3.11 SCOPE OF WORK BODY WORN CAMERA (BWC)

3.11.1 The State of Nevada is seeking a qualified vendor that can provide at a minimum, the following:

3.11.1.1 A Video Management System (VMS) that is either an externally hosted cloud-based data storage solution with the capability of organizing/managing video/digital evidence, server based or consist of a hybrid solution and be accessible via the internet to multiple users simultaneously. The State prefers the Cloud or Hybrid solution. The system must meet the State's geographical needs as described in this RFP.

Complies. Evidence.com is a cloud-based data storage solution with the capability of organizing/managing video/digital evidence, and is accessible via the internet to multiple users simultaneously.

3.11.1.2 Up to 489 high quality Body Worn Cameras necessary to outfit 465 sworn (Lieutenants and below) with 5% spares.

Complies. The attached quote includes 5% spares.

3.11.1.3 The VMS shall have the ability to convert video to a portable media device i.e.: (DVD, external hard drive) without compromising its authenticity to include all metadata and chain of custody requirements.

Complies. Users can access a file on Evidence.com, download the file, and then copy it to a CD/DVD or flash/thumb drive. DVDs and CDs can be created using any DVD or CD writing software. Axon cameras record using MP4 format, which is playable without the need for proprietary software.

Users can download individual files and can bulk download files in ISO or ZIP file format, either of which is suitable for removable media. This offers flexibility in packaging depending on HHP requirements.

Evidence.com ensures a reliable chain of custody for all video files by providing a high level of security, reliability, and expandability. Proper documentation of chain of custody is preserved and can be used to ensure video evidence can be tendered in court as an exhibit. There are also several levels of evidence protection implemented such as, encryption, access control, hashing and other security protocols.

To ensure a robust chain of custody, evidence can be verified for authenticity by matching the SHA hash of original file ingested in Evidence.com with the copy.
Audit trails associated with each and every piece of evidence stored in your agency's account will be able to demonstrate:

- ***how the video was taken***
- ***when the video was taken***
- ***where the video was taken***
- ***how the video was stored***

- ***who had access to the video from the time it was taken through the time it is introduced in court, and***
- ***Details on whether or not it has been altered and how (the original file is never altered, a new copy is created with any changes)***

By the end of 2016 the solution will fully migrate to SHA-2.

<u>Sharing Audit Report</u>
The Sharing Audit report exports a list of all user actions related to sharing evidence and cases to a CSV file. You can specify the date range for the report. Included in the report are the following details:

- ***Date and time of the sharing event***
- ***Who initiated the sharing event***
- ***What was shared — evidence or a case***
- ***How was it shared — internal or external to your Evidence.com agency***
- ***The ID of the evidence or case shared***
- ***The recipient of the shared evidence or case***
- ***The permissions shared to the recipient***

A full list of the metadata included in the report is listed below.

- ***Date Time***
- ***Action***
- ***Share Type***
- ***User***
- ***Owner***
- ***Evidence ID***
- ***Evidence Title***
- ***Case ID***
- ***Files Shared***
- ***Recipient email(s)***
- ***Agency***
- ***Duration***
- ***Expiration***
- ***View Permission***
- ***Download Permission***
- ***View Audit Trail Permission***
- ***Post Notes Permission***
- ***Reshare Download Permission***

3.11.1.4 Full service vendor support including installation, maintenance/ support, warranty, training, documentation, and project management throughout the contract period.

Complies. TASER will provide support including installation, maintenance/ support, warranty, training, documentation, and project management throughout the contract period.

3.11.1.5 All-inclusive pricing for all hardware (body worn cameras, workstations, servers, archiving hardware, video back-up systems, access points, automatic triggering devices, connectivity (Ethernet wiring), and software (system, database, and video management) installation, configuration, and training).

Complies. Please see the attached quote and Master Services and Purchasing Agreement.

3.11.1.6 Proposed systems that consist of server based video evidence management must be turn-key and provide warranties and full service maintenance and support on all hardware, wiring infrastructure, and software for a period of five (5) years.

Not applicable. Evidence.com is a cloud-based solution.

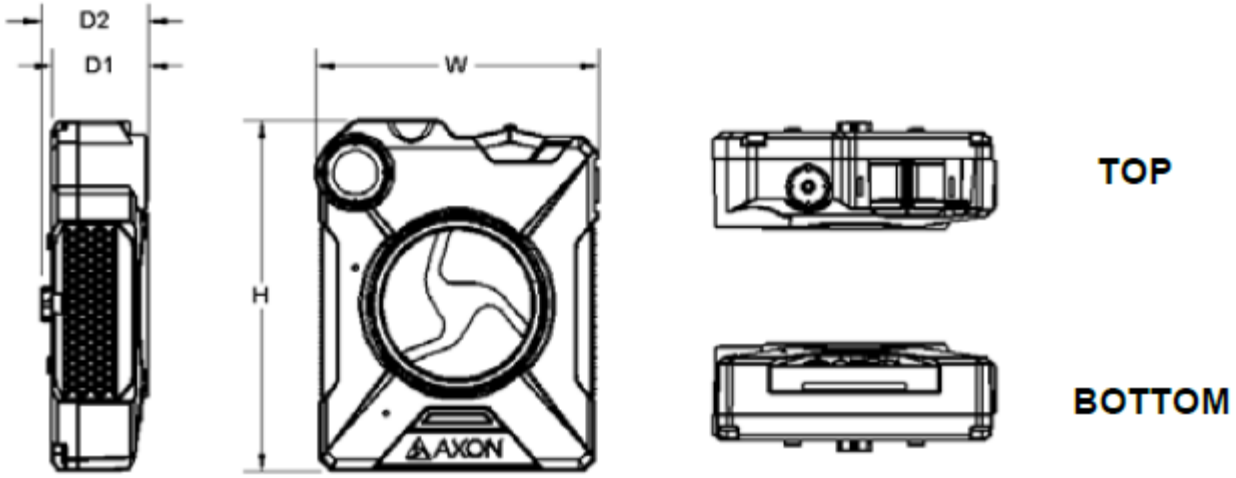
3.11.2 Body Worn Cameras

Specifications are provided by area including BWC Hardware Requirements, Evidence Managements System, Video Storage, System Security, Information Security, In-car Video Integration, Training and warranty.

3.11.3 BWC Hardware Requirements

3.11.3.1 Cameras worn by officers shall be lightweight, preferably six ounces or less in total combined weight.

Yes. The total weight of the <u>Axon Body 2</u> is 5.0 oz. (142 grams) (inclusive of all fastenings for the standard Klick Fast mount). The device is extremely compact and does not have any moving parts. The camera, which is slightly larger than a pack of cards measures 3.42 in x 2.76 in x 1.01 in (8.7 cm x 7.0 cm x 2.6 cm).



3.11.3.2 Cameras shall have minimal wiring, not exceed two wires or cables and shall be designed to disengage to prevent the wearer from becoming entangled.

Yes. The <u>Axon Body 2</u> is a self-contained audio-visual unit with no external wires.

3.11.3.3 Cameras shall have recording capability of at least ten continuous (10) hours (the State would prefer twelve (12) hours of continuous recording capability).

Yes. The <u>Axon Body 2</u> video camera has a minimum video resolution of 480P and a maximum video resolution of 1080P. It utilizes an aspect ratio of 16:9 at 1080P and 720P and a 4:3 aspect ratio at 480P. The video resolution, the encoding bitrate, the frame rate and the video encoding format impact the size of the files captured at each setting. The Axon Body 2 has 64GB of non-removable storage.

The Axon Body 2 video camera has four video quality settings, Low SD, High SD, Low HD, High HD spanning 480P, 720P and 1080P video resolutions.

- ***The Low SD setting captures video at a 480P video resolution at a rate of .81 GB per 60 minutes of video. This allows for over 70 hours of recording***
- ***The High SD setting captures video at a 480P video resolution at a rate of 1.8 GB per 60 minutes of video. This allows for over 35 hours of recording***
- ***The Low HD setting captures video at 720P video resolution at a rate of 2.7 GB per 60 minutes of video. This allows for over 23 hours of recording***
- ***The High HD setting captures video at 1080P video resolution at a rate of 5.4 GB per 60 minutes of video. This allows for 11.3 hours of recording***

At 480p and 720p, the Axon Body 2 will provide enough power for 12+ hours of recording time. At 1080P, the Axon Body 2 will provide enough power for 10+ hours of recording time.

3.11.3.4 Cameras must have a minimum stand-by battery life of ten (10) hours without recharging or additional batteries, with pre-record on.

Yes. The <u>Axon Body 2</u> battery will last 12+ hours when turned on and in buffering mode.

3.11.3.5 BWC Shall be user friendly that can be activated easily during times of stressful events.

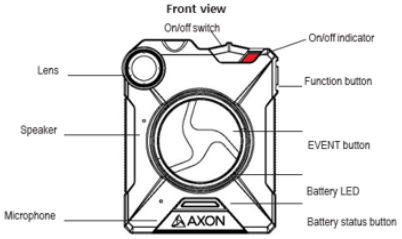
Yes. A complicated activation mechanism is cumbersome in the field and can impede more important duties, especially considering officers often have to start a recording at a moment's notice.

The <u>Axon Body 2</u> was designed specifically for use by law enforcement in tactical policing situations. Activation of event recording is simple and accessible, so officers can operate the device in a high-stress situation. Recordings are initiated with a single "Event Button" located on the front of the device, so an officer can easily reach it with one hand.

The Axon Body 2 camera has two operating modes:

1. ***BUFFERING (turning on the camera and starting pre-event buffering)***
2. ***EVENT (event recording)***

To initiate Buffering Mode (turn the camera on) Move the ON/OFF switch on the camera to the ON position. The raised on/off switch is strong enough to prevent accidentally powering the device down, yet can still be switched on if an officer is wearing gloves.



