This document is made available electronically by the Minnesota Legislative Reference Library as part of an ongoing digital archiving project. https://www.lrl.mn.gov

INDEPENDENT AUDITOR'S REPORT

PRAIRIE ISLAND TRIBAL POLICE DEPARTMENT BODY-WORN CAMERA PROGRAM

JANUARY 5, 2022

RAMPART DEFENSE, LLC
P.O. BOX 23 CLEARBROOK, MN 56634

What Follows is the Prairie Island Tribal Police Department Policy noted as APPENDIX A, as presented to Rampart Defense LLC for compliance auditing check. After that Policy you will find our audit overview and recommendations.

APPENDIX A:

PRAIRIE ISLAND INDIAN COMMUNITY **Police Department**			Policy No:	41
			Date:	8/30/2017
BODY-WORN CAMERA POLICY			Revision:	0.0
Authorized By:	Date:		Page 1 of 11	

Purpose:

The primary purpose of using body-worn-cameras (BWCs) is to capture evidence arising from police-citizen encounters. This policy sets forth guidelines governing the use of BWCs and administering the data that results. Compliance with these guidelines is mandatory, but it is recognized that officers must also attend to other primary duties and the safety of all concerned, sometimes in circumstances that are tense, uncertain, and rapidly evolving.

Policy:

It is the policy of this department to authorize and require the use of department-issued BWCs as set forth below, and to administer BWC data as provided by law.

Scope:

This policy governs the use of BWCs in the course of official duties. It does not apply to the use of squad-based (dash-cam) recording systems. The Chief or Chief's designee may supersede this policy by providing specific instructions for BWC use to individual officers, or providing specific instructions pertaining to particular events or classes of events, including but not limited to political rallies and demonstrations. The Chief or designee may also provide specific instructions or standard operating procedures for BWC use to officers assigned to specialized details, such as carrying out duties in courts or guarding prisoners or patients in hospitals and mental health facilities.

Definitions:

The following phrases have special meanings as used in this policy:

A. **MGDPA or Data Practices Act** refers to the Minnesota Government Data Practices Act, Minn. Stat. § 13.01, et seq.

B. **Records Retention Schedule** refers to the General Records Retention Schedule for Minnesota Cities.

C. **Law enforcement-related information** means information captured or available for capture by use of a BWC that has evidentiary value because it documents events with respect to a stop, arrest, search, citation, or charging decision.

D. **Evidentiary value** means that the information may be useful as proof in a criminal prosecution, related civil or administrative proceeding, further investigation of an actual or suspected criminal act, or in considering an allegation against a law enforcement agency or officer.

E. **General Citizen Contact** means an informal encounter with a citizen that is not and does not become law enforcement-related or adversarial, and a recording of the event would not yield information relevant to an ongoing investigation. Examples include, but are not limited to, assisting a motorist with directions, summoning a wrecker, or receiving generalized concerns from a citizen about crime trends in his or her neighborhood.

F. **Adversarial** means a law enforcement encounter with a person that becomes confrontational, during which at least one person expresses anger, resentment, or hostility toward the other, or at least one person directs toward the other verbal conduct consisting of arguing, threatening, challenging, swearing, yelling, or shouting. Encounters in which a citizen demands to be recorded or initiates recording on his or her own are deemed adversarial.

G. **Unintentionally recorded footage** is a video recording that results from an officer's inadvertence or neglect in operating the officer's BWC, provided that no portion of the resulting recording has evidentiary value. Examples

of unintentionally recorded footage include, but are not limited to, recordings made in station house locker rooms, restrooms, and recordings made while officers were engaged in conversations of a non-business, personal nature with the expectation that the conversation was not being recorded.

H. **Official duties,** for purposes of this policy, means that the officer is on duty and performing authorized law enforcement services on behalf of this agency.

Use and Documentation:

A. Officers may use only department-issued BWCs in the performance of official duties for this agency or when otherwise performing authorized law enforcement services as an employee of this department.

B. Officers who have been issued BWCs shall operate and use them consistent with this policy. Officers shall conduct a function test of their issued BWCs at the beginning of each shift to make sure the devices are operating properly. Officers noting a malfunction during testing or at any other time shall promptly report the malfunction to the officer's supervisor and shall document the report in writing. Supervisors shall take prompt action to address malfunctions and document the steps taken in writing.

C. Officers should wear their issued BWCs at the location on their body and in the manner specified in training.

D. Officers must document BWC use and non-use as follows:

1. Whenever an officer makes a recording, the existence of the recording shall be documented in the WatchGuard Evidence Library, and any resulting incident report.

2. Whenever an officer fails to record an activity that is required to be recorded under this policy or captures only a part of the activity, the officer must document the circumstances and reasons for not recording in the WatchGuard Evidence Library, and any resulting incident report. Supervisors shall review the evidence library / reports and initiate any corrective action deemed necessary.

E. The department will maintain the following records and documents relating to BWC use, which are classified as public data:

1. The total number of BWCs owned or maintained by the agency;

2. A daily record of the total number of BWCs actually deployed and used by officers and, if applicable, the precincts in which they were used;

3. The total amount of recorded BWC data collected and maintained; and

4. This policy, together with the Records Retention Schedule.

General Guidelines for Recording

A. Officers shall activate their BWCs when anticipating that they will be involved in, become involved in, or witness other officers of this agency involved in a

pursuit, Terry stop of a motorist or pedestrian, search, seizure, arrest, use of force, adversarial contact, and during other activities likely to yield information having evidentiary value. However, officers need not activate their cameras when it would be unsafe, impossible, or impractical to do so, but such instances of not recording when otherwise required must be documented as specified in the Use and Documentation guidelines, part (D)(2) (above).

B. Officers have discretion to record or not record general citizen contacts.

C. Officers have no affirmative duty to inform people that a BWC is being operated or that the individuals are being recorded.

D. Once activated, the BWC should continue recording until the conclusion of the incident or encounter, or until it becomes apparent that additional recording is unlikely to capture information having evidentiary value. The officer having charge of a scene shall likewise direct the discontinuance of recording when further recording is unlikely to capture additional information having evidentiary value. If the recording is discontinued while an investigation, response, or incident is ongoing, officers shall state the reasons for ceasing the recording on camera before deactivating their BWC. If circumstances change, officers shall reactivate their cameras as required by this policy to capture information having evidentiary value.

E. Officers shall not intentionally block the BWC's audio or visual recording functionality to defeat the purposes of this policy.

F. Notwithstanding any other provision in this policy, officers shall not use their BWCs to record other agency personnel during non-enforcement related activities, such as during pre- and post-shift time in locker rooms, during meal

breaks, or during other private conversations, unless recording is authorized as part of an administrative or criminal investigation.

Special Guidelines for Recording

Officers may, in the exercise of sound discretion, determine:

A. To use their BWCs to record any police-citizen encounter if there is reason to believe the recording would potentially yield information having evidentiary value, unless such recording is otherwise expressly prohibited.

B. To use their BWCs to take recorded statements from persons believed to be victims of and witnesses to crimes, and persons suspected of committing

crimes, considering the needs of the investigation and the circumstances pertaining to the victim, witness, or suspect.

In addition,

C. Officers need not record persons being provided medical care unless there is reason to believe the recording would document information having evidentiary value. When responding to an apparent mental health crisis or event, BWCs shall be activated as necessary to document any use of force and the basis for it, and any other information having evidentiary value, but need not be activated when doing so would serve only to record symptoms or behaviors believed to be attributable to the mental health issue.

D. Officers shall use their BWCs and squad-based audio/video systems to record their transportation and the physical transfer of persons in their custody to hospitals, detox and mental health care facilities, juvenile detention centers, and jails, but otherwise should not record in these facilities unless the officer anticipates witnessing a criminal event or being involved in or witnessing an adversarial encounter or use-of-force incident.

Downloading and Labeling Data

A. Each officer using a BWC is responsible for transferring or assuring the proper transfer of the data from his or her camera via the WatchGuard Transfer Station by the end of that officer's shift. However, if the officer is involved in a shooting, in-custody death, or other law enforcement activity resulting in death or great bodily harm, a supervisor or investigator shall take custody of the officer's BWC and assume responsibility for transferring the data from it.

B. Officers shall label the BWC data files at the time of video capture or transfer to storage, and should consult with a supervisor if in doubt as to the appropriate labeling. Officers should assign as many of the following labels as are applicable to each file:

1. **Evidence—criminal:** The information has evidentiary value with respect to an actual or suspected criminal incident or charging decision.

2. **Evidence—force:** Whether or not enforcement action was taken or an arrest resulted, the event involved the application of force by a law enforcement officer of this or another agency.

3. **Evidence—property:** Whether or not enforcement action was taken or an arrest resulted, an officer seized property from an individual or directed an individual to dispossess property.

4. **Evidence—administrative:** The incident involved an adversarial encounter or resulted in a complaint against the officer.

5. **Evidence—other:** The recording has potential evidentiary value for reasons identified by the officer at the time of labeling.

6. **Training:** The event was such that it may have value for training.

7. **Not evidence:** The recording does not contain any of the foregoing categories of information and has no apparent evidentiary value. Recordings of general citizen contacts and unintentionally recorded footage are not evidence.

C. In addition, officers shall flag each file as appropriate to indicate that it contains information about data subjects who may have rights under the MGDPA limiting disclosure of information about them. These individuals include:

1. Victims and alleged victims of criminal sexual conduct and sex trafficking.

2. Victims of child abuse or neglect.

3. Vulnerable adults who are victims of maltreatment.

4. Undercover officers.

5. Informants.

6. When the video is clearly offensive to common sensitivities.

7. Victims of and witnesses to crimes, if the victim or witness has requested not to be identified publicly.

8. Individuals who called 911, and services subscribers whose lines were used to place a call to the 911 system.

9. Mandated reporters.

10. Juvenile witnesses, if the nature of the event or activity justifies protecting the identity of the witness.

11. Juveniles who are or may be delinquent or engaged in criminal acts.

12. Individuals who make complaints about violations with respect to the use of real property.

13. Officers and employees who are the subject of a complaint related to the events captured on video.

14. Other individuals whose identities the officer believes may be legally protected from public disclosure.

D. Labeling and flagging designations may be corrected or amended based on additional information

Administering Access to BWC Data:

A. **Data subjects.** Under Minnesota law, the following are considered data subjects for purposes of administering access to BWC data:

1. Any person or entity whose image or voice is documented in the data.

2. The officer who collected the data.

3. Any other officer whose voice or image is documented in the data, regardless of whether that officer is or can be identified by the recording.

B. **BWC data is presumptively private.** BWC recordings are classified as private data about the data subjects unless there is a specific law that provides differently. As a result:

1. BWC data pertaining to people is presumed private, as is BWC data pertaining to businesses or other entities.

2. Some BWC data is classified as confidential (see C. below).

3. Some BWC data is classified as public (see D. below).

C. **Confidential data.** BWC data that is collected or created as part of an active criminal investigation is confidential. This classification takes precedence over the "private" classification listed above and the "public" classifications listed below.

D. **Public data.** The following BWC data is public:

1. Data documenting the discharge of a firearm by a peace officer in the course of duty, other than for training or the killing of an animal that is sick, injured, or dangerous.

2. Data that documents the use of force by a peace officer that results in substantial bodily harm.

3. Data that a data subject requests to be made accessible to the public, subject to redaction. Data on any data subject (other than a peace officer) who has not consented to the public release must be redacted if practicable. In addition, any data on undercover officers must be redacted.

4. Data that documents the final disposition of a disciplinary action against a public employee.

However, if another provision of the Data Practices Act classifies data as private or otherwise not public, the data retains that other classification. For instance, data that reveals protected identities under Minn. Stat. § 13.82, subd. 17 (e.g., certain victims, witnesses, and others) should not be

released even if it would otherwise fit into one of the public categories listed above.

E. **Access to BWC data by non-employees.** Officers shall refer members of the media or public seeking access to BWC data to Chief of police, who shall process the request in accordance with the MGDPA and other governing laws. In particular:

1. An individual shall be allowed to review recorded BWC data about him- or herself and other data subjects in the recording, but access shall not be granted:

    a. If the data was collected or created as part of an active investigation.

    b. To portions of the data that the agency would otherwise be prohibited by law from disclosing to the person seeking access, such as portions that would reveal identities protected by Minn. Stat. § 13.82, subd. 17.

2. Unless the data is part of an active investigation, an individual data subject shall be provided with a copy of the recording upon request, but subject to the following guidelines on redaction:

    a. Data on other individuals in the recording who do not consent to the release must be redacted.

    b. Data that would identify undercover officers must be redacted.

    c. Data on other officers who are not undercover, and who are on duty and engaged in the performance of official duties, may not be redacted.

F. **Access by peace officers and law enforcement employees.** No employee may have access to the department's BWC data except for legitimate law enforcement or data administration purposes:

1. Officers may access and view stored BWC video only when there is a business need for doing so, including the need to defend against an allegation of misconduct or substandard performance. Officers may review video footage of an incident in which they were involved prior to preparing a report, giving a statement, or providing testimony about the incident.

i. Employees seeking access to BWC data for non-business reasons may make a request for it in the same manner as any member of the public.

G. **Other authorized disclosures of data.** Officers may display portions of BWC footage to witnesses as necessary for purposes of investigation as allowed by Minn. Stat. § 13.82, subd. 15, as may be amended from time to time. Officers should generally limit these displays in order to protect against the incidental disclosure of individuals whose identities are not public. Protecting against incidental disclosure could involve, for instance, showing only a portion of the video, showing only screen shots, muting the audio, or playing the audio but not displaying video. In addition,

1. BWC data may be shared with other law enforcement agencies only for legitimate law enforcement purposes that are documented in writing at the time of the disclosure.

2. BWC data shall be made available to prosecutors, courts, and other criminal justice entities as provided by law.

Data Security Safeguards

A. Access to the WatchGuard Server shall be limited to employees who have been certified by the BCA to have access to Criminal Justice Information as outlined in the CJDN Security Policy. Backup of data contained on the WatchGuard Server shall be done in accordance with the backup procedures of the Prairie Island Indian Community Information Technology Department.

B. Access to BWC data from city or personally owned and approved devices shall be managed in accordance with established city policy.

C. Officers shall not intentionally edit, alter, or erase any BWC recording unless otherwise expressly authorized by the Chief or the Chief's designee.

D. As required by Minn. Stat. § 13.825, subd. 9, as may be amended from time to time, this agency shall obtain an independent biennial audit of its BWC program.

Agency Use of Data

A. At least once a month, supervisors will randomly review BWC usage by each officer to ensure compliance with this policy and to identify any performance areas in which additional training or guidance is required.

B. In addition, supervisors and other assigned personnel may access BWC data for the purposes of reviewing or investigating a specific incident that has given rise to a complaint or concern about officer misconduct or performance.

C. Nothing in this policy limits or prohibits the use of BWC data as evidence of misconduct or as a basis for discipline.

D. Officers should contact their supervisors to discuss retaining and using BWC footage for training purposes. Officer objections to preserving or using certain footage for training will be considered on a case-by-case basis. Field training officers may utilize BWC data with trainees for the purpose of providing coaching and feedback on the trainees' performance.

Data Retention

A. All BWC data shall be retained for a minimum period of 90 days. There are no exceptions for erroneously recorded or non-evidentiary data.

B. Data documenting the discharge of a firearm by a peace officer in the course of duty, other than for training or the killing of an animal that is sick, injured, or dangerous, must be maintained for a minimum period of one year.

C. Certain kinds of BWC data must be retained for six years:

1. Data that documents the use of deadly force by a peace officer, or force of a sufficient type or degree to require a use of force report or supervisory review.

2. Data documenting circumstances that have given rise to a formal complaint against an officer.

D. Other data having evidentiary value shall be retained for the period specified in the Records Retention Schedule. When a particular recording is subject to multiple retention periods, it shall be maintained for the longest applicable period.

E. Subject to Part F (below), all other BWC footage that is classified as non-evidentiary, becomes classified as non-evidentiary, or is not maintained for training shall be destroyed after 90 days.

F. Upon written request by a BWC data subject, the agency shall retain a recording pertaining to that subject for an additional time period requested by the subject of up to 180 days. The agency will notify the requestor at the time of the request that the data will then be destroyed unless a new written request is received.

G. The department shall maintain an inventory of BWC recordings having evidentiary value.

H. The department will make available this policy, together with its Records Retention Schedule, upon request.

Compliance

Supervisors shall monitor for compliance with this policy. The unauthorized access to or disclosure of BWC data may constitute misconduct and subject individuals to disciplinary action and criminal penalties pursuant to Minn. Stat. § 13.09.

Audit Overview and Recommendations

Dear Prairie Island Tribal Council and Chief Priem:

We have audited the body-worn camera (BWC) program of the Prairie Island Police Department (PIPD) for the two-year period ended 6/30/2021. Minnesota Statute §13.825 mandates that any law enforcement agency operating a portable recording system (PRS)[1] program obtain an independent, biennial audit of its program. This program and its associated data are the responsibility of the Prairie Island Police Department. Our responsibility is to express an opinion on the operations of this program based on our audit.

On November 11, 2021, Rampart Defense LLC (Rampart) met with Chief of Police Jon Priem, who provided information about PIPD's BWC program policies, procedures and operations. As part of the audit, Rampart reviewed those policies, procedures and operations for compliance with Minnesota Statute §626.8473, which sets forth the requirements for creating and implementing a BWC program, and Minnesota Statute §13.825, which governs the operation of BWC programs. In addition, Rampart also conducted a sampling of BWC data to verify PIPD's recordkeeping.

The purpose of this report is to provide an overview of this audit, and to provide recommendations to improve the PIPD BWC program and enhance compliance with statutory requirements.

PIPD BWC Program Implementation and Authorization

Effective August 1, 2016, Minnesota Statute §626.8473 Subd. 2 requires that:

> A local law enforcement agency must provide an opportunity for public comment before it purchases or implements a portable recording system. At a minimum, the agency must accept public comments submitted electronically or by mail, and the governing body with jurisdiction over the budget of the law enforcement agency must provide an opportunity for public comment at a regularly-scheduled meeting.

As part of our audit, Chief Priem furnished to Rampart the following:

1. Images of the November 2016 and December 2016 issues of the Prairie Island Indian Community "Tinta Wita" newsletter, announcing the planned acquisition of an upgraded mobile video recording system by the Police Department, to include body-worn cameras, and soliciting public comment.
2. A copy of the signed Prairie Island Tribal Council Resolution approving the Prairie Island Police Department Body-Worn Camera Policy, dated 8/30/2017.

[1] It should be noted that Minnesota statute uses the broader term "portable recording system" (PRS), which includes body-worn cameras. Because body-worn cameras are the only type of portable recording system employed by PIPD, these terms may be used interchangeably in this report.

Chief Priem also advised us that because Tribal Council Meetings are closed to the public, he scheduled a separate open house for public comments prior to the Tribal Council considering the motion to approve the body-worn camera resolution.

In our opinion, Prairie Island Police Department met the public notice and comment requirements prior to the implementation of their BWC program later that year.

In addition, §626.8473 Subd. 3(a) requires that the law enforcement agency establish and enforce a written policy governing the use of its portable recording system, and states "[t]he written policy must be posted on the agency's Web site, if the agency has a Web site."

Chief Priem also furnished to Rampart a copy of PIPD's written BWC policy. Prairie Island Police Department does not have its own website.

PIPD BWC WRITTEN POLICY

As part of this audit, we reviewed PIPD's BWC policy, a copy of which is attached to this report as Appendix A.

Minnesota Statute §626.8473 Subd. 3(b) requires a written BWC policy to incorporate the following, at a minimum:

1. The requirements of section 13.825 and other data classifications, access procedures, retention policies, and data safeguards that, at a minimum, meet the requirements of chapter 13 and other applicable law;
2. Procedures for testing the portable recording system to ensure adequate functioning;
3. 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;
4. Circumstances where recording is mandatory, prohibited, or at the discretion of the officer using the system;
5. Circumstances under which a data subject must be given notice of a recording;
6. Circumstances under which a recording may be ended while an investigation, response, or incident is ongoing;
7. Procedures for the secure storage of portable recording system data and the creation of backup copies of the data; and
8. Procedures to ensure compliance and address violations of the policy, which must include, at a minimum, supervisory or internal audits and reviews, and the employee discipline standards for unauthorized access to data contained in section 13.09.

Due to their complexity and interrelatedness, clauses 1 and 7 are discussed separately below. Clause 8 is also discussed separately.

In our opinion, the PIPD BWC policy is compliant with respect to clauses 2 – 6.

PIPD BWC Data Retention

Prairie Island Police Department follows the General Records Retention Schedule for Minnesota Cities (GRRSMC) with respect to BWC data classified as evidentiary in nature. PIPD's BWC policy defines this to include "information [that] may be useful as proof in a criminal prosecution, related civil or administrative proceeding, further investigation of an actual or suspected criminal act, or in considering an allegation against a law enforcement agency or officer." A review of the relevant sections of the current GRRSMC schedule indicates that the stated retention guidelines appear to meet or exceed the requirements specified for each category of BWC data enumerated in §13.825 Subd. 3(b). PIPD's policy specifies a 90-day retention period for all other BWC data, as required in §13.825 Subd. 3(a).

PIPD employs Watchguard body-worn cameras, with all BWC data stored on a secure, in-house server. PIPD manages BWC data retention automatically through its Watchguard software, based on the data classification assigned to each video at the time of upload.

PIPD's BWC policy requires that each officer transfer data from his or her body-worn camera via the Watchguard Transfer Station by the end of each shift, and also requires that the officer assign the appropriate label or labels to each file to identify the nature of the data.

Chief Priem advised us that BWC data are shared with outside agencies only upon receipt of a written request. Data sharing is accomplished via a weblink through Watchguard's cloud service. No BWC data is uploaded to the cloud; rather, that service is used to create and distribute the weblink. Chief Priem advised us that he will discuss with Watchguard the possibility of adding a statement regarding the receiving agency's obligations under §13.825 Subd. 8(b) to maintain BWC data security, along with a mandatory acknowledgment of those obligations.

In our opinion, PIPD's written BWC policy is compliant with respect to applicable data retention requirements.

PIPD BWC Data Destruction

As discussed in the preceding section, Chief Priem advised us that PIPD BWC data are stored on an in-house server, with data retention and deletion schedules managed automatically through the Watchguard software based on the assigned data classification of each video.

Chief Priem advised us that any server used to store BWC data will be subject to degaussing in accordance with Federal Bureau of Investigation Division of Criminal Justice Information Services (CJIS) digital media sanitation guidelines at such time as that server is removed from service. The server would then be subject to physical destruction.

In our opinion, PIPD's written BWC policy is compliant with respect to the applicable data destruction requirements.

PIPD BWC Data Access

Any requests for access to BWC data by data subjects would be facilitated by Chief Priem in accordance with the provisions of §13.825 Subd. 4(b).

According to PIPD policy, BWC data "may be shared with other law enforcement agencies only for legitimate law enforcement purposes that are documented in writing at the time of the disclosure." As discussed above, Chief Priem has expressed his intent to add a mandatory acknowledgment of the requesting agency's obligations under §13.825 Subd. 8(b) regarding security of BWC data.

In our opinion, PIPD's written BWC policy is compliant with respect to the applicable data access requirements.

PIPD BWC Data Classification

PIPD BWC Policy states that "BWC data is presumptively private," and further states that "BWC recordings are classified as private data about the data subjects unless there is a specific law that provides differently." Active criminal investigation data are classified as confidential. PIPD BWC Policy also identifies certain categories of BWC data that are public.

This section of the PIPD BWC policy mirrors the categories and language of §13.825 Subd. 2. In our opinion, this policy is compliant with respect to the applicable data classification requirements.

PIPD BWC Internal Compliance Verification

The PIPD BWC Agency Use of Data section states that:

> At least once a month, supervisors will randomly review BWC usage by each officer to ensure compliance with this policy and to identify any performance areas in which additional training or guidance is necessary.
>
> In addition, supervisors and other assigned personnel may access BWC data for the purpose of reviewing or investigating a specific incident that has given rise to a complaint or concern about officer misconduct or performance.

The PIPD BWC Compliance section states that "[s]upervisors shall monitor for compliance with this policy."

Chief Priem advised us that he conducts internal audits both weekly and monthly.

PIPD's written BWC policy addresses consequences associated with violations of the policy, to include both disciplinary action and potential criminal penalties pursuant to Minnesota Statute §13.09.

In our opinion, this policy is compliant with respect to the compliance and disciplinary requirements contained in §626.8473 Subd. 3(b)(8).

PIPD BWC Program and Inventory

PIPD currently possesses eight (8) Watchguard body-worn cameras.

The PIPD BWC policy identifies those circumstances in which deputies are expected to activate their body-worn cameras, as well as circumstances in which they are prohibited from activating their body-worn cameras. The policy also provides guidance for those circumstances in which BWC activation is deemed discretionary.

Chief Priem advised us that he is able to determine through their system not only the number of BWCs deployed at any given time, but identify the officers deploying those devices. This information can also be determined after the fact by reviewing the schedule and/or payroll data.

As of 11/11/2021, PIPD maintained 6.52 TB of BWC data.

PIPD BWC Physical, Technological and Procedural Safeguards

PIPD BWC data are initially recorded to a hard drive in each officer's BWC. Those files are then transferred through a manual process to an in-house server. During the period covered by our audit, PIPD experienced a loss of BWC data due to an apparent software issue, which is discussed in greater detail in the Data Sampling section of this report.

Officers have view-only access to their own data for report writing, trial preparation, data administration, investigatory purposes and other legitimate law enforcement purposes. Officers are required to document the reasons for accessing BWC data each time they do so. All BWC data access is logged in the Watchguard software and is available for audit purposes.

As noted above, requests by other law enforcement agencies for PIPD BWC data must be approved by Chief Ryan. This data is furnished to the requesting agency via a weblink. PIPD follows this same process when providing BWC data to prosecutors and the courts.

Enhanced Surveillance Technology

PIPD currently employs BWCs with only standard audio/video recording capabilities. They have no plans at this time to add enhanced BWC surveillance capabilities, such as thermal or night vision, or to otherwise expand the type or scope of their BWC technology.

If PIPD should obtain such enhanced technology in the future, Minnesota Statute §13.825 Subd. 10 requires notice to the Minnesota Bureau of Criminal Apprehension within 10 days. This notice must include a description of the technology and its surveillance capability and intended uses.

Data Sampling

Rampart selected a random sample of 135 ICRs from which to review any available BWC recordings. In addition, Rampart conducted an exception check of two ICRs labeled "CAD_PUSH_PENDING." It should

be noted that not every call will result in an officer activating his or her BWC. For example, an officer who responds to a driving complaint but is unable to locate the suspect vehicle would be unlikely to activate his or her BWC. It should also be noted that because the audit covers a period of two years, while most BWC data is only required to be retained for 90 days, there is a significant likelihood that the sample population will include ICRs for which BWC data was created, but which has since been deleted due to the expiration of the retention period. The auditor reviewed the retained BWC videos to verify that this data was accurately documented in PIPD records.

Chief Priem explained that the two ICRs labeled "CAD_PUSH_PENDING" were "blank" ICRs that were created by accident, with no corresponding call for service or officer ever assigned.

During this review, nine (9) of the requested videos were identified as "Event Archived - Unable to restore." Chief Priem explained that PIPD's Watchguard server has experienced an intermittent issue in which the server fails to roll over to a new hard drive when the current drive becomes full, resulting in the overwriting and loss of BWC data. Chief Priem made Information Technology staff available to explain the issue in greater detail. Prairie Island IT staff advised that they are working directly with Watchguard IT staff to resolve the issue.

With the exception of the videos identified as "Event Archived – Unable to restore," which our auditor was unable to view, all of the videos selected for review were found to be labeled and retained correctly. The Rampart auditor then conducted additional testing to confirm that videos identified as purged had, in fact, been purged.

We recommend that Prairie Island Police Department consider employing a cloud-based service or utilize other means to create a back-up copy of all BWC data as a safeguard against the future loss of BWC data due to software or hardware issues associated with their Watchguard server.

Audit Conclusions

In our opinion, the Prairie Island Police Department's Body-Worn Camera Program is substantially compliant with Minnesota Statutes §13.825 and §626.8473.

Daniel E. Gazelka

Rampart Defense LLC

1/05/2022