Biennial Audit of the Starbuck Police Department Portable Recording System (Body-Worn Cameras) Conducted by LEADS Consulting
Audit Summary Report
Submitted July 23, 2018

Pursuant to Minnesota Statute 13.825, LEADS Consulting conducted an audit of the Portable Recording System (Body Worn Cameras) at the Starbuck Police Department to ensure compliance with state law. The site visit was conducted on March 27, 2018. Police Chief Mitch Johnsrud, who manages the system, was the point of contact for auditors. Chief Johnsrud serves as the department "Responsible Authority" for data practices related issues and also supervised the maintenance of data for the Portable Recording System. The Starbuck Police Department policies regarding "Body Worn Cameras" were collected and reviewed in detail in the weeks following the site visit. A copy is attached to this audit as appendix A.

Verbal information regarding operations and practices was received from Chief Johnsrud. The audit examined the policies and practices of the department in regards to the use and operation of their Portable Recording Systems including the following functions:

1. Portable Recording System Technology
2. Records Maintenance and Data Protection
3. Data Classification
4. Retention and Destruction of Data
5. Data Use and Access to Data by Agency
6. Sharing Data with other Agencies
7. Access to Data by Subjects

Starbuck Police Department Policy

The Starbuck Police Department Policy regarding their Portable Recording System is complete and specific regarding use and practices. It includes provisions regarding access to data, agency use of data, classification of data and retention of data. A copy of the policy known as General Order 49 is attached to this report as appendix A.

Starbuck Portable Recording System Technology

The Starbuck Police Department has been utilizing the "WatchGuard Body-Worn Camera System since June of 2016. At the time of the site visit they had two body worn cameras shared by 4 full time officers and 8 part time officers. As of March 27, 2018, the system data base had recorded 839 video events. Each event is coded with an event category upon its creation or in the near future by the officer who initiated the recorded event. It was noted that the WatchGuard version being used by the Starbuck Police Department was not the most current version. Chief Johnsrud stated that upgrading to the most current version would involve additional cost that had not yet been approved. Their current version did not provide an audit trail for auditors to examine who had accessed the video system.

Maintenance of Records and Data Protection

The WatchGuard system used by the Starbuck Police Department maintains detailed records showing the date and time that portable recording system data were collected. The Starbuck Police Department has a dedicated computer server at their police department to house the data with support from the Pope County IT unit. The system is password and user role protected from unauthorized intrusion.

Data Classification

The Starbuck Police Department utilizes the applicable classification of data under Minnesota Statute 13.825. Their department policy includes several references to data classification for Body Worn Camera data and makes reference to the Minnesota Data Practices law and MN Statute 13.825. Chief Johnsrud is knowledgable of the "Portable Recording System" data classifications required under MN statues and he also serves as the "Responsible Authority" under the Data Practices provisions.

The Starbuck Police Department had not had a recording of an incident documenting the discharge of a firearm by a police officer in the course of duty or an incident documenting the use of force by a police officer that resulted in substantial bodily harm. Active criminal investigative data are considered confidential or protected nonpublic.

The department had not had a request from a subject of a video recording to make the data public or to extend the retention period.

The Starbuck Police Department policies and practices regarding data classification are consistent with state statutes.

Retention and Destruction of Data

Minnesota Statute 13.825 Subd. 3 sets out specific minimum data retention requirements for different types of incidents captured by Portable Recording System devices. PRS data that are not active or inactive criminal investigation must be maintained for 90 days. After 90 days the data may be destroyed according to the agency's records retention schedule.

The Starbuck Police Department has a portable recording system data retention policy that is consistent with state law and references MN Statute 13.825. A copy of the policy is attached. At the time of the site visit they had not deleted or destroyed any line of duty data. The data that is not required to be kept under Minnesota Statutes will be destroyed consistent with the city's retention schedule which is based on the recommended policy of the League of Minnesota Cities. A copy of the retention schedule was provided to the auditors.

The WatchGuard system allows the officers to create event descriptions that provide guidance as to whether the data has a further investigative purpose or requires longer retention.

Active criminal investigative data is maintained and destroyed pursuant to MN Statute and the department's retention schedule.

The examination indicates that the Starbuck Police Department is in compliance with the "retention and destruction" of data provisions regarding Portable Recording Systems.

Data Use and Access to Data

The Starbuck Police Department has a detailed policy regarding access to data which states “No employee may have access to the department’s BWC data except for legitimate law enforcement or data administrative purposes.” The policy goes on to state, “Officers may access and view stored BWC video only when there is a business need.” The system does not have an audit trail; however, the department policy does require officers to document in their reports if they access the data base for review.

Supervisors are also authorized to “randomly review BWC usage by officers to ensure compliance with policy and identify any performance area in which additional training or guidance is required”.

Auditors examined randomly selected 43 video data events. As mentioned there was no audit trail to examine as this version of WatchGuard did not include an audit trail function. All recordings were made in the line of duty.

There is no evidence to suggest that there was any inappropriate access to the video data, however, LEADS auditors recommend that the City of Starbuck upgrade the WatchGard system to version 4 to ensure that an audit trail capacity exists.

Sharing Data with other Law Enforcement Agencies

All requests for sharing of data from other agencies are directed to Chief Johnsrud. He states that they have only had requests from other agencies when they are on a joint call for service. Their policy states, “BWC data may be shared with other law enforcement agencies only for legitimate enforcement purposes that are documented in writing at the time of the disclosure.”

The Starbuck Police Department is in compliance with the “Sharing Among Agencies” provision of state law.

Access to Data by Subjects

The Starbuck Police Department follows MN Data Practice law and provides for release of subject data when requested. Chief Johnsrud is the “responsible

authority" for those requests but states that at the time of the site visit they had not received any citizen requests for Portable Recording System video data.

The Starbuck Police Department is in compliance with the "Access to Data by Subjects" provision of state law.

Audit Conclusion

The Starbuck Police Department has a Portable Recording System policy that reflects MN statute 13.825 and contains significant specific regulations to ensure compliance with the statute. The department's policies and practices are consistent with state law. The data system is properly maintained and professionally monitored by Chief Mitch Johnsrud. LEADS Consulting recommends updating the WatchGuard system to a newer version in order enable the audit trail capacity desired by the Minnesota Legislature.

LEADS Consulting finds the Starbuck Police Department "Portable Recording System" policies and practices to be in compliance with the provisions referenced in Minnesota Statute 13.825 Subd. 9, Biennial Audit.

Bob Fletcher
Director
LEADS Consulting
Law Enforcement Audit and Data Services
www.leads50.com

SECTION 8 – BODY WORN CAMERA

(Updated 4/6/2018)

GENERAL ORDER 49
BODY WORN CAMERA

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 Records Retention Schedule of Minnesota State Statute 13.825 sub. 3.

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 an incident report or on the Evidence Section in RMS (LETG) if no report is written.

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 an incident report or in the Case Notes in RMS (LETG) if no

report is written. Supervisors shall review these 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 should 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 to that officer's folder located on the digital evidence computer 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 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/Administrative Assistant 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. Except as provided in the critical incident response policy, 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.

2. Agency personnel shall document their reasons for accessing stored BWC data within incident reports/supplements/case notes to the case file relate to the video, at the time of each access. Agency personnel are prohibited from accessing BWC data for non-business reasons and from sharing the data for non-law enforcement related purposes, including but not limited to uploading BWC data recorded or maintained by this agency to public and social media websites.

3. 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. All BWC files recorded will be only downloaded onto the departments Digital Evidence computer. This computer will not be connected to any network and will have mirrored drive to prevent any data loss.

B. Personally owned devices, including but not limited to computers and mobile devices, shall not be programmed or used to access or view agency BWC data.

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 - Follows MN State Statute 13.825 sub. 3

A. Portable recording system data that are not active or inactive criminal investigative data and are not described in paragraph (b) must be maintained for at least 90 days and destroyed according to the agency's records retention schedule approved pursuant to section 138.17.

B. Portable recording system data must be maintained for at least one year and destroyed according to the agency's records retention schedule approved pursuant to section 138.17 if:

1. the data document (i) the discharge of a firearm by a peace officer in the course of duty if a notice is required under section 626.553, subdivision 2, or (ii) the use of force by a peace officer that results in substantial bodily harm; or

2. a formal complaint is made against a peace officer related to the incident.

C. If a subject of the data submits a written request to the law enforcement agency to retain the recording beyond the applicable retention period for possible evidentiary or exculpatory use related to the circumstances under which the data were collected, the law enforcement agency shall retain the recording for an additional time period requested by the subject of up to 180 days and notify the requester that the recording will then be destroyed unless a new request is made under this paragraph.

D. Notwithstanding paragraph (b) or (c), a government entity may retain a recording for as long as reasonably necessary for possible evidentiary or exculpatory use related to the incident with respect to which the data were collected.

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

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.

The department will post this policy, together with its Records Retention Schedule, on its website.