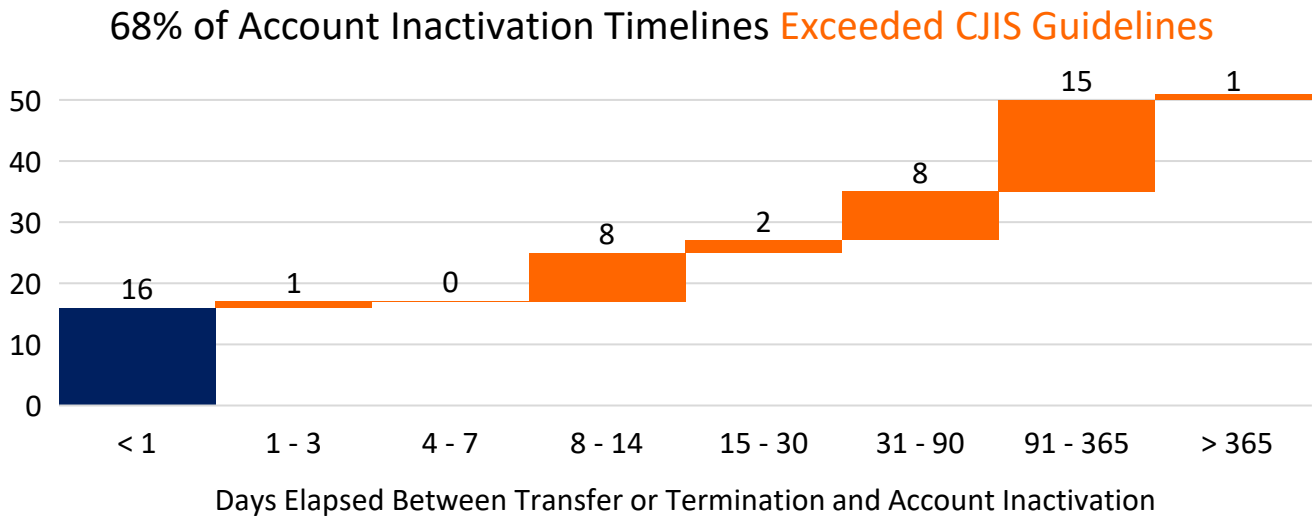
processes." Although BWC footage is not CJIS data in and of itself, Minnesota Statute, section 13.825 subdivision, 11(b) states that vendors storing BWC data must protect it according to CJIS standards.

Met Council standard TECH-01-ST ("Access Control Standard") states that administrators will review accounts annually to "validate that the assigned privileges are appropriate." The standard also lists user management guidelines stating that "supervisors must also inform application administrators of any systems that do not use Active Directory" when an employee's role changes or when their employment ends. For terminated employees, the standard recommends using an automated account to disable an account "immediately" upon "termination, rights revocation, or role change." IS staff confirmed that for terminated employees they work with the service desk to automatically deactivate accounts linked to Active Directory "immediately" and that employees who resign are scheduled for automatic deactivation after their last day. However, Evidence.com accounts are currently deactivated manually.

Separated or transferred employee accounts within Evidence.com were not inactivated in a timely manner. Within scope (September 1, 2024, to March 26, 2026), the MTPD inactivated 51 user accounts. 16 of these (32%) were inactivated within 24 hours of the employee's separation or transfer, while the remaining 35 of the 51 (68%) ranged from three to 411 days (**Figure Two**). Auditors compared the list of current and former users in Evidence.com against a list of current and separated employees and role configurations. 195 of the 201 active employees work for the MTPD, alongside a total of six auditors and IS department staff.[19] All active users have legitimate business need to access the system. No former employees still have access. For former users in Evidence.com, auditors compared the date their account was inactivated with their employee status including job title and date of separation or transfer to a new role, if applicable.

[19] Four auditors required access to complete testing, and two other users work for IS. One of these was a contracted worker. Audit confirmed that this person is authorized to access the system and learned that over the course of testing this person was hired as a permanent Met Council employee.

Figure Two: Days Elapsed Between Transfer or Termination and Account Inactivation



Despite the late inactivation, no employees with old accounts logged into Evidence.com after their termination or transfer date, which means that there was no unauthorized access. However, if an unauthorized employee accessed the system, they could view confidential and protected nonpublic data related to criminal investigations. In addition to potential legal risks related to active investigations, there could be reputational and compliance implications.

There are also financial and operational impacts of keeping old accounts active. Licenses cost between about $500 and $600 each. The MTPD ran out of available licenses in the early stage of this audit and needed to work with Procurement and Axon to purchase additional ones. This led to both operational delays for the MTPD in onboarding new employees and could have limited Audit's ability to complete other tests if not resolved.

The MTPD experienced significant turnover and restructuring within the time period in scope for this audit. Employees previously completed regular reviews of accounts and audit logs, though they did not have access to adjust user roles themselves. After another employee took responsibility for the unit a few years ago, regular (more than annual) user reviews were discontinued based on a claim that they were not necessary. The current employees feel that more frequent user reviews are an important practice, supported the idea of performing more regular reviews, provided evidence of a recent review that was performed, and still do a review at least annually.

Although the MTPD meets the requirement to review users at least annually, as-needed inactivation is done manually and 5 of the 16 days with account deactivations missed at least one user. Of the 51 terminations within scope, 18 should have been caught in at least one earlier review of users. Review accuracy and timeliness generally improved over time, as seen by the more frequent deactivation dates, smaller ranges of days to deactivate, and fewer accounts missed. Currently, account inactivation were based on reports from payroll to inform MTPD administrators of employee position changes, which could result in delays of up to 14 days to inactivate access. It is not likely that terminations or transfers taking effect on weekends are a major driver of late inactivation, as only one of the 35 late inactivation was within the 1-3-day window that would result from a weekend termination and Monday inactivation. Although single-sign-on (SSO) is an option for Evidence.com, it has not

been implemented. SSO would allow the Human Resources and IS offboarding processes to automatically inactivate Evidence.com access without relying on the existing manual process.

Recommendations:

1. MTPD administrators and the Local Agency Security Officer (LASO) should work with IS to re-examine the feasibility of using single-sign-on (SSO) for Evidence.com and any other relevant MTPD systems, to reduce the need for manual inactivation. If it is not possible to set up SSO, this team should research other options beyond the payroll reports to reduce the time an account may remain active after an employee terminates or transfers.

2. MTPD administrators should resume regular and documented reviews of all users at a defined interval, in addition to any as-needed account inactivation.

   Management Response: Agree. MTPD has initiated the transition to SSO for Evidence.com with the support of IS. On 9/22/26 the IS Change Approval Board (CAB) approved this initiative. This board includes LASO Security Team representation. An IS Systems Engineer has been assigned to facilitate the change to SSO. A user access review was conducted in September 2026 and will be conducted on an annual basis as well as any as-needed spot checking to eliminate any separated employee accounts. In addition to HR removing separated employees from the network, payroll has reinforced language to notify supervisors of the requirement to remove user access.

   Timetable: End of Q4, year 2026.

   Staff Responsible: BWC/Video Supervisor.

   Audit Follow-Up: Confirmation.

Observation 8: An accurate, independent inventory of BWC hardware is not maintained or reconciled at regular intervals.

According to Minnesota Statutes, section 13.825 subdivision 5, “A law enforcement agency that uses a portable recording system must maintain the following information, which is public data: (1) the total number of recording devices owned or maintained by the agency;” To fulfill this requirement, the MTPD relies on Axon’s Evidence.com platform to manage its inventory of BWC cameras and docking stations, creating a third-party vendor dependency within the control environment. In lieu of a spreadsheet or asset management system, staff verify inventory during refreshes using the invoices and device serial numbers. This manual inventory is not completed at regular intervals and instead follows the camera refresh schedule, which is typically once every three years.

Auditors reviewed inventory records approximately a month after a recent refresh and found that inventory records were inaccurate, showing approximately double the number of BWCs as the MTPD had on hand. According to the “Device Summary” report, the agency owned 501 BWC devices, but staff reported that this number should have been 259 (**Table Four**). This number is higher than actual inventory because staff must wait for Axon to accept returns of old BWCs and update the inventory status. 240 Body 4s should be relinquished by Axon soon, resulting in a final count of 204 assigned and 55 in stock once the inventory is updated. The two Axon Body 3s listed in the inventory were

outliers that should have been removed previously as they are not in stock and were not a part of the most recent refresh.

Table Four: Count of In Stock and Assigned BWCs July 2026

Device Type	Count In Stock	Count Assigned	Total
Axon Body 3	2	0	2
Axon Body 4	295	204	499
Total	**297**	**204**	**501**

The area is significantly understaffed. Only two employees are responsible for setting up devices and maintaining inventory, in addition to their many other responsibilities including managing release requests and providing training to new officers. Establishing an internal system with additional inventory controls would be time-consuming and was likely not prioritized given the importance and time sensitivity of other tasks, such as responding to data requests. In the past, the department assigned three staff members to this function, but after one staff member left, management reassigned the full-time employee (FTE) to the records unit.

Maintaining an accurate inventory of IT assets is critical. The Center for Internet Security (CIS) 1.1 instructs organizations to inventory their assets.[20] Relying on inventory maintained by the vendor carries inherent risk, as the vendor has a financial interest related to inventory. For example, MTPD staff would not be able to independently validate vendor information and may purchase extra devices or be overcharged for devices that no longer exist. It can take many weeks for Axon to update statuses of returned devices. As a result, inventory records may not accurately reflect the agency's current BWC inventory. The department may base procurement decisions for additional BWCs and software licenses on inaccurate inventory information. This could have an operational impact causing either unnecessary expenditure or insufficient equipment.

Recommendation:

1. The MTPD should maintain an inventory of hardware outside of Evidence.com using an appropriate asset management system and perform and document inventories at regular intervals at least annually to ensure accurate and complete inventory.

   Management Response: Agree. Currently MTPD contracts with Axon to support inventory management as a part of the entire service agreement package. MTPDs experience and analysis of Axon's inventory management indicate it is a reliable system with built in audit trail capability to track assignment and location including GPS. To assist with risk reduction for the BWC program, MTPD is taking part in Axon's Technology Assurance Program (TAP). The

[20] CIS 1.1 instructs organizations to "Establish and maintain an accurate, detailed, and up-to-date inventory of all enterprise assets with the potential to store or process data, to include: end-user devices (including portable and mobile), network devices, non-computing/IoT devices, and servers. Ensure the inventory records the network address (if static), hardware address, machine name, enterprise asset owner, department for each asset, and whether the asset has been approved to connect to the network. For mobile end-user devices, MDM type tools can support this process, where appropriate. This inventory includes assets connected to the infrastructure physically, virtually, remotely, and those within cloud environments. Additionally, it includes assets that are regularly connected to the enterprise's network infrastructure, even if they are not under control of the enterprise. Review and update the inventory of all enterprise assets bi-annually, or more frequently".

intention of this program is to ensure an officer will never be in a position to go on duty without an operational body camera. This is a part of our multi-year contract and provides spare cameras for immediate replacement, as well as no additional cost replacement in case of loss or damage to equipment. In addition to Axon, MTPD practices individual issues rather than shared use of this technology to have strict inventory control.

To eliminate third-party vendor dependency, MTPD will create inventory redundancy on an annual basis by exporting the Axon inventory metadata and saving it on a secure shared MTPD drive. Additional review of inventory will occur before and after future hardware refreshes.

Timetable: Completed September 2026.

Staff Responsible: BWC/Video Supervisor.

Audit Follow-Up: Confirmation.

Section Two: Footage Review

Methodology:

Auditors reviewed footage from August 1, 2025, through March 30, 2026. The review included only sworn officer footage with an Archived, Active, or Pending Deletion status. Auditors excluded CSO and civilian footage. Auditors only tested BWC videos and only viewed squad cars or other footage types if needed to establish context for a sample BWC video. Auditors used three sampling approaches, with each approach designed to meet a specific testing objective.

The first method used stratified random sampling to select videos from specific categories, including high-risk "Use of Force" and "Homicide/Criminal Sexual Conduct (CSC)/Arson/Death," and from lower-risk categories such as "Call for Service/Citizen Contact". Auditors sampled 522 videos (**Table Five**).[21] Auditors had to resample one video due to a conflict of interest[22] and removed two videos from the sample that were deleted per retention schedule. In total, auditors reviewed 520 videos, approximately 145 hours of footage accounting for approximately 1.1% of all footage recorded during the period. High-risk videos accounted for 27% of videos reviewed.

For each video reviewed, auditors assessed: activation, deactivation, muting, functionality (adequate audio and video), privacy compliance, and categorization. Audit did not specifically review for misconduct. When auditors identified potential policy violations or unprofessional conduct, they consulted with the Audit Manager and escalated the observations as appropriate. The Audit Manager, Chief Audit Executive, Chief of Police, Internal Affairs, and Office of the General Counsel were notified of the escalations. Of the 520 videos reviewed, auditors referred seven for further review.

---

[21] Auditors selected sample size considering the population size of each stratum, a 5% sampling error, a 95% confidence level and a 50% expected error rate.
[22] If an auditor saw someone they knew in a video, they could not review that video. One person appeared as a bystander in a randomly selected video that all of the auditors knew.

Table Five: Sample Selection (Main Footage Review Testing)

Video Type One - High Risk (Use of Force & Homicide/CSC/Arson/Death				
Set n		**Statistically Significant Sample**	**Sampled Seconds**	**% of total videos**
224		141	260,609	63%
Video Type Two - All Other Categories				
Set n		**Statistically Significant Sample**	**Sampled Seconds**	**% of total videos**
46,767		381	261,311	0.81%
Totals	**46,991**	**522**	**521,920**	**1.11%**

The second sample focused on compliance with pre-shift function tests (PFTs). Auditors requested a list of officer shifts for one week within the shortest retention period (90 days) and selected a stratified sample of 61 officer shifts to cover all work assignments. For each sampled officer shift, auditors searched in Evidence.com for videos recorded by that officer during the shift, and looked at the shortest video, the first video, or any marked as "Test/Accidental/Non-Evidentiary." Then, auditors viewed the videos to determine if it was a PFT and if so, if it contained the required elements.

The third sample assessed compliance with Policy 472.5 (BWC Activation), by reviewing CAD calls to confirm whether footage existed and was properly recorded. Auditors randomly selected one week of CAD calls, March 30 through April 4, 2026, to assess whether officers activated their BWCs as required by Policy 472 when performing law-enforcement-related activities. Due to the PDF data format, auditors used interval sampling. 159 CAD calls (approximately 5% of all calls that week) were reviewed, 63 of which had direct citizen contact. Auditors excluded calls classified as "cancelled", "information only," "gone on arrival," "directed patrol," or "onboard."

Observation 9: Approximately 10% of BWC videos reviewed showed late activation, and approximately 10% showed premature deactivation.

Officers activated BWCs late in approximately 10% (50/499) of videos reviewed.[23] Timely activation means that BWCs were activated prior to arrival for calls for service and as soon as practicable.[24] Officers deactivated approximately 10% (51/499) of videos prematurely.[25] Premature means that recording ended before the conclusion of the call for service or law enforcement activity, meaning the officer was still interacting with or in the proximity of citizens related to the initial call.[26] Auditors took

[23] 21 videos reviewed were not applicable due to being pre-shift function tests or non-enforcement.
[24] Specifically, MTPD policy 472 states: "Members should activate their BWC during all calls for service and the performance of law enforcement-related functions. Members are not required to activate their BWC during casual or informal contacts with members of the public that are not part of or related to law enforcement functions. However, members should activate their BWC any time a contact with an individual becomes hostile or adversarial."
[25] 21 videos reviewed were not applicable due to pre-shift function tests or non-enforcement.
[26] Specifically, MTPD policy 472 states: "Unless otherwise authorized by this policy or approved by a supervisor, BWCs should remain activated until the call for service or law enforcement-related function has concluded. A member may cease recording if they are simply waiting for a tow truck or a family member to arrive, or in other similar situations. At no time is a member expected to jeopardize their safety to activate their BWC. However, the BWC should be activated as soon as reasonably practicable in required situations."

into consideration privacy concerns outlined in the policy, for example, if officers entered a medical facility and deactivated their BWCs, this was not considered to be a premature deactivation. Ten videos both started late and ended early, resulting in a total exception rate of 18% (**Table Six**).

Table Six: Late Activation and Early Deactivation Rates for Footage Review Sample

	Ended on Time	Ended Prematurely	Total
Activated on Time	408	41	**449**
Activated Late	40	10	**50**
Total	**448**	**51**	**499**

Late activation results in gaps at the beginning of an encounter. Although the system captures the 30 seconds preceding activation, that portion lacks audio. These gaps can omit critical context leading up to an incident. Premature deactivation similarly creates gaps at the conclusion of an encounter. Together, these gaps compromise the completeness and reliability of the video. These gaps can weaken the video's evidentiary value and undermine transparency and accountability, creating operational and reputational risks.

A lack of refresher training (*Observation 4*) combined with recent changes in policy could have contributed to late activation and premature deactivation. Where the earlier policy provided a detailed list of specific triggers for activation (e.g., traffic stops, crowd control, crime scene perimeters), the later policy is broader and contains more general language that could be interpreted differently by different officers. The new policy also introduces new and loosely defined exceptions for deactivation.

Supervisory review is the primary control for identifying activation and deactivation exceptions; however, it has significant room for improvement. The process for escalating activation and deactivation issues is undocumented and key terms such as “Activated Correctly” “Ended Correctly” and “Late Activation,” are undefined. These challenges have led to inconsistent review. Currently metadata is not analyzed by the MTPD. This is discussed in further detail in *Observation 5*. Increasing the use of supervisory review data could lead to more targeted training opportunities.

Recommendation:

1. The MTPD should implement regular monitoring of supervisory reviews of BWC footage to identify and address recurring activation and deactivation timing issues.

   Management Response: Agree: All personnel will receive at least 2 forms of BWC training. (Ref: Mgt. response- Observation 4)
   MTPD will produce Standard Operating Procedures (SOPs) that will establish clear expectations for supervisory reviews that will include BWC activation and deactivation, BWC categorization, BWC Pre-Shift Function Testing, documentation, follow-up, escalation, and corrective action for violations. (Ref: Mgt. response- Observation 5)
   Escalation and corrective action can include the Internal Affairs (IA) unit who will determine the appropriate corrective action based on the nature and frequency of the violation. The IA Unit will forward findings and recommend corrective action to the Chief.
   Supervisors will receive training and instruction regarding the review, documentation, notification, and corrective-action process.

   Timetable: The process will be implemented by end of Q3, 2027.

Staff Responsible: Patrol Captain.

Audit Follow-Up: Confirmation.

Observation 10: Approximately 16% of BWC videos reviewed were miscategorized, and 11% were missing associated case or incident ID.

MTPD policy requires that officers categorize footage appropriately. Policy 472.6.1 states, "Members should tag all media captured by their BWC with their name and/or identification number, the case or incident number, and the event type." Evidence.com provides fixed category options, but the system and supplementary guidance do not define the categories or explain how officers should apply them. Supervisors perform random reviews, but without work instructions or category definitions, the interpretation of the "ID and Category Listed" and "Missing Id/Category" and "Correctly Classified" fields varied between the five supervisors interviewed. Furthermore, the department does not aggregate supervisory review data and therefore cannot identify trends in mis-categorization.

Of the 520 videos auditors reviewed, 82 (16%) were miscategorized. Of the 82 miscategorized videos, "Arrest/Cite/Investigation/Evidence" was missing the most often with 44 total instances of missing tags (≈54%). Another 30% of missing categories involved events that officers did not categorize as "Call for Service/Citizen Contact." Auditors identified two miscategorized videos in the "Homicide/CSC/Arson/-Death" category, one being an overdose (death) and the other being Criminal Sexual Conduct (CSC). Auditors also identified four instances of use of force without the tag "Use of Force" (**Table Seven**).

Table Seven: Count of Missing Categories by Type

Missing Category	Count
Arrest/Cite/Investigation/Evidence	44
Call for Service/Citizen Contact	25
Homicide/CSC/Arson/Death	2
Test/Accidental/Non-Evidentiary	3
Traffic/Accident Investigation	4
Use of Force	4
Total	**82**

In addition, auditors observed 56 of 502 (≈11%) videos that did not have an associated case or incident ID.[27] Auditors flagged a discrepancy whenever an arrest or citation occurred, or footage was tagged as evidentiary,[28] without a corresponding case number attached to the video.

Evidence.com communicates with the CAD system to allow auto tagging. The combination of automated case number assignment and manual entry can create a gap in responsibility. Officers

[27] Total videos are equal to 502 rather than 520 due to the removal of non-applicable pre-shift function tests.
[28] Auditors considered all tags other than "Test/Accidental/Non-Evidentiary" and "Call for Service/Citizen Contact" to have some form of evidentiary value.

may feel a false sense of security when Evidence.com frequently successfully communicates with CAD to assign a case number. However, this system can assign the improper number or fail to sync, and then case number association relies on the manual entry by the officer or reviewers. This creates the potential for human error. In addition, there was a breakdown of controls during staffing transitions. In the past, the former Manager of Police Business Systems sent out a list every two weeks reminding officers to add ID and category to their videos. During the audit, the review for misclassified videos and reminders to officers were not occurring consistently.

All footage needs to be appropriately categorized to ensure that it is retained in accordance with MTPD Policy. Each category has an associated retention schedule. If a video is improperly categorized, it could be prematurely deleted or kept beyond the required retention schedule. All arrests, citations, or evidence must be linked to a valid case number to ensure proper documentation and traceability. Without an associated case number, evidentiary footage cannot be reliably linked to the corresponding incident, arrest, or citation. This could lead to footage not being found for discovery or data requests. This creates an operational risk because incomplete evidence could weaken cases or contribute to case dismissals. It also poses a reputational risk if a request for footage is incomplete due to missing case numbers.

Recommendations:

1. The MTPD should create clear definitions of categories for officers to refer to and should clearly define how officers are supposed to use the auto tagging feature in Evidence.com. These definitions should be incorporated into onboarding and periodic refresher training.

2. The MTPD should implement a control to ensure all footage tagged as evidentiary is associated with a valid case number.

   Management Response: Agree. Categorization requirements and standardized definitions developed by MTPD will be added to the BWC policy in Lexipol. These definitions will be incorporated into BWC training curriculum (Ref: Mgt. response-Observation 5) and provide instruction on associating cases with applicable case numbers, the appropriate use of the auto-tagging feature, and include practical calibration exercises using representative examples to promote consistency in categorization.

   Supervisors will be required to access Evidence.com daily to verify that direct reports have appropriately categorized their BWC activations. Patrol Lieutenants/Watch Commanders will conduct weekly audits to monitor compliance.

   All personnel will receive at least 2 forms of BWC training. One- Training will be administered as part of annual in-service training for sworn officers and CSOs. Two- Via Learning and Development portal (Ref: Mgt. response-Observation 5).

   Timetable: The department has already begun addressing this recommendation through roll-call training, supervisor direction, and onboarding. In- Service training completion by end of Q3 year, 2027.

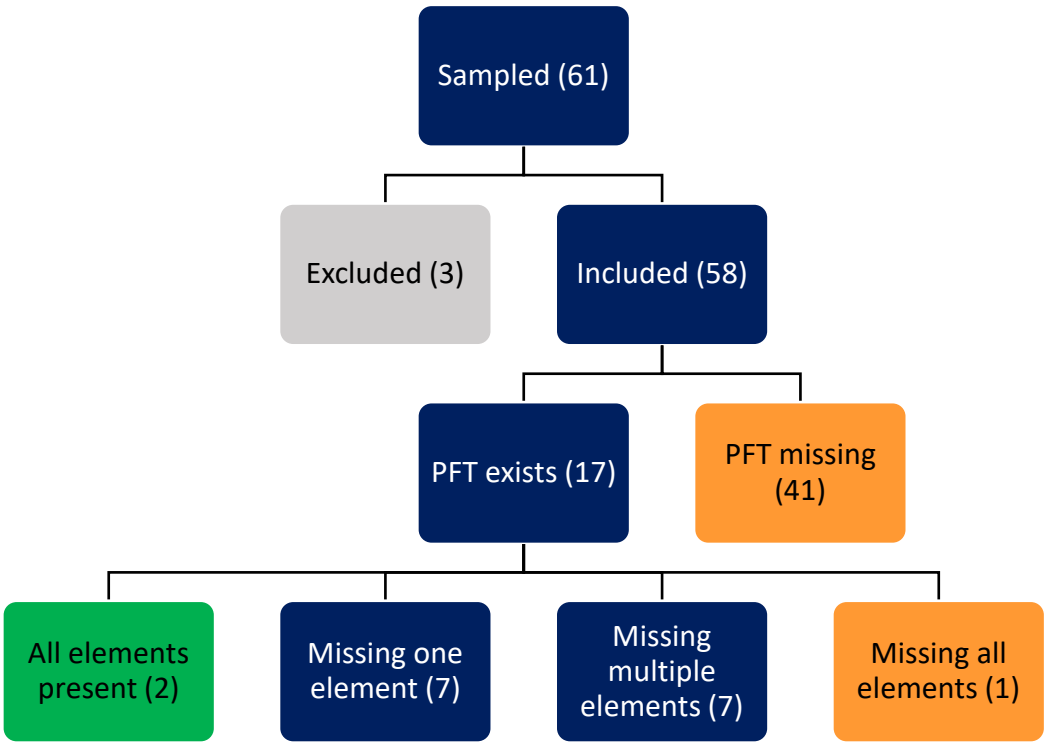
   Staff Responsible: Training Unit Supervisor, Patrol Captains, Accreditation and Policy Analyst with the support of the BWC Manager.

   Audit Follow-Up: Confirmation.

Observation 11: Pre-shift function tests were performed 29% of the time (17/58) and are not reviewed.

MTPD's BWC policy requires officers to perform Pre-shift Function Tests (PFTs) to ensure the BWC is operational. Auditors sampled 61 officers' shifts, then reviewed footage for existence and alignment with policy. Auditors excluded three shifts because they involved desk duty only or had no assigned staff (such as if an officer called out sick). Of the 58 remaining shifts, auditors could only identify 17 (29%) PFTs. Only two of these fully met MTPD policy (**Figure Three**). PFT completion rates were low and consistent across shifts and commands, suggesting a department-wide issue rather than one tied to specific officers or supervisors.[29]

Figure Three: PFT Testing Results



Most officers who performed a PFT correctly stated their name (16 of 17, 94%) and badge number (14 of 17, 82%), about half stated their assignment (9 of 17, 53%), and a few stated the date and time (3 of 17, 18%). The information and quality of PFT's varied. Only two PFTs met all requirements (**Table Eight**).

[29] No shift had more than 50% of PFTs present, other than Sergeants and Lieutenants where four out of seven (57%) completed a PFT. The portion of missing PFTs for East Command (14 of 21, 67%) and West Command (20 of 28, 71%) were comparable.

Table Eight: PFT Testing Results

Required Elements[30]	Met	Not Met	N/A[31]	% Met (of PFTs)	% Met (of Shifts)
PFT Exists	17	41	3		29%
State Name	16	1	41	94%	27%
State Badge Number	14	3	41	83%	24%
State Assignment	9	8	41	53%	16%
State Date and Time	3	14	41	18%	5%
Met All Criteria	**2**	**56**	**3**	**12%**	**3%**

According to Minnesota Statutes, section 626.8473, subdivision 3, all agencies with BWCs must also have "procedures for testing the portable recording system to ensure adequate functioning" and "procedures to address a system malfunction or failure, including requirements for documentation by the officer using the system at the time of a malfunction or failure." MTPD Policy 472 states "at the beginning of each shift or period of BWC use, the member should inspect their assigned BWC to confirm it is charged and in good working order. As part of the inspection, the member should perform a function test by activating the BWC and recording a brief video stating their name, identification number, assignment, and the date and time."

If a malfunction is not caught early by the officers, it may result in missing or otherwise unusable footage. Depending on the nature of the malfunction, this could also include inaccurate location tags or timestamps which could obscure the documented timeline of events. Although there are usually multiple BWCs recording during high-risk events like arrests, each angle provides new perspectives and may capture information that others do not. Emergency situations may also occur with only one or two officers present, with backup arriving later. Additionally, if a BWC malfunction is only identified later and is not properly reported, it may not be fixed in a timely manner and could affect videos for multiple shifts or incidents.

PFTs are shorter than other types of BWC footage. The randomly selected videos for supervisory review (*Observation 5*) exclude videos shorter than one minute or longer than six minutes, and supervisors stated they have never seen a PFT in their sample of 40 random videos per month. The length of videos selected for random review impacts the kinds of videos included, even though no categories are directly excluded from review. This duration under-represents arrests and evidence by about 28%, uses of force by about 73%, and slightly under-represents test and non-evidentiary videos by about 8% (28.0% of 1-6-minute-long videos vs 30.4% of all videos) (**Table Nine**). Pre-shift function tests are often shorter than one minute and are therefore excluded from random supervisory reviews. There is no separate process to review PFTs specifically.

Table Nine: Proportion of Videos Tagged as Each Category by Video Duration

Category	≤ 1 Minute	1-6 Minutes	>6 Minutes	All Videos
Arrest/Cite/Investigation/Evidence	8.9%	18.9%	42.5%	26.3%
Use of Force	0.1%	0.1%	0.9%	0.4%
Test/Accidental/Non-Evidentiary	77.3%	28.0%	7.8%	30.4%

[30] The total for "PFT Exists" is 58 sampled shifts, while the rest of the rows are based on the 17 PFTs.
[31] For "PFT Exists," N/A means the shift was either desk duty only or not staffed, which means there is no expectation for a PFT. For the other rows, N/A counts the number of missing PFTs.

As a result, supervisors do not assess PFT completion or quality. Without this monitoring, supervisors lack the data needed to hold staff accountable for complying with policy. In addition to the random video review by supervisors, there is no other regular random review of footage that would capture this topic. Further, there is no report or other tool that aggregates the results of supervisory review to identify trends or recurring issues, though supervisors expressed interest in this (*Observation 5*). Officers do not receive any refresher training (*Observation 4*) and may miss out on a reminder that this is a requirement. Finally, although PFTs are required by policy, if they are not regularly monitored, and enforced then it makes it harder to hold officers accountable. When policies are rarely or only selectively enforced, they lose their strength as a control.

Recommendation:

1. The MTPD should establish a process to monitor PFT completion and compliance, in accordance with policy.

   Management Response: Agree. Effective immediately shift supervisors will communicate expectations to personnel regarding the requirement to complete a Pre-Shift Function Test (PFT). All personnel will complete the PFT at the conclusion of roll call and before leaving the police department for their patrol assignment.

   Signage will be posted at the exit of each command to remind personnel to complete the required PFT. Signage will prominently display:

   "BWC FUNCTION TEST?"

   The signage will provide instruction on the information personnel are required to document:
   - Name
   - ID Number
   - Assignment
   - Date/ Time

   Timetable: The department has already begun addressing this recommendation through roll-call training, supervisor direction, and onboarding. MTPD expects compliance improvement by end of Q2, year 2027.

   Staff Responsible: Shift Supervisors and Patrol Lieutenants/Watch Commanders.

   Audit Follow-Up: Confirmation.

Observation 12: In approximately 28% (18/63) of CAD calls reviewed with citizen contact, officers did not activate their BWC.

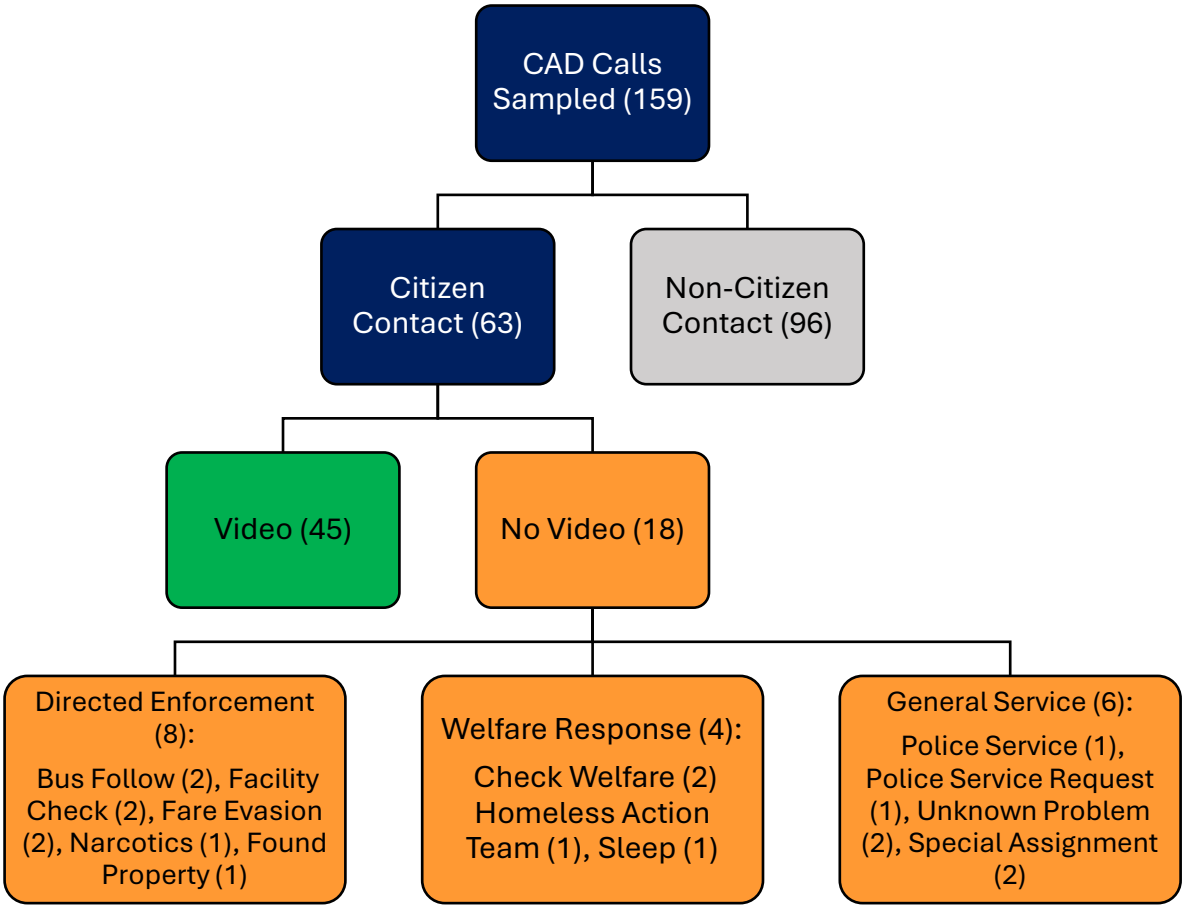
The sample included 159 CAD calls. Auditors identified 63 calls involving citizen contact after excluding calls classified as cancelled, information only, gone on arrival, directed patrol, or onboard. These calls were excluded because citizen contact may not have occurred. Of the 63 citizen-contact calls, 18 had no BWC footage associated with the primary officer. Twelve calls resulted in an assist, five resulted in advising and sending, and one was cleared up by a report. The calls included fare evasion, welfare checks, sleep-related calls, and facility checks. Two calls classified as "unknown problem" also lacked BWC footage (**Figure Four**).

Policy 472.5 requires officers to activate their BWCs during all calls for service and law-enforcement-related functions. Officers must also activate their BWCs when informal contact becomes hostile. “Enforcement Activities” are not clearly defined in policy, which may contribute to misunderstanding of expectations for recording calls, especially if related to non-criminal conduct such as welfare checks. Unclear activation requirements may also lead to inadvertent or intentional policy violations, increasing compliance and reputational risks for the MTPD and the Met Council. If officers do not activate their BWCs during citizen contacts as required, the MTPD may fail to capture and preserve evidence needed for investigations.

The current Policy 472 provides less specific guidance than the former Policy 451, which identified circumstances such as vehicle and person stops, arrests, confrontational police-citizen contacts, and transports. The lack of specific examples may create uncertainty about when officers must activate their BWCs and increase the risk of inconsistent compliance.

Other than initial training during the new officer academy, officers are not given periodic refresher training (*Observation 4*) if they are operating a BWC. Instead, officers are meant to acknowledge the policy when there are changes made, which were tracked by MTPD’s policy software, Lexipol. Supervisors were expected to review officer’s footage, however there were no work instructions on how to complete these reviews (*Observation 5*). In addition, the training manager also needs to review footage, but after a conversation with the Lieutenant of the training unit, these reviews were not conducted (*Observation 6*).

Figure Four: CAD Calls Reviewed



Recommendation:

1. The MTPD should strengthen monitoring of activation compliance by implementing periodic reviews of CAD calls to ensure footage exists for all enforcement activities.

   Management Response: Agree. The department will take the following actions: Require each supervisor to conduct at least one random CAD-call/BWC review for each direct report during each shift rotation. Adjust the supervisory review process to reduce the number of general random video reviews while increasing targeted reviews of BWC footage associated with direct reports. This instruction will be implemented in the MTPD SOPs that will establish clear expectations for supervisory reviews that will include BWC activation and deactivation.

   All personnel will receive at least 2 forms of BWC training. One- Training will be administered as part of annual in-service training for sworn officers and CSOs. Two- Via Learning and Development portal.

   Supervisors will receive training and instruction regarding the review, documentation, notification, and corrective-action process. (Ref: Mgt. response-Observation 5)

   Timetable: In- Service training completion by end of Q3 year, 2027.

   Staff Responsible: Patrol Captains, BWC/Video Manager.

   Audit Follow-Up: Confirmation.

Section Three: Redaction and Release

Methodology:

Auditors observed MTPD Principal Administrative Specialists to understand the redaction and release workflow. BWC data is available to verified data subjects and access may be requested by submission of a MTPD BWC Video Request Form either online or in person. Data sharing is documented in a Sharing Audit Report and in an Excel tracking spreadsheet.

Auditors randomly selected five requests from each of the four categories included in the tracking spreadsheet: Assist Other Agencies (AOA), Discovery, and Public Data Request entries, and sampled all five redacted requests released in 2025 and 2026. For each sampled request, auditors pulled corresponding audit trails from Evidence.com. For AOA and discovery, Auditors confirmed that agencies were on the approved list in Evidence.com. Auditors requested documentation of all requests to confirm retention and to verify responses to requests were timely. However, because responses from outside of Evidence.com were not retained, neither the review of supporting documentation nor confirmation of the 10-day release timeline could be tested.

When a release occurred, auditors viewed released and redacted footage to confirm appropriate redaction of non-consenting individuals, and to verify that on-duty officers were not improperly redacted. Auditors only reviewed BWC footage and excluded squad-car footage. Auditors used a combination of file titles and audit log details to identify videos that had been redacted. Auditors calculated days to completion for public data requests. Auditors obtained a Critical Incident Log to identify use-of-force cases with distinct release requirements, confirming that neither identified critical incident case had an associated public release request during the sample period.

Observation 13: Auditors could not verify compliance with MGDPA timely release requirements due to a manually maintained BWC release tracker that is incomplete and inaccurate.

The MTPD uses a manual spreadsheet to track data requests for BWC footage. Staff manually track data requests and do not track a critical component: the date of response. This date is a key benchmark to comply with statutory promptness requirements. Ten public requests were made in 2025 and 33 in 2026. Only one of the five public requests reviewed had documented evidence of a response. Staff responded to this public request 20 days later than the ten business day requirement, with the response received on February 12th but replied to on March 26th. In 2026, public requests took on average 44.5 days to complete, compared with 35.3 days in 2025 (**Table Ten**).[32]

Table Ten: Average Number of Days to Complete Public Requests

Year	Average Number of Days from Receipt to Completion
2026	44.5
2025	35.3

In addition, auditors observed significant discrepancies between the source documentation from Evidence.com and the release tracker, such as:

- An internal request was marked as completed with two videos released to requestor. However, the audit trails for the seven related BWC videos show that the MTPD did not release the footage and only MTPD personnel viewed it, not the requestor.
- A public release request marked five BWC videos redacted but only four existed, and none of the four videos were redacted or released in Evidence.com.
- A public request had no identifying information such as case number.
- Another public request had no staff member assigned to fulfill it. The request remained marked as “in progress.” However, staff released two of the seven videos after redaction. No videos were marked as released in the tracker, rather the video number contained an "x."

Minnesota Statute, section 13.04 subdivision 3 “access to data by individual” states that “The responsible authority or designee shall comply immediately, if possible, with any request made pursuant to this subdivision, or within ten days of the date of the request, excluding Saturdays, Sundays and legal holidays, if immediate compliance is not possible.” Met Council Policy RF 8-1 and Procedure RF 8-1a incorporate this requirement.

Poor tracking and delayed responses are due to poor systems integration as well as understaffing. The group tasked with footage release is composed of only two staff members, relying on two interns to complete daily work. The MTPD does not use the DPO portal, which automatically tracks items such as request and response date. Historically, there has been limited collaboration between the Met Council’s DPO and the MTPD. DPO, housed within the Met Council’s OGC, occasionally plays an advisory role for the BWC program. The office serves as the Met Council’s central authority on data

[32] This is likely a low estimate as auditors excluded requests that remained pending, were on hold, or lacked a documented completion date (7 of 10) in 2025 and (16 of 33) in 2026.

governance and public data requests. The office receives and manages all non-MTPD data requests, classification, retention, and release. Prior conversations between DPO and the MTPD decided the processes should be handled separately.

Tracking BWC data requests manually adds an administrative burden and causes a lack of key metadata, making it difficult to track requests efficiently. This manual approach requires additional staff time to maintain and, because it captures less metadata, makes oversight difficult. It may also create legal exposure if a request cannot be reliably linked through its original description and related correspondence. A lack of traceability could create complications for a contestation process under Minnesota Statutes, section 13.04, subdivision 4, and could raise issues under section 13.03, subdivision 3f if a request is denied. Under the MGDPA such deficiencies can expose the Met Council to a civil penalty of up to $1,000 per violation under section 13.08, subdivision 4.

Recommendation:

1. The MTPD should work with DPO to make use of the existing data request portal to improve tracking.

   Management Response: Agree. MTPD will work with IS Business Partner to prioritize IS support to create a public facing portal to support this workflow. MTPD has had initial discussions with IS Business Partner and determined it would be ideal for IS to create a similar portal as the one that was recently created for DPO.

   Timetable: The IS ticket will be submitted immediately with a goal of having the portal operational end of Q3, year 2027.

   Staff Responsible: BWC/Video Supervisor with the support of IS staff.

   Audit Follow-Up: Confirmation.

Observation 14: MTPD public data request records are incomplete and only retained for six months, which does not align with the Council's records retention schedule.

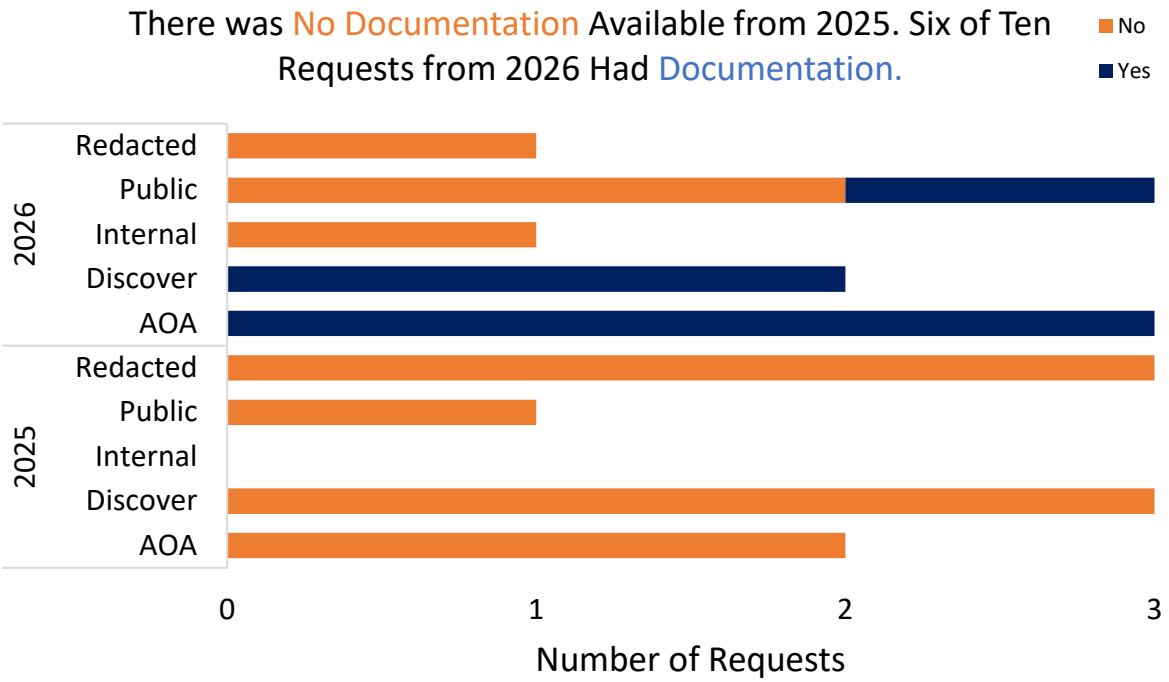
The MTPD currently cannot produce a complete request-to-response audit trail for requests made over six months ago. Staff in MTPD Police Business Systems unit kept initial requests and subsequent responses for BWC footage via email with an automated retention period of only six months. This is significantly less time than the six years required for public data requests, responses, data provided, and originals under the Met Council's Approved Functional Retention Schedule. No documentation from sampled 2025 release requests was available for any category: Discovery, AOA, Internal, Public, and Public Requests with Redaction. In 2026, Discovery and AOA documentation was available 100% of the time, though testing took place mostly in the beginning of the year. Of the three public and one redacted public request in 2026, only one had documentation available (**Figure Five**).

The audit team received a walk-through on how redactions and releases were completed. The department had two Principal Administrative Specialists who performed redaction, release, discovery, internal requests, and AOA. While one staff member was responsible for internal and discovery

requests, both would complete AOA requests from other agencies. There were three separate email inboxes maintained. The Principal Administrative Specialists in charge of AOA and discovery requests kept records in an Outlook folder. Folders in Outlook typically have longer rolling archive schedules than inboxes. The employee who managed public data requests was able to provide more limited supporting documentation due to the use of the Met Council's standard inbox and default six-month email retention schedule. Emails were not saved outside of the inbox, and paper copies were not maintained.

The Met Council's retention schedule was made to align with Chapter 13 of the MGDPA. While Chapter 13 does not set a statutory retention period for the requests or copies of records, section 13.03 subdivision 2.(a) requires agencies to "establish procedures to ensure that requests for government data are received and complied with in an appropriate and prompt manner."

Figure Five: 2025-2026 Summary of Request Documentation Maintained



The limited record maintenance practices reflect limited supervision over staff's handling of requests. Not only does this limit the assurance that Audit can provide, but it also leaves management without a mechanism to ensure that requests are handled consistently, promptly, and in line with policy. This could directly damage public trust. The absence of a clearly defined final storage location for archived records increases the risk that staff could inadvertently delete records before the required retention period expires. Moreover, failing to maintain documentation of public records requests exposes the Met Council to compliance and legal risk. It increases litigation exposure because, without documentation of what was requested and why a denial was issued, the organization has no basis to defend its decisions if challenged.

Recommendations:

1. The MTPD should create an archive to store requests and related documents and communication for six years to align with Council Policy.

2. The MTPD should implement periodic supervisory reviews of release requests to ensure documentation is maintained.

   Management Response: Agree. MTPD's development of a portal to support Video and BWC data requests will include a mechanism to store requests and related documents and communication for 6 years to align with council policy. In the interim, MTPD has requested IS to change the retention period for the shared mailboxes (MTPDevidence and MTPDbwcVideo).

   Timetable: IS ticket completed. Goal of having the video and BWC portal operational is end of Q3, year 2027.

   Staff Responsible: BWC/Video Supervisor with the support of IS staff.

   Audit Follow-Up: Confirmation.

Observation 15: One instance of identifying information was unredacted from released BWC footage.

The MTPD released two requests with redactions in 2026 and three in 2025. Audit reviewed all five redacted releases. While faces were redacted to protect identities of non-consenting subjects, one video contained an operator's badge number. The MTPD released this video to another data subject.

Chapter 13 of the MGDPA provides information on redaction and release of data. Under section 13.825 subdivision 2. (2) (i) "data on a subject who is not a peace officer and who does not consent to the release must be redacted." "Data on individuals" is defined under 13.02 Subdivision 5. as "all government data in which any individual is or can be identified as the subject of that data, unless the appearance of the name or other identifying data can be clearly demonstrated to be only incidental to the data and the data are not accessed by the name or other identifying data of any individual." According to MTPD Policy 810.5, "Examples of release restrictions include: (a) Personal identifying information."

The MTPD did not have a formal SOP or job aid outlining the process and requirements for releasing BWC footage. There was also no secondary review before footage was released. MTPD staff reported that the primary focus of redaction is on faces, license plates, and sometimes audio. DPO, however, described a broader definition of personally identifying information that includes publicly facing employee IDs. While there are some tools to help automatically select and track faces for the purpose of redaction, the process also relies on manual redaction of other identifying information.

Failure to appropriately define what must be redacted and to redact identifying information from non-consenting individuals poses compliance risks with the possibility of fines and penalties. Operator safety could be compromised, and the organization faces reputational risk if it cannot appropriately protect the identities of the non-consenting public.

Recommendations:

1. The MTPD should work with DPO to establish an SOP that defines what must be redacted.

2. The MTPD should implement a secondary review of BWC footage before release to ensure all required information has been properly redacted.

   Management Response: Agree. MTPD is currently working with DPO to establish a full-time partnership. With their assistance we will establish an SOP that defines what must be redacted in reference to Chapter 13 of the MGDPA. MTPD will also include the requirement of a secondary review prior to release.

   Timetable: End of Q4, year 2027.

   Staff Responsible: BWC/Video Supervisor with the support of DPO staff.

   Audit Follow-Up: Confirmation.

Conclusions

The department meets minimum statutory policy requirements and has implemented a system of controls to ensure data access is approved and documented. The MTPD BWC program also aligns with best practices, meeting all required elements of the BJA scorecard. However, improvements in documentation, oversight, and consistent policy enforcement would help the MTPD more reliably achieve the program's evidentiary and accountability objectives.

This audit identified gaps between MTPD's BWC program as designed and as practiced, spanning governance, technical controls, and day-to-day compliance. Improvements to administrative and governance controls will help address the officer compliance issues identified in this audit including delays in activation, late deactivation, and incorrect categorization.

Many procedures require documentation and improved oversight is necessary. Supervisory review criteria were not clearly defined, and where reviews were conducted, the compiled results do not match underlying system metadata, nor were these results being aggregated to detect patterns of policy non-compliance. Refresher training was not being provided periodically as required by policy, which has likely contributed to the observed deficiencies.

Administrative controls also require strengthening. Delays in access deprovisioning upon employee termination must be improved, and inventory management controls need to be implemented so that the MTPD can independently verify equipment. Incomplete maintenance of redaction and release data makes it more difficult for the MTPD to demonstrate compliance with applicable data practices requirements. Improvements to request tracking and updates would strengthen transparency. The MTPD could address some of these challenges by better leveraging existing Council resources and reducing administrative burdens on employees, such as working with DPO to improve data request tracking and aligning MTPD and Met Council policies to clarify responsibilities before the next biennial audit.

Collectively, these findings were rooted in insufficient documentation, unclear ownership of review functions, and inconsistent supervision and enforcement. Addressing these gaps will help the MTPD strengthen program oversight and reduce risks related to evidentiary concerns, privacy, public records compliance, and public confidence in the program.

October 13, 2026
Sandra Ludwig
Chief Audit Executive

Appendix A: Follow-Up Categories

Program Evaluation and Audit recommendations are categorized according to how Audit will follow-up on them. The categories are:

- **Retest —** Audit will retest the area using the same or similar procedures after a recommendation has been implemented and sufficient time has passed for the changes to take effect. The retest will take place on a specified timetable. The recommendation will be closed once the change has occurred. A new audit project will be opened for retesting, and any new findings will include new recommendations
- **Confirmation —** Audit will confirm that an adequate risk response has been completed on the agreed upon timeline. The recommendation will be closed once the change has taken place.
- **Assess Risk —** Audit will not plan for specific follow up to these recommendations. Audit will discuss the area as part of its annual risk assessment activities and consider future audit work in the area.

Appendix B: Acronyms

AOA: Assist Other Agency

BCA: Bureau of Criminal Apprehension

BJA: Bureau of Justice Assistance

BWC: Body-Worn Camera

CAD: Computer-Aided Dispatch

CIS: Center for Internet Security

CSC: Criminal Sexual Conduct

CSO: Community Service Officer

CJIS: Criminal Justice Information Services Security Policy

IA: Internal Affairs

IIA: Institute of Internal Auditors

IS: Information Services

LASO: Local Agency Security Officer

MGDPA: Minnesota Government Data Practices Act

MT: Metro Transit

MTPD: Metro Transit Police Department

OGC: Office of General Counsel

PFT: Pre-shift Function Test

TRIP: Transit Rider Investment Program

SOP: Standard Operating Procedure

SSO: Single-Sign-On

Appendix C: Distribution List

All audit reports are reported to the general public and are available on *www.metrocouncil.org*. This audit report was distributed to the following parties:

External:

- Chairs and ranking minority members of the committees of the Minnesota House of Representatives and the Minnesota Senate with jurisdiction over data practices and public safety issues
- Legislative Commission on Data Practices and Personal Data Privacy

Internal:

- Council Members
- Audit Committee Members
- Chair of the Metropolitan Council
- Regional Administrator, RA
- Deputy Regional Administrator, RA
- General Counsel, RA
- Deputy General Counsel, RA
- Chief of Staff, RA
- Director, Governmental Affairs, RA
- Director, Communications, RA
- Chief Financial Officer, RA
- Chief Procurement Officer, RA
- Chief Information Officer, RA
- Local Agency Security Officer, RA
- Head of Data Practices, RA
- General Manager, MT
- Assistant General Manager, Admin & External Affairs, MT
- Chief Operations Officer and Deputy General Manager, MT
- Chief of Staff, MT
- Chief of Police, MTPD, MT
- Director, Finance, MT
- Police Accountability Liaison, MTPD, MT
- Captain of Support Services, MTPD, MT
- Police Business Systems Manager, MTPD, MT

390 Robert Street North
Saint Paul, MN 55101-1805

651.602.1000
TTY 651.291.0904
public.info@metc.state.mn.us
metrocouncil.org