To initiate Event Recording Mode, simply tap the large concave button on the front of the camera two times. While the device is easily activated when worn in a shirt pocket or housed in a case, it is still protected against unintentional event triggering. To end the recording, simply hold down the button for three seconds.

3.11.3.6 BWC should have automatic triggers, as a standalone system.

Yes. Axon Signal is a system for secure activation of Axon camera devices. It is protocol, which operates over Bluetooth Low Energy. The effective range of Axon Signal is 30ft (~10 meters). The Axon Signal protocol is implemented by all Axon cameras, by the Axon Signal box and by an upcoming battery module for TASER conductive electric weapons.

Signal can convey specific telemetry messages that describe the state of the environment. Axon cameras capture these messages and store them as metadata within the video. Depending on the specific telemetry contained within the message, Axon cameras can decide to start or stop recording.

Specific activation criteria are listed below:

- ***Binary triggers: on-off triggers for 1 - 24V inputs. These inputs include door switches, light-bar, shotgun/patrol rifle release, brake switches or dedicated on-off switches.***
- ***ECU speed trigger: this input measures the time between speed pulses from the vehicle ECU. The period between pulses is changes in proportion to the vehicle speed. The Signal Box can be configured to match the time between pulses at 60 MPH to provide a highly accurate representation of vehicle speed. On the receiving side, Axon cameras can be configured to activate at a specific speed, such as 90mph.***
- ***Accelerometer: All Axon cameras include an accelerometer and can be configured to activate based on a high-G event, such as that of a crash.***
- ***MDT GPS: Should the MDT laptop or tablet contain a GPS receiver, the solution can utilize that source of GPS data. This data is used to store location and vehicle speed data within the video files.***
- ***Mobile Application: mobile apps can send activation events. These events will allow future functionality such as real-time CAD activation where an officers cameras are activated as soon as they are assigned to a call.***
- ***Another Wearer's Axon Camera: Axon cameras can be configured to broadcast Signal messages when activated. Thus Fleet cameras will activate when a nearby Axon Body 2 begins recording.***
- ***TASER CEW: TASER is producing a retrofit battery for existing TASER weapons. This battery will activate Axon cameras when the CEW safety is disabled.***

- ***External GPS: Axon Signal will accept a NMEA-format serial input from external GPS devices, such as those used for AVL systems. This GPS data can be added to the video as the definitive source of GPS data. This functionality will be enabled by the end of the 2016.***

3.11.3.7 Rechargeable battery must be able to reach full charge, from no power, in no more than six (6) hours.

Yes. The recharge time for 12+ hours of buffering mode is approximately six (6) hours when a camera with a fully depleted battery is charged in the Axon Dock.

3.11.3.8 Cameras must have a minimum of thirty-two (32) GB internal/integrated memory and storage media not be removable.

Yes. The Axon Body 2 has 64GB of non-removable storage.

3.11.3.9 Rechargeable battery must be able to withstand at least three hundred (300) charging cycles, maintaining the 10 hour record time.

Yes. The Axon battery is capable of hundreds of charges.

3.11.3.10 BWC lens must have a field of view from 95 to 145 degrees.

Yes. The Axon Body 2's 143° wide-angle lens was designed to record a wide field of view (FOV) to capture accurate evidence, even when the device is mounted on an officer's beltline. Axon Body 2's diagonal field of view is 107° horizontal and 78° vertical.

A wide FOV provides a better representation of what the officer is seeing and provides a record of the officer's environment.

Distortion Correction

In order to achieve an ultra-wide FOV, most cameras use an ultra-wide angle lens or 'fisheye' lens. Fisheye lenses result in distortion of the image. The Axon Body 2 automatically corrects for this distortion. Correcting for this distortion results in an overall better quality video. This difference is especially noticeable when dealing with still images generated from wide FOV video.

Distortion Correction via Software

Unlike many competitors' cameras, TASER's Axon Body 2 camera automatically corrects for fisheye on the camera. TASER's backend software (Evidence.com) currently provides the NHP the ability to correct for wide-angle distortion through Evidence.com.

3.11.3.11 The recording speed shall be no less than 30 frames per second (fps).

Yes. The Axon records 30 FPS.

3.11.3.12 Camera shall record video images in full color with a minimum resolution of 640 pixels x 480 pixels. Adjustable resolution is preferable.

Yes. The Axon Body 2 represents excellent value, with the ability to record synchronized audio and video with image quality in excess of Color 640x480. The device also has an HD option. The device can

record at 480P, 720P, or 1080P.

The device's HD settings (720, 1080P) provide the necessary resolution to facilitate the creation of still images or future advanced analytics (e.g. facial recognition, ANPR, etc.). This protects the NHP's investment by providing functionality that will be required in the future, without the need for further outlay.

The Axon Body 2 records at 30 FPS; in policing situations, officers often deal with objects in motion. The higher frame rate results in smoother video, resulting in a clearer, more functional piece of evidence.

3.11.3.13 Video compression shall be H.263 or higher.

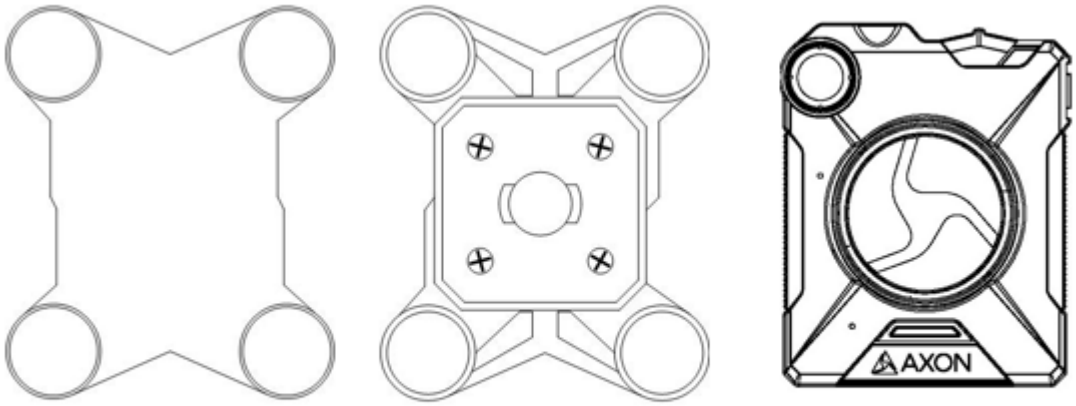
Yes. The Axon Body 2 conforms to the MPEG-4 Layer 2 video compression format, which utilizes a MP4 container and the H.264 compression standard. This format is non-proprietary and allows for playback from any general video player.

3.11.3.14 Cameras shall have multiple mounting options to accommodate varying uniformed officers, plain-clothed officers, and tactical field situations. Examples include, but are not limited to, lapel, shoulder, eyeglasses, cap, helmet, holster, button shirt, zipper shirt, utility belt, snow suit etc. Mounts shall not require modification to current in-service uniforms.

Yes. <u>The Axon Body 2</u> is a self-contained audio-visual unit with no external wires. The camera mounts utilize RapidLock technology, an attachment mechanism that allows the camera to be connected and disconnected from the mount in less than one second, while remaining securely and stably attached during an officer's shift. Officers can easily remove and remount the camera as desired, decreasing the time interacting with mounts and camera holsters on a daily basis.

The proprietary RapidLock design facilitates articulation at the mount (rather than the camera itself) giving the user greater control over the direction the unit is pointed. This improves the quality of video captured by allowing the camera to tilt, rotate, etc. And, by moving articulation to the mount, the camera design is more rugged as compared to cameras with integral moving parts.

RapidLock Mount



Back Lock Camera

TASER provides a variety of mounting options to suit your agency needs. Some are optimized for security (Z-Bracket, Molle, and Clip Mounts), while others are built for versatility (Magnet and Velcro mounts).

Tactical Axon Body 2 Mounts

The Z-Bracket Mount can be worn inserted in between the buttons of a shirt and is available oriented for both male and female uniforms.

Z-Bracket Mount

We also offer two Magnetic Mounts - one that is flexible for lighter weight uniform shirts and a thicker version for outerwear. Powerful magnets keep the device fully secure, and offer a wider range of space to mount the on the body as they do not rely on close proximity to buttons or pockets.

Outerwear Magnet Mount Flexible Magnet Mount

We offer two Molle Mounts, which attach to the Molle straps on tactical vests. The mounts can withstand >100 lbs of retention force. The Double Molle Mount provides more lateral stability, while the Single Molle Mount is lighter and more versatile.

Tactical Vest

Single Molle Mount

Double Molle Mount

Versatile Axon Body 2 Mounts

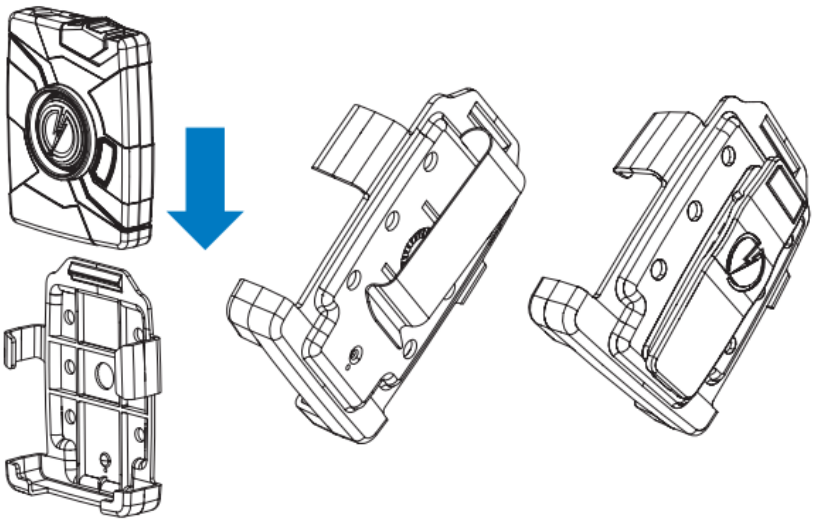
For uniforms, we offer a 4" and 6" Shirt Pocket Mount. The Axon Body 2 Clip Mount is simple and easy to install and offers versatile mounting locations for non-tactical use. A Velcro Mount will available for uniforms or vests with Velcro patches applied in Q4 of 2016.

Shirt Pocket Mount

Clip Mount

The Axon Flex system offers several mounting options for wearing the Flex camera and carrying the Flex controller.

Axon Flex Controller Mounts



Hybrid Holster

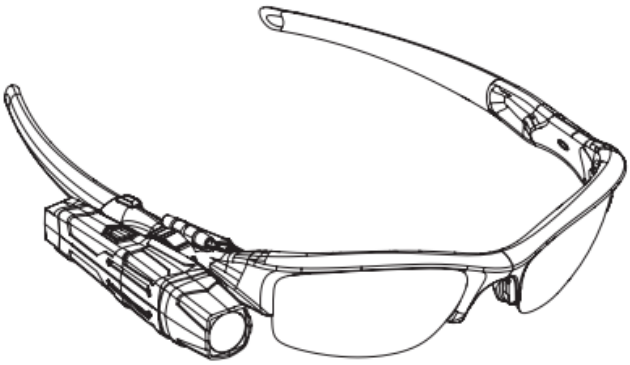
The controller can be carried in a holster that clips to your clothing or gear. Two clips are available for you to place the controller in a way that best meets your needs. Both options are compatible with many standard duty belt clips.

- ***Large Utility Belt Clip***
- ***Regular Utility Belt Clip***

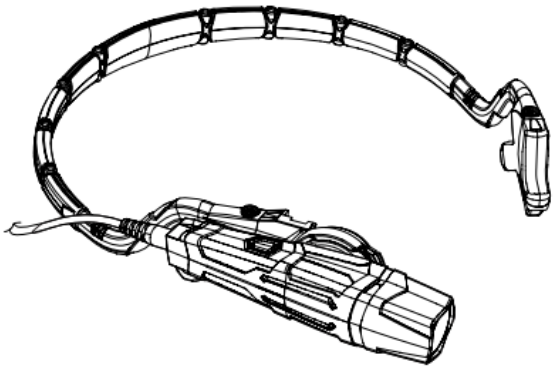
Axon Flex Camera Mounts

Oakley Eyewear Mount

The Axon Flex camera can be attached to Oakley Flak Jacket® glasses. With this system, the camera is designed to directly capture your point of view because it is mounted at eye level.



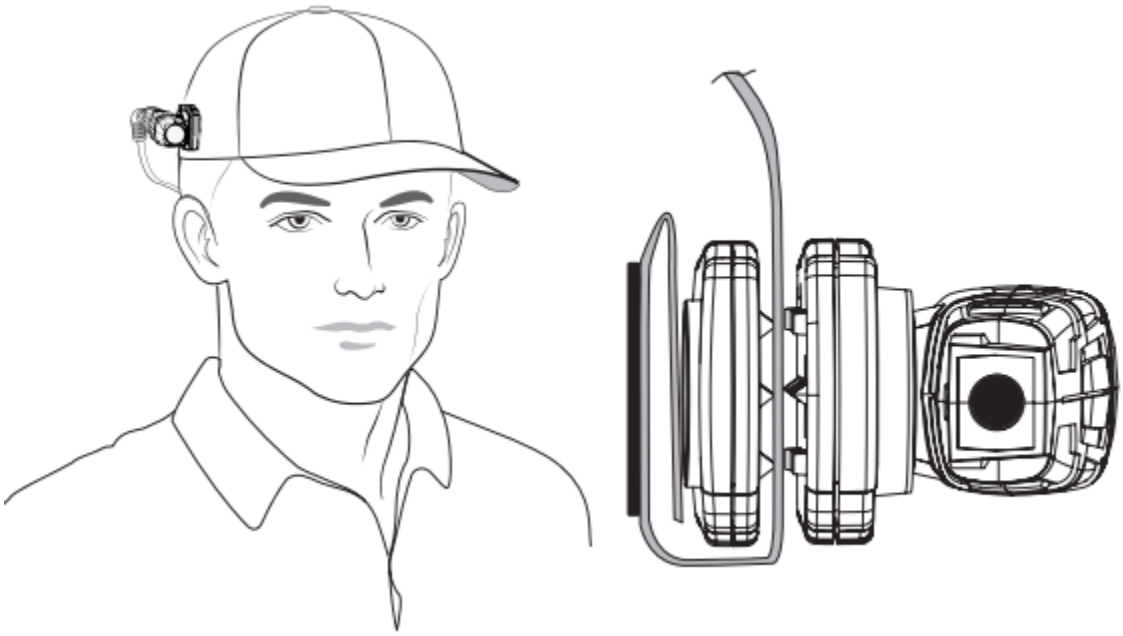
Low Rider Headband



Designed for use with the Flex system, the Low Rider headband provides a comfortable frame to wear the camera on your head. As with the Oakley eyewear mount, the Low Rider headband places the camera at your eye level, and is designed to capture your perspective of the incident.

Hat Mount

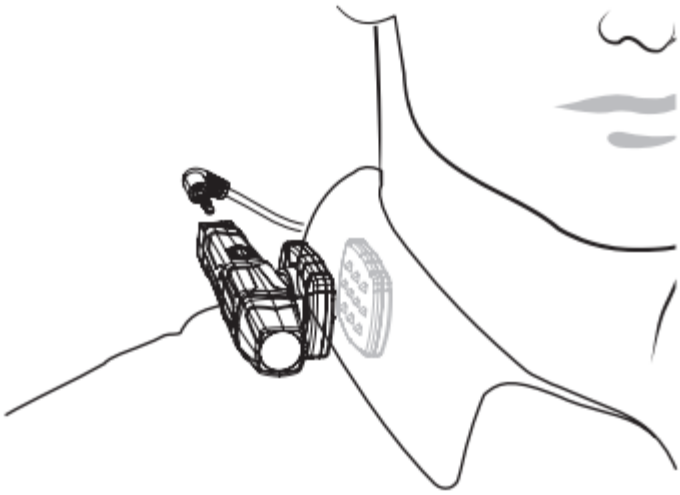
The camera can be worn with headgear, including baseball caps. One magnetic clip is placed on the inside of the baseball cap, while the rest of the assembly goes on the outside, held in place by magnetic attraction.



Collar Mount

The universal magnetic clip is compatible with most uniform shirt collars.

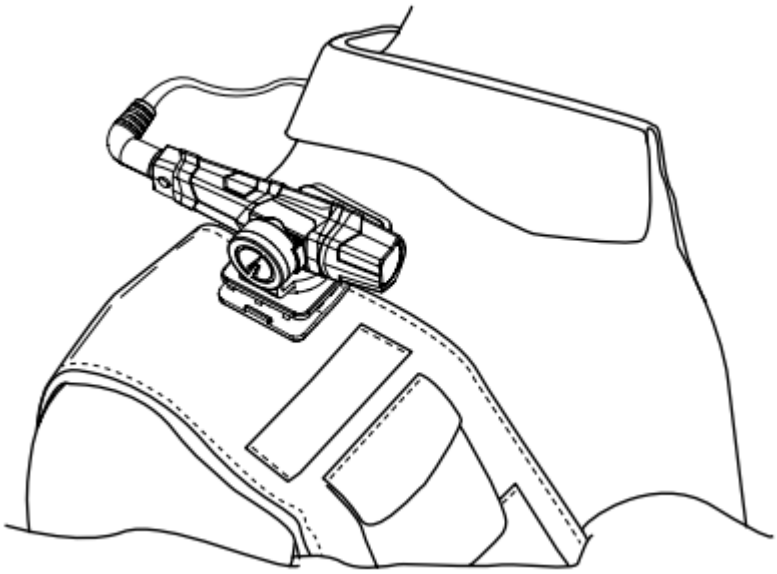
A collar support bar also is available. It consists of an inside magnetic clip combined with a metal band designed to wrap underneath the collar, towards the back of the neck.



Epaulette Mount

If your uniform shirt has epaulettes, you can attach the Axon Flex camera to them. The drawing shows the camera worn above the epaulette, but the mount can be positioned to place the camera below the epaulette, if desired.

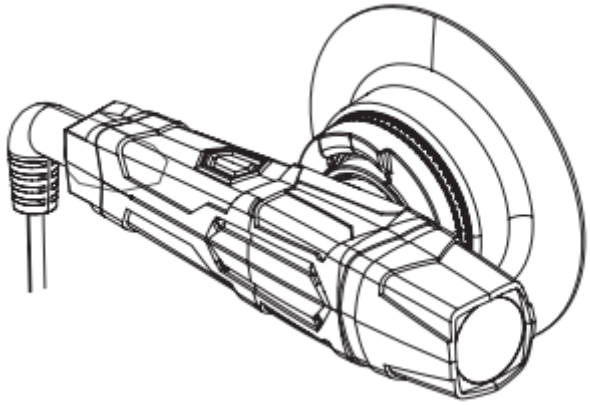
The epaulette mount also works with equipment vests.



Adhesive Mount

The adhesive mount allows the camera to attach to most smooth, hard surfaces, like helmets.

We also have two additional helmet mounts, built specifically for use with the Shoei and HJC helmet brands.



SWAT Mounts

SWAT officers know better than anyone that body-worn cameras are at risk of getting knocked off in highly physical situations. That's why we've developed a Picatinny rail mount that secures Axon Flex to the SWAT officer's helmet and holds true through the most critical incidents. With this new mounting option, the Axon Flex controller and camera both attach to the SWAT helmet, keeping the system consolidated on the helmet and avoiding any interference with other gear.

3.11.3.15 Camera should allow for on scene (in the field) viewing? If so, describe the ability to playback or view video.

Yes. Axon View is a free mobile application that wirelessly connects with your Axon camera to provide instant playback of unfolding events from the field, in the field. You can use the app's live display to ensure your camera is well-placed, and the playback function helps eliminate the "he said, she said" on the spot.

Turns Routine Video into Valuable Evidence

Available for both Android and iOS devices, Axon View automatically maps video with GPS data and allows real-time tagging of metadata from your phone. Before you set foot in the office, your video is filed into the correct retention schedule automatically. When you need it, evidence can be accessed quickly with a simple keyword search.

- ***Pairs Axon cameras with Android or iOS devices***
- ***Instant replay prevents frivolous dispute of recorded events***
- ***Live video streaming assists with optimal camera placement***
- ***GPS tagging maps video evidence automatically***
- ***Real-time metadata input enables easy searching and accurate retention***

Alternatively, using Evidence Sync, TASER's Microsoft Windows application, the Axon camera can be connected to an in-car MDT or MDC via USB cable. Features are similar to Axon View, except that when video are played back over Axon View, they are played at 5 frames per second, Evidence Sync will playback video at the source frame rate of 30 frames per second.

3.11.3.16 Camera shall provide feedback to user when activated, either via a visual indicator or audible tone.

Yes. The Axon Body 2 provides audible (beeps), visual (LEDs), and/or haptic (vibration) feedback to clearly indicate the current mode of operation.

Visual Notifications

The Operation LED is located on the top of the Axon Body 2 so the officer can easily see the status. A blinking red LED indicates recording. Pressing the Battery button will momentarily light both the Operation LED and the Battery LED, displaying the current operating mode.

The system has two operating modes, Buffering and Event mode. Buffering mode is the default mode of operation (when the unit is turned on) and is activated seconds after turning on the device. The Axon Body 2 is in Event mode as soon as an officer double-taps the Event button to initiate the recording of an event. By default, the previous 30 seconds captured in Buffering mode will also be saved (without audio) as the beginning of the event. Your agency can extend the Buffering mode's duration to two minutes total. The Axon Body 2 can also be configured to record sound as well as video in Buffering mode.

To initiate event recording, simply tap the large concave button on the front of the camera two times. While the device is easily activated when worn in a shirt pocket or housed in a case, it is still protected against unintentional triggering. To end the recording, simply hold down the button for three seconds. The activation method was designed based on extensive customer feedback.

Audible Notifications

To clearly indicate activation of the device to the user, the camera can also be configured to emit audible (beeps) and/or haptic (vibration) feedback. This ensures that the user knows the status of the device without having to look at it, which improves user experience and officer safety.

Operating Mode	*Audio Notification*	*Haptic Feedback (Vibration)*
Powering on or off	*One beep*	*Once*
Recording an event	*Two beeps (every two minutes)*	*Twice (every 2 minutes)*
Press the battery button while the camera is recording	*Two beeps*	*Twice*
The device is ending an event and returning to Buffering mode	*One long beep*	*Once, long duration*
The battery is at 20 percent capacity or lower	*Four quick beeps (every 20 seconds)*	*Four times, quickly, every five minutes*

Operating Mode	*Audio Notification*	*Haptic Feedback (Vibration)*
The camera memory is full	***Three beeps. The camera will not start recording.***	***Three times***

Automatic Hands Free Activation

Axon cameras are compatible with Axon Signal technology, a feature unique to TASER. Auto-activation of camera recording is initiated by a variety of pre-determined "triggers" (blue-lights, TASER CEW activation, etc.). This eliminates the risk of an officer forgetting to turn on his camera due to the stress of the incident.

3.11.3.17 Camera shall have the ability to be set to stealth mode while in the field.

Yes. For some situations, an officer may wish to turn off the lights on the Axon Body 2. You can turn off the lights through the Evidence Sync software application or by using the Battery button.

To turn the lights off using the Battery button:

- ***Press and hold the Battery button for 10 seconds.***

To turn the lights back on:

- ***Press and hold the Battery button for 10 seconds.***

To use Evidence Sync:

1. ***Connect the Axon Body 2 camera to the Evidence Sync application.***
2. ***Select the device settings.***
3. ***Select the option to turn off the device LEDs.***
   - ***The Operation LED flashes red, yellow, and then green before shutting down the lights.***
   - ***Pressing the Battery button will momentarily light both the Operation LED and the Battery LED, displaying the current operating mode and battery level.***

To turn the lights back on:

1. ***Connect the Axon Body 2 camera to the Evidence Sync application.***
2. ***Select the device settings.***
3. ***Select the option to turn on the device LEDs.***

3.11.3.18 Camera must have an indicator that shows current operating mode.

Yes. The Axon Body 2 provides a clear visual indication the device is recording in the form of an LED light, located on the top of the unit.

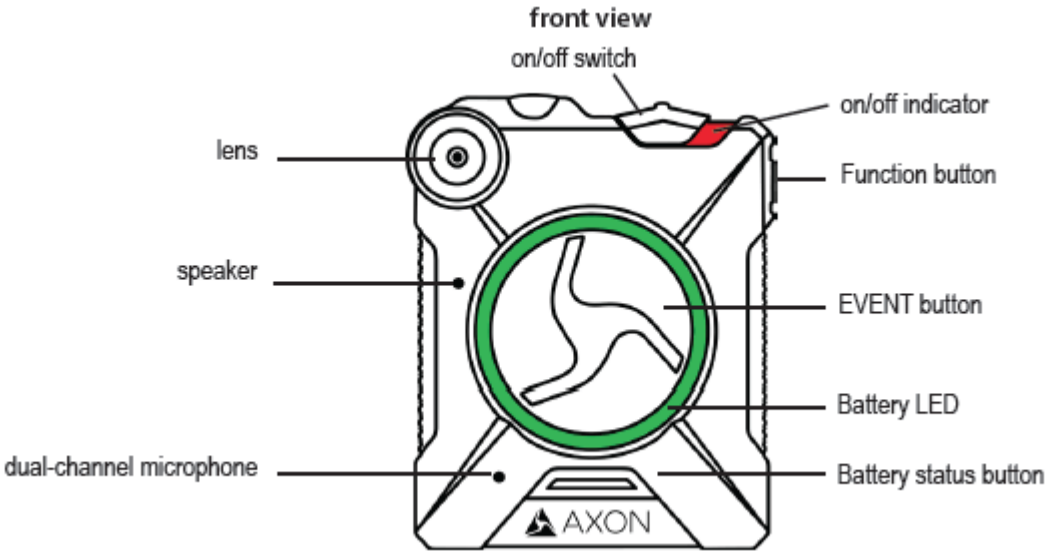
While recording, the LED will blink red to clearly indicate that the device is recording; the device's LED blinks green, the camera is in buffering mode.

Axon Body 2 Operating Mode	*Operation LED*
Recording ***Recovering interrupted video****	***Blinking Red***
Buffering	***Blinking Green***
Booting Up ***Error state*****	***Solid Red***

**** When the Function LED also is blinking red.***
***** When the Function LED also is solid red.***

Charging Mode

When you place an Axon Body 2 camera in the Axon Dock, the device will begin to charge.
The Battery LED around the EVENT button will light up and indicate the battery's charging status.

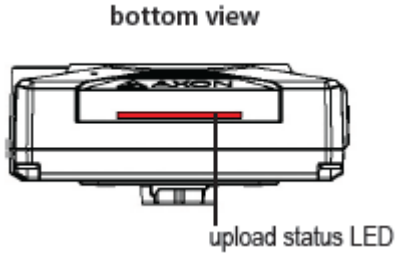


Battery Status	*Battery LED (Around Event Button)*
Battery capacity is 41-100%	***Green***
Battery capacity is 20-40%	***Yellow***
Battery capacity is less than 20%	***Red during operation; flashing red and yellow during charging***
Battery critically low	***Blinking red and yellow***

Upload Mode

Once the Axon Body 2 camera is inserted into the Axon Dock, the LED on the bottom of the camera will display red to start and then change colors to indicate the camera's status in the queue and upload process.

The upload LED is located on the bottom of the Axon Body 2 camera, which will be upright when it is inserted in the bay. The camera displays a green upload status LED before removing it from the dock.



Upload Status LED	
System Status	***LED Indication (on bottom of camera)***
Initial connection (momentary)	***Solid red (for 20 seconds or fewer)***
In queue awaiting upload	***Solid yellow***
Uploading data	***Blinking yellow*** ***Do NOT remove the camera from the Axon Dock***
Device ready (all videos uploaded successfully) and fully charged	***Solid green***
Device not assigned, agency mismatch, camera set in the offline mode, or device error	***Blinking red***
Uploading data	***Blinking yellow – DO NOT remove the camera from the Axon Dock***
Firmware update, internal battery charging, extremely low battery, or memory full	***Blinking red and yellow – DO NOT remove the camera from the Axon Dock***
Transfer error, device re-trying to transfer	***Blinking green and yellow***
Network error	***Blinking red, yellow, and then green (cycling all colors)***

When the video is successfully uploaded to Evidence.com and the battery is fully charged, both the Battery LED and Upload Status LED will be green.

3.11.3.19 If the camera offers night vision enhancement, the State shall have the ability to enable or disable it.

The Axon Body 2 has "Retina Low-Light" Imaging Technology of ≤ 0.1 lux. The human eye has a lux rating of approximately 0.1 lux. By matching that sensitivity, the camera is able to more accurately capture and portray the experience of the user.

High Quality Optics

In order to achieve outstanding reproduction in low light, cameras can either utilize electronics (amplification) or optics (lenses). Axon cameras utilize high quality lenses. This is superior to amplification, which results in graininess and inaccurate reproduction. The videos offer a more accurate depiction of the officer's experience and provide better evidentiary value.

3.11.3.20 The System should provide automatic indexing functionality of video files and be capable of interfacing with existing computer-aided dispatch (CAD) vendor.

Yes. Axon body-worn cameras can interface with your Agency CAD/RMS system. The solution is provider agnostic, and the printout required for tagging and categorization is queried directly from the database, effectively bypassing the CAD/RMS front-end interface. TASER integrations are an option for any system that has an accessible back-end database (SQL DB, etc.). Often, these reports are already pulled for crime statistics reporting. TASER's solution enables automatic tagging of Axon videos with the correct Incident ID, Category, and Location. Automatic retention is accomplished through categorization mapping. TASER's solution uses a proprietary algorithm written to compare CAD/RMS call start and end times with Axon video recording start and end times by officer identifier. TASER supplies a small integrator application that automatically encrypts the automated database printout, sends to Evidence.com via SSL port 443 and then deletes the file from the local server. Automatic tagging occurs once daily with the ability to tag videos from the previous 72-hours.

3.11.3.21 Cameras shall automatically embed a time/date stamp in the recorded video.

Yes. Video files generated by the Axon are embedded with metadata, or data about data. Every time an Axon video is created, the date and time of the recording is logged as metadata and embedded in the MP4 file. Any time a camera is docked into the Axon Dock or connected to a computer running Evidence Sync, the time is automatically checked and reset.

The dates and timestamps sync with the atomic clocks at the National Institute of Standards and Technology (NIST) and cannot be altered, which protects the chain of custody.

3.11.3.22 Cameras shall prevent users from deleting recorded files without authorization.

Yes. Officers cannot delete, alter or edit the videos stored on their camera. Using Axon View in the field, an officer can update the evidence title, ID and assign a category, however; the integrity of the original data can never be changed.

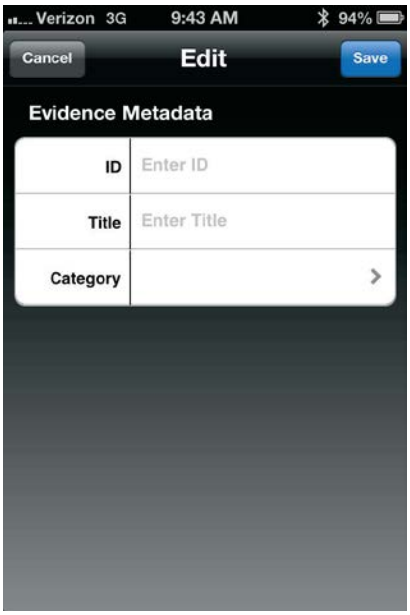
The device uses a non-standard connection to access data on the camera and a granular device-level audit trail will be available in a future release.

Content on the device is only deleted once it has been successfully transferred to the system, and once in the system can only be deleted in accordance with the NHP's retention or Role Based Access Control (RBAC) policies as defined and applied in the categorization of the video content.

A cryptographic SHA hash is automatically created by the camera every time a video is finished recording. This SHA is sent to the application to verify the integrity of the file and is used for auditing purposes. The hash can be used to demonstrate that the recording has not been modified, down to the last bit.

3.11.3.23 Camera should have a method for adding desired metadata to video in the field prior to upload.

Yes. Metadata can be added to Axon video files from the field in the following ways prior to upload to Evidence.com.

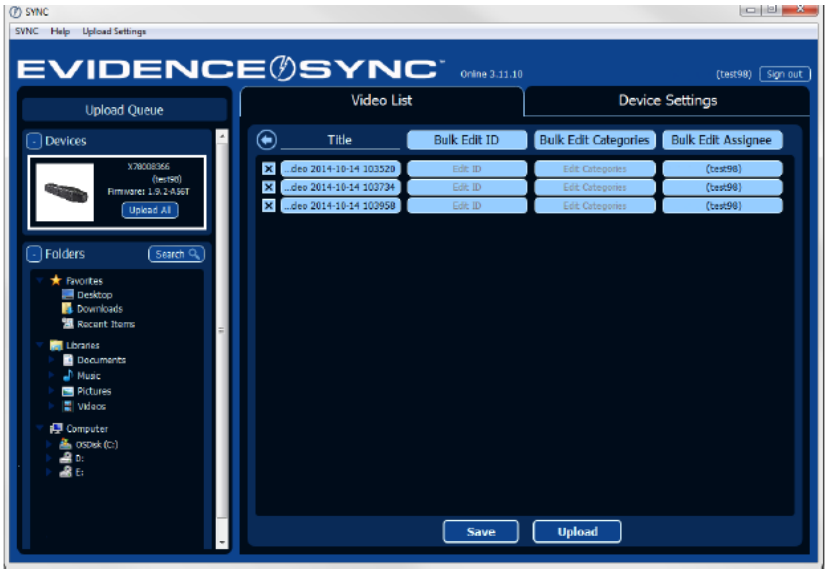


1. ***Pairing an Axon camera to a smart device via a Bluetooth connection and adding tags using the Axon View application.***

   GPS markers are automatically added to videos captured with the Axon when paired to a smart device with GPS capabilities.

   Evidence.com allows for the following indexing fields using Axon View:

   - ***ID – Case ID of incident***
   - ***Title – Titles are defaulted to the date and time of the video capture "Flex Video 2012-10-13 1447." This field can be updated by the user at the time of capture to display a more specific title i.e. "Boat Crash at Lake of the Ozarks."***
   - ***Category – Allows searching for any category type or to specify any category added by the Agency.***



2. ***Connecting an Axon camera via USB to an in-car computer (i.e., MDT, MDC) using the Evidence Sync desktop application.***

   - ***Adding Categories to Records with Evidence Sync***
     1. ***Using Evidence Sync, you can add information to each video, one by one, or you can add information to multiple records at once.***
     2. ***If you want to update the files in bulk, you have several options:***
        - ***Replace the system-generated title with a new one.***
        - ***Apply an appropriate ID for a video by typing it in the Edit ID box. If appropriate, you can add the same ID to all videos.***
        - ***Add your agency's case categories by selecting the appropriate categories from the drop-down menu.***
        - ***If you need to change the person assigned to the videos, type the appropriate ID in the boxes.***

3. ***Integrating Evidence.com with an existing CAD/RMS system, automatically tagging video based on this data, eliminating need to manually to add metadata.***

Evidence.com provides dependable, logical integration from an agency's CAD system (or CAD plus RMS systems) to Evidence.com. With integration, Evidence.com programmatically applies metadata exported from your CAD system to video-evidence files in Evidence.com. Evidence.com can accurate apply ID, retention category, and event location information from event records to evidence files.

With TASER's integration solution, officers no longer have to spend valuable time entering this data after each incident, and supervisors no longer have to search extensively for untagged or incorrectly tagged videos.

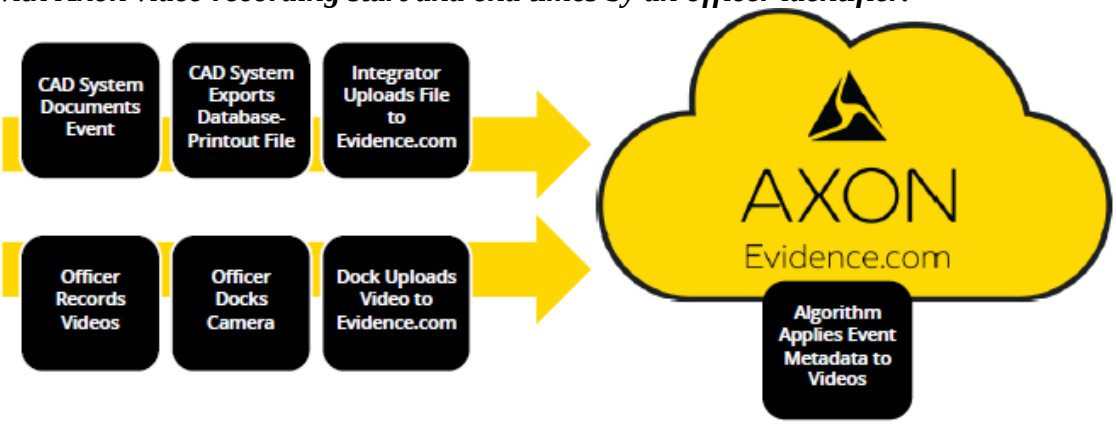
Greater Accuracy

- ***Improves data accuracy of information***
- ***Correlates your RMS or CAD events with Axon videos adds Incident ID, Category and Location to videos automatically***
- ***Avoids the misspellings and incomplete info of manual entry***
- ***Makes searching and retrieving evidence easier later***

Increased Efficiency

- ***Automates metadata entry for every recording***
- ***Requires minimal involvement from the NHP's IT staff***
- ***Works with any system without involving RMS vendors***
- ***Enables supervisors to manage evidence more effectively***
- ***Ensures evidence receives the appropriate automatic retention period***

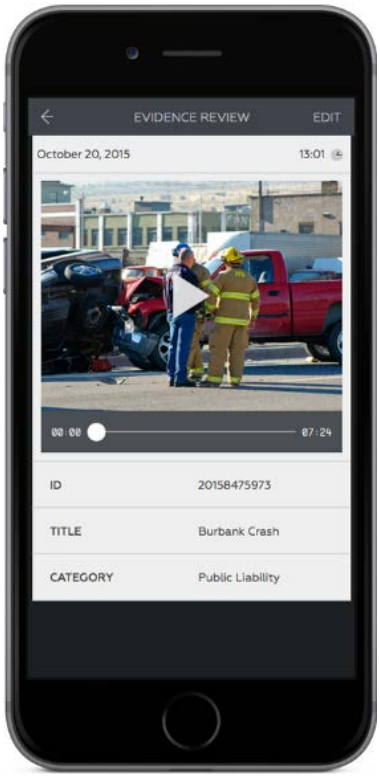
TASER's solution uses a proprietary algorithm written to compare CAD/RMS call start and end times with Axon video recording start and end times by an officer identifier.



TASER supplies a small integrator application that automatically encrypts the automated database printout, sends to Evidence.com via SSL port 443 and then deletes the file from the local server. Automatic tagging occurs once daily with the ability to tag videos from the previous 72 hours.

3.11.3.24 Officers should have the ability to playback or view video in the field on mobile cameras and/or MDC's (Panasonic FZ-G1 Tablet) wirelessly (i.e. Bluetooth).

Yes. Officers can playback or view video on the field on mobile devices and/or MDC's.



Axon View is a free mobile application that wirelessly connects with your Axon camera to provide instant playback of unfolding events from the field, in the field. You can use the app's live display to ensure your camera is well-placed, and the playback function helps eliminate the "he said, she said" on the spot.

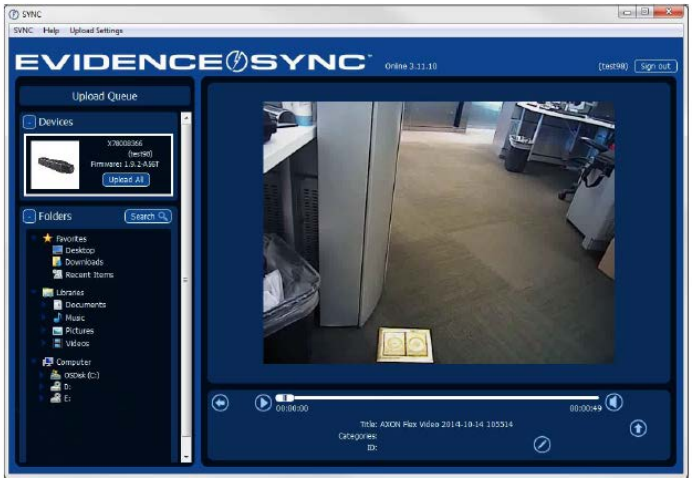
Available for both Android and iOS devices (including tablets, smartphones, etc.), Axon View automatically maps video with GPS data and allows real-time tagging of metadata from your phone. Before you set foot in the office, your video is filed into the correct retention schedule automatically. When you need it, evidence can be accessed quickly with a simple keyword search.

- ***Pairs Axon cameras with Android or iOS devices***
- ***Instant replay prevents frivolous dispute of recorded events***
- ***Live video streaming assists with optimal camera placement***
- ***GPS tagging maps video evidence automatically***
- ***Real-time metadata input enables easy searching and accurate retention.***

Evidence Sync

From a computer or your MDT or MDC, you can upload video to Evidence.com via Evidence Sync (with an internet connection).

- ***Previewing TASER Axon Videos with Evidence Sync***
  1. ***Connect the camera to your computer with the 2.5 mm to USB cable.***
  2. ***Type your login information and click Sign in.***
  3. ***Double-click the video you want to watch, and then click play.***



3.11.3.25 Camera shall have a pre-event record feature (BWC should capture at least thirty (30) seconds of video prior to officer initiating the recording). Adjustable times are preferable.

Yes. The Axon Body 2's pre-event buffer is configurable from 0-120 seconds (in 30 second increments) and features configurable on/off audio capture to record the evidence your agency's needs. Camera will export in a standard, open format, such that it can be replayed in freely available software without processing or conversion. Proprietary data formats shall not be accepted.

3.11.3.26 The vendor must offer a multi-dock station capable of uploading digital evidence from multiple cameras simultaneously and have the capability to upload video via Wi-Fi and/or cellular LTE connectivity. If via cellular, product should be compatible with Fenny Wireless Skyus X modem.

Yes. Perhaps the most exciting feature of the Axon workflow is the ease with which files are uploaded to Evidence.com, TASER's cloud-based storage solution. At the end of his or her shift, the officer simply places his Axon camera in his agency's Axon Dock, and goes home. That's it. Not only does the dock allow for easy upload, but it also charges the device and upgrades the device firmware version without the need for a computer. The Axon Dock utilizes a RJ45 Ethernet connection.

3.11.3.27 The multi-dock station must charge the camera batteries, securely transfer files without loss of quality or metadata, and delete the files from the camera once transferred to the evidence management system.

Yes. Each Axon Dock can charge up to six (6) Axon units simultaneously. Restrictions on uploading data from cameras is only limited by the bandwidth available to the Agency. Axon videos are downloaded automatically once the camera is docked in the Axon Dock. Once in the dock, an encrypted 256-bit AES SSL session is established with the local storage device; videos are then sorted and uploaded.

As a video is being downloaded, it is broken into small blocks of approximately 2-3 megabytes in size. Prior to upload the block is hashed using the SHA algorithm to generate a unique fingerprint or checksum. The block is then downloaded and upon receipt the block is hashed again using the SHA algorithm, if an identical checksum is generated then the file's fingerprints match and the block is unaltered from its original state on the Axon.

The dock uploads one file from one camera at a time, then moves on to the next file on that camera. Once the first camera's files have all been transported to Evidence.com, the dock begins uploading the next camera's files.

The block upload process is repeated until the entire MP4 is transferred. Using the same method that was used to validate the blocks, a contiguous checksum of the entire file will be evaluated to ensure that the MP4 file has been uploaded successfully and identical to when it was recorded. Once Evidence.com confirms receipt, the video is deleted from the camera and the upload process moves to the next file.

3.11.3.28 The multi-dock station should not require a department computer to operate, connect or interface with the Internet (e.g. the multi-dock station should be a standalone device that connects to the cloud storage solution or server via an Ethernet connection).

Yes. Axon Docks upload via Ethernet connectivity to the local network.

3.11.3.29 The camera should not cause electromagnetic interference with nearby airwave radios (and other electronic equipment and radio communication systems).

Yes. Axon cameras will not cause nor be affected by electromagnetic interference. Axon cameras are designed to ensure that the device neither affects nor is affected by external sources of electromagnetic interference (radio, CEWs, etc.). This is accomplished through careful consideration throughout the design of the product (PCBA construction, electrical layer stack-up, trace length / impedance) as well as through shielding of critical components (sealed connecters, microphone, speaker holes, etc.).

Axon cameras are CE & Federal Communications Commission (FCC) certified and conform to the electromagnetic compatibility (EMC), electrostatic discharge (ESD), and product safety requirements of the European Community.

<u>Use with TASER Smart Weapons</u>

Axon cameras have the unique distinction of being developed to operate alongside TASER conducted electrical weapons (CEWs), not interfere with them.
CEWs function by using transformers to step up voltage, resulting in a large amount of electromagnetic interference. Axon cameras are specifically designed to be unaffected by this level of electromagnetic interference to ensure any incident where the device is used is captured. Considering that some of the cameras may be used by officers carrying CEWs - it is critical that the video not be corrupted by the deployment of a CEW. Firing logs from TASER smart weapons can also be ingested into Evidence.com alongside body worn camera video.

3.11.3.30 Loss of power to the camera must not cause data to be lost/corrupted.

Yes. Loss of power will not cause data to be lost or corrupted. The Axon Body 2 maintains a suitable amount of "backup" power to ensure proper shutdown. For example, if the device were to lose power, the device would properly close out all incident files to ensure that no data was lost or corrupted. In the event of sudden and complete power loss, the device will perform a video recovery operation during the next boot process and close out the incident file.

The interrupted recording file, as well as any previously recorded files, will be available once power has been restored.

3.11.3.31 Cameras will be ruggedized. Cameras shall be able to survive a six-foot drop test. Cameras shall be able to operate at minimum temperature of -12 degrees Fahrenheit and a maximum temperature of 130 degrees Fahrenheit.

Yes. The Axon Body 2 is extremely ruggedized, shock-resistant, and water-resistant with a rating of IEC 60529 IP67.

These levels of ingress protection (IP) provide users with longer-lasting cameras with fewer failures and overall lower total cost of ownership. The device features complete protection against dust/debris and protection against water immersion at 1 meter for 30 minutes. The Axon Body 2 is also tested to and passes MIL-STD-810G Test Methods (vibration, salt fog, and blowing dust resistance, etc.).

The device is impact certified from a height of 6 feet. The most common damage to BWC devices comes as a result of a drop. The Axon Body 2 protects against damage resulting from this common occurrence, providing lower costs associated with damage and downtime. The camera's magnetic mount is strong enough to hold the camera in place while running or fighting.

The Axon Body 2 is unique in that it was designed with robustness and shock resistance in mind. The device is designed as a sealed compartment with no moving parts or fragile electronics (LCD screen). By moving articulation to the mount, the camera design is more rugged as compared to cameras with integral moving parts.

The Axon's ability to withstand high temperatures may prove valuable during particularly warm days when storing the video device in a vehicle or when responding to a scene that has high temperatures such as a residential fire, helping keep crucial evidence safe and available after extreme events and conditions.

Operating Temperature Range
Axon body-worn cameras have an operating temperature of −4 °F to 122 °F [−20 °C to 50 °C].

Storage Temperatures
Axon body-worn cameras have a storage temperature of −4 °F to 95 °F [−20 °C to 35 °C]. Long-term storage should be in a climate-controlled environment, less than 1 month at the highest temperature.

Charging Temperature Range
Axon body-worn cameras have a charging temperature range of 41 °F to 95 °F [5 °C to 35 °C].

3.11.3.32 Vendor will state camera's Ingress Protection (IP) rating. The State prefers an IP rating of IP67.

Yes. The Axon Body 2 is extremely ruggedized, shock-resistant, and water-resistant with a rating of IEC 60529 IP67.

These levels of ingress protection (IP) provide users with longer-lasting cameras with fewer failures and overall lower total cost of ownership. The device features complete protection against dust/debris and protection against water immersion at 1 meter for 30 minutes. The Axon Body 2 is also tested to and passes MIL-STD-810G Test Methods (vibration, salt fog, and blowing dust resistance, etc.).

3.11.3.33 Describe what features devices have in place to prevent accidental activations of camera by the user (without the need for accessories or alteration of equipment by user).

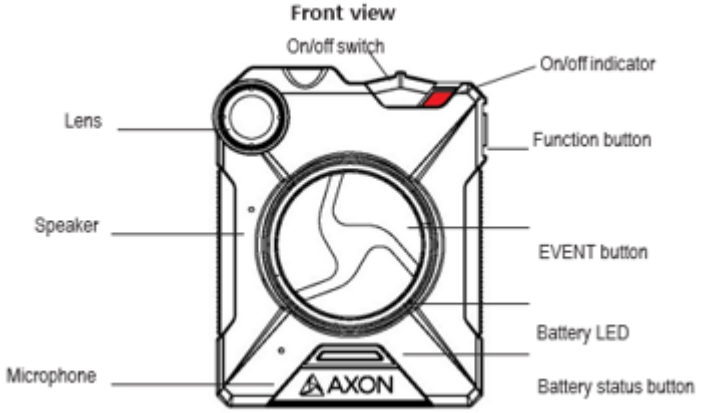
Yes. A complicated activation mechanism is cumbersome in the field and can impede more important duties, especially considering officers often have to start a recording at a moment's notice.

The Axon Body 2 was designed specifically for use by law enforcement in tactical policing situations. Activation of event recording is simple and accessible, so officers can operate the device in a high-stress situation. Recordings are initiated with a single "Event Button" located on the front of the device, so an officer can easily reach it with one hand.

The Axon Body 2 camera has two operating modes:

3. **BUFFERING (turning on the camera and starting pre-event buffering)**
4. **EVENT (event recording)**

To initiate Buffering Mode (turn the camera on) Move the ON/OFF switch on the camera to the ON position. The raised on/off switch is strong enough to prevent accidentally powering the device down, yet can still be switched on if an officer is wearing gloves.



To initiate Event Recording Mode, simply tap the large concave button on the front of the camera two times. While the device is easily activated when worn in a shirt pocket or housed in a case, it is still protected against unintentional event triggering. To end the recording, simply hold down the button for three seconds.

3.11.3.34 Vendor shall define the required time for automated indexing (specific time frame after upload of video evidence) and any expected error rate percentage upon indexing, if applicable.

As soon as it is available the Evidence.com the information is available for indexing.

3.11.3.35 The vendor must state the transfer rate of video from the multi-dock station to the cloud in sixty or thirty-minute increments. Vendors shall break down transfer rates by video quality (i.e. Hi Def).

480p 1.6GB/hr | 720p 2.7GB/Hr | 1080p 5.4GB/Hr. The transfer from the multi-dock transfers at 10Mbps however the rate of transfers between itself and the cloud is dependent upon the NHP's infrastructure and internet upload speed.

3.11.3.36 Describe device wireless activation features (e.g. device is automatically activated with the activation of patrol vehicle's light bar), if applicable.

Yes. Axon Signal is a system for secure activation of Axon camera devices. It is protocol, which operates over Bluetooth Low Energy. The effective range of Axon Signal is 30ft (~10 meters). The Axon Signal protocol is implemented by all Axon cameras, by the Axon Signal box and by an upcoming battery module for TASER conductive electric weapons.

Signal can convey specific telemetry messages that describe the state of the environment. Axon cameras capture these messages and store them as metadata within the video. Depending on the specific telemetry contained within the message, Axon cameras can decide to start or stop recording.

Specific activation criteria are listed below:

- ***Binary triggers: on-off triggers for 1 - 24V inputs. These inputs include door switches, light-bar, shotgun/patrol rifle release, brake switches or dedicated on-off switches.***
- ***ECU speed trigger: this input measures the time between speed pulses from the vehicle ECU. The period between pulses is changes in proportion to the vehicle speed. The Signal Box can be configured to match the time between pulses at 60 MPH to provide a highly accurate representation of vehicle speed. On the receiving side, Axon cameras can be configured to activate at a specific speed, such as 90mph.***
- ***Accelerometer: All Axon cameras include an accelerometer and can be configured to activate based on a high-G event, such as that of a crash.***
- ***MDT GPS: Should the MDT laptop or tablet contain a GPS receiver, the solution can utilize that source of GPS data. This data is used to store location and vehicle speed data within the video files.***
- ***Mobile Application: mobile apps can send activation events. These events will allow future functionality such as real-time CAD activation where an officers cameras are activated as soon as they are assigned to a call.***
- ***Another Wearer's Axon Camera: Axon cameras can be configured to broadcast Signal messages when activated. Thus Fleet cameras will activate when a nearby Axon Body 2 begins recording.***
- ***TASER CEW: TASER is producing a retrofit battery for existing TASER weapons. This battery will activate Axon cameras when the CEW safety is disabled.***
- ***External GPS: Axon Signal will accept a NMEA-format serial input from external GPS devices, such as those used for AVL systems. This GPS data can be added to the video as the definitive source of GPS data. This functionality will be enabled by the end of the 2016.***

3.11.4 Maintenance & Repairs (Hardware)

3.11.4.1 Vendor shall propose and provide a detailed description of the maintenance services that are available once the one-year warranty has expired.

TASER warrants that its law enforcement hardware products are free from defects in workmanship and materials for a period of one (1) year from the date of receipt. TASER-Manufactured Accessories are covered under a limited 90-day warranty from the date of receipt. Non-TASER manufactured accessories are covered under the manufacturer's warranty.

Extended Warranty

There are extended warranties available, which will cover the hardware for 3 years total (1 year manufacturer's warranty plus 2 years extended).

The TASER Assurance Plan (TAP)

The TASER Assurance Plan (TAP) includes the extended warranty coverage described above, as well as spare products and upgraded models at the end of the TAP Term. The TASER Assurance Plan (TAP) is bundled into the purchase price of the Ultimate and Unlimited Plan Evidence.com licenses. The TAP includes Axon camera upgrades every 2.5 years, TASER's extended warranty and spare cameras.

The TASER Assurance Plan (TAP) includes the extended warranty coverage described in the current hardware warranty, as well as spare products and upgraded models at the end of the TAP Term. TAP does not apply to software or services offered for, by, on, or through the TASER.com or Evidence.com websites. You may not have both an optional extended warranty and TAP on Axon products.

Software Upgrades and Updates
The latest product features and enhancements are included as part of your investment in Evidence.com. Software is updated regularly throughout the year, and these updates are included in the price of your software licenses.

Please see the attached Master Services and Purchasing Agreement, which outlines the full terms and conditions of the standard manufacturer warranty, extended warranty and TASER Assurance Plan.

Repairs
The Return Material Authorization (RMA) department is located at the TASER International Headquarters in Scottsdale, Arizona, USA. The RMA department prioritizes returned products for analysis and/or repair on a First-In-First-Out (FIFO) basis, based on the severity of the complaint (or unless otherwise requested by the agency). The general turn-around-time for a full resolution is less than 14 calendar days from receipt of the returned product.

Agencies are required to submit a request for repair/replacement via the TASER RMA website and are responsible for all shipping costs (unless already agreed upon in advance). Upon receipt of them item(s), the RMA department will conduct a failure analysis investigation to determine the root cause of the issue and repair the item if possible. It is at TASER's sole discretion to repair or replace a device as identified in the original manufacturer warranty and/or the extended warranty policy.

3.11.4.2 Vendor shall provide on-site repair services as required.

Yes. If for any reason a BWC unit cannot be repaired using the standard process outline above.

3.11.5 Video Management System

3.11.5.1 Vendors must be able to provide documentation establishing that their technology has undergone rigorous field testing by an independent and relevant scientific body. This documentation must be provided with the vendor's proposal response.

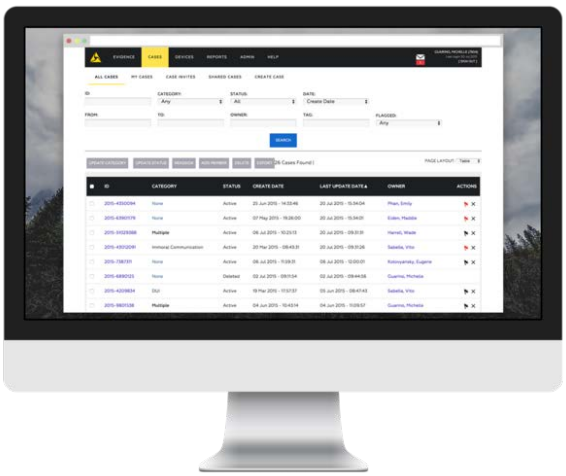
Please see the requested documentation in Tab IX.

3.11.5.2 Vendors shall be willing to provide an expert witness to testify in a court of law, to support court cases utilizing video from their BWC System, at a reasonable fee. Vendors must specify hourly rate for expert witness testimony within ***Attachment H ~ Cost***.

TASER employs experts in technology, who can testify in court for the NHP. TASER will send an expert to testify in court matters free of charge (capped at 100 hours per year of employee time) in relation to the Axon and Evidence.com product lines regarding security and chain of custody matters. NHP must provide TASER with reasonable notice, in no event less than five business days. If NHP requires more than 100 hours per year during the term of the Contract, an hourly rate will be negotiated by the parties and travel expenses will be reimbursed by NHP at GSA per diem rates. Please see Attachment H for costs.

3.11.5.3 VMS shall either be an externally hosted cloud-based data storage solution with the capability of organizing/managing video/digital evidence, server based or consist of a hybrid solution and be accessible via the internet to multiple users simultaneously. The State prefers the Cloud or Hybrid solution.

Yes. Evidence.com is a cloud-hosted digital evidence management solution provided as a service (SaaS) application. It is horizontally scalable and can elastically adapt to accommodate any traffic volumes. Internally, the solution uses a service oriented architecture where functionality is provided by discrete compassable services that can run on one or many servers. This allows individual components to scale to handle changes in traffic volumes.



The application is designed to support uploads from multiple users, devices, and locations, simultaneously from thousands of agencies across the United States. It is also possible for concurrent users to access the same video at the same time.

A SCALABLE SOLUTION

As the sources of digital evidence expand, storage alone is not enough to keep track of the body-worn camera videos, photos, audio recordings, and other data that is overwhelming agency servers and systems.

Evidence.com is a robust end-to-end solution that allows agencies not only to store all that data, but it also enables new workflows for managing and sharing that data securely, from anywhere.

Officers and command staff can upload content from Axon and TASER devices or other systems easily, manage it simply with search and retrieval features, and then collaborate effortlessly with prosecutors and other partners by using powerful sharing features. When storage needs increase, the cloud-based system allows agencies to scale instantly and cost-effectively.

3.11.5.4 VMS shall allow for remote access with complete functionality (review, enter metadata and send video) with NHP mobile devices and/or computers.

Yes. Users can access Evidence.com, TASER's web-based evidence management interface, from any supported internet browser. This is a standard feature of Evidence.comand requires no configuration.

3.11.5.5 VMS shall provide an automatic audit trail for when files and videos are accessed.

Yes. TASER's complete on-officer video and evidence management systems safeguards against a break in the chain of custody. Evidence.com automatically logs a detailed Evidence Audit Trail for every piece of digital evidence and of anything that happens to that video or its metadata. The log can be used to determine a chain of custody that surpasses chain of custody regulations.

<u>Evidence Audit Trail</u>
The detailed Evidence Audit Trail can be used to determine compliance with chain of custody regulations. All content uploaded to Evidence.com is paired with an audit trail indicating every action applied to that evidence and its metadata. Information such as viewed by, downloaded by, and deleted by, is all included in the audit trail, in addition to the source IP Address of the person who made the change. All audit trails can be exported to a PDF document.

To ensure a robust chain of custody, evidence can be verified for authenticity by matching the SHA hash of original file ingested in Evidence.com with the copy. The original data associated with a video is never changed. All modifications are handled by creating new, derivative files. Detailed audit logs track all evidence access.

<u>User Audit Trail</u>
The User Audit Trail shows many of the actions taken by a user in addition to changes to the user's account. It does not show activities related to devices, evidence, or cases.

User Audit Trails are available in the following formats.

1. ***PDF format — Well suited for use in court.***
2. ***Comma-separated values (CSV) format — Supported by spreadsheet applications such as Microsoft Excel and helpful for simplifying reporting and integration with other systems.***

The Evidence.com auditing functionality provides the source IP Address of all actions. Location can be associated with uploaded content, and can be viewed on Evidence.com. In addition to evidence-related user actions, the User Audit Trail provides the following information:

- ***Failed login attempts will be entered into the user's individual audit trail and show the IP address.***
- ***When a user is locked out of their account due to multiple failed login attempts the user's audit trail will show the IP address of the computer that attempted logging in.***
- ***When a user's password has been reset or their account has been unlocked the audit trail will show the username, first and last name, and badge ID of user who has taken that respective action.***

Evidence-related user actions that appear in user audit trails include the following:
- ***View evidence***
- ***Watch video evidence***
- ***Initiate evidence deletion***
- ***Restore deleted evidence***
- ***Upload evidence***
- ***Add or edit evidence title***
- ***Add or edit evidence ID***

- ***Add or edit categories assigned to evidence***
- ***Add or edit evidence location***
- ***Edit evidence recorded date and time***
- ***Extend evidence retention period***
- ***Flag or un-flag evidence***
- ***Share evidence internally (with users in your Evidence.com agency)***
- ***Share evidence externally (with users outside your Evidence.com agency)***
- ***Add or edit evidence tags***
- ***Add or edit evidence description***
- ***Add, edit, or remove evidence notes***
- ***Reassign evidence***
- ***Add evidence to a case***
- ***Add a marker***
- ***Download a marker***
- ***Add a video clip***
- ***Add video redaction***

Case-related user actions that appear in user audit trails include the following:

- ***Create case***
- ***Viewed case***
- ***Add evidence to a case***
- ***Remove evidence from a case***
- ***Share case by download link***
- ***Share case with partner agency***
- ***Share case with user in your agency (add member to case)***
- ***Download case***
- ***Add or remove folder***
- ***Add or edit categories assigned to case***
- ***Edit case title***
- ***Add or edit case description***
- ***Add, edit, or delete case notes***
- ***Add or remove case tags***

Sharing Audit Report

The Sharing Audit report exports a list of all user actions related to sharing evidence and cases to a CSV file. You can specify the date range for the report. Included in the report are the following details:

- ***Date and time of the sharing event***
- ***Who initiated the sharing event***
- ***What was shared — evidence or a case***
- ***How was it shared — internal or external to your Evidence.com agency***
- ***The ID of the evidence or case shared***
- ***The recipient of the shared evidence or case***
- ***The permissions shared to the recipient***

A full list of the metadata included in the report is listed below.

- ***Date Time***
- ***Action***

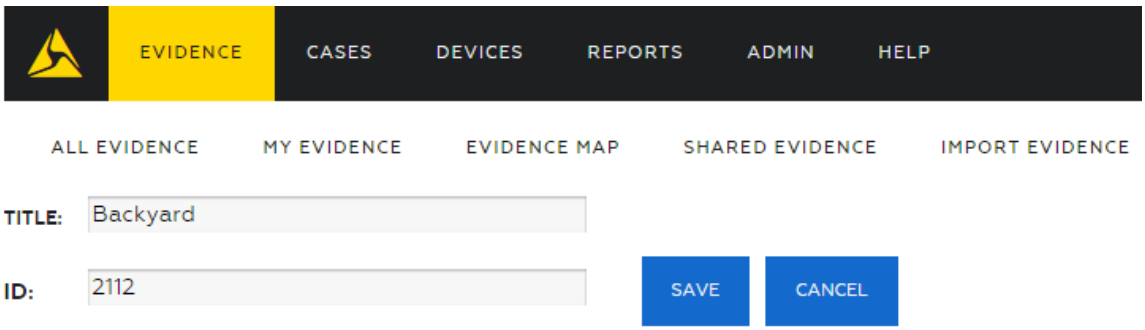
- ***Share Type***
- ***User***
- ***Owner***
- ***Evidence ID***
- ***Evidence Title***
- ***Case ID***
- ***Files Shared***
- ***Recipient email(s)***
- ***Agency***
- ***Duration***
- ***Expiration***
- ***View Permission***
- ***Download Permission***
- ***View Audit Trail Permission***
- ***Post Notes Permission***
- ***Reshare Download Permission***

3.11.5.6 VMS shall allow officers to enter additional metadata to recorded files, such as notes or comments.

Yes. By enabling officers to annotate Axon video with meta-data, Evidence.com turns what was once an overwhelming amount of files and information into a database of highly searchable evidence.

From the View Evidence page on the Evidence.com dashboard users can view and work with evidence listed in search results if any of the following are true:

- ***You own the evidence***
- ***The owner of the evidence has shared it with you***
- ***Your user role allows you to view all evidence***
- ***You are a monitor of a group that the evidence owner is a member of***
- ***You are an administrator***



Once a user has located the file they wish to manage, they can perform the following actions when working with any file type. All actions will be recorded in the evidentiary audit log.

- ***Edit Title and ID***
- ***Add or Remove Tags – Tags are labels that can be applied to evidence. Tags can be added to evidence for easy locating in the future. Evidence searches allow users to filter the search results by tags.***
- ***Edit Location – The specified location for evidence determines where the pin representing the***

evidence appears on evidence maps.

- ***Add, Edit and Delete Notes – Notes can be posted about evidence. In addition to the text of the note, Evidence.com shows the author of the note and the date and time that the note was created and updated.***

On the View Evidence page, the Notes area appears below the evidence and description. If the Also with ID area appears, the Notes area appears below this area.

- ***Edit Description – Descriptions of the evidence can be added or edited.***
- ***Edit Recorded Date and Time***
- ***Download Evidence File – Data can be exported to external media such as CD-ROMS, flash drives, and external hard drives.***
- ***Flag or Un-Flag Evidence – Evidence can be flagged to make it easy to find in the future. Evidence searches allow users to filter the search results by the flag status of evidence.***
- ***Add to or Remove Evidence from a Case – Users can add or remove evidence to one or more cases.***
- ***Reassign Evidence – Users can assign evidence to a user. The user to whom the evidence is assigned becomes the owner of the evidence.***
- ***View Evidence Audit Trail***
- ***Delete Evidence – Users can manually initiate the deletion of an evidence file. Deleted evidence is added to a deletion queue for 7 days. This helps prevent deleting evidence unintentionally.***
- ***Restore Deleted Evidence – If evidence has a status of Queued for Deletion, users can restore the evidence, which removes it from the deletion queue.***
- ***Assign and Un-Assign Categories – For evidence that is not assigned to a case, changing the categories that the evidence is assigned to may change the scheduled deletion date. If the scheduled deletion date has already passed, the evidence will be added to the deletion queue.***
- ***Extend Retention Period – If evidence is scheduled for deletion, users can extend how long the system retains the evidence before adding it to the deletion queue. The period of time that the retention is extended is equal to the length of the retention policy currently in effect for the evidence. The category assigned to the evidence determines the retention policy. If more than one category is assigned to evidence, the longest retention policy is applied.***

For example, if an evidence file is assigned a category with a 30-day retention policy and deletion is scheduled 20 days from today, extending the retention period would reschedule deletion to 50 days from today.

- ***View Evidence with Same ID – If other evidence in an agency has the same ID as the evidence being viewed, the Also with ID area appears below the evidence description. A paginated table of evidence with the same ID shows the title, owner, and upload date of each evidence file.***

3.11.5.7 Solution must support all major digital file types (avi, jpeg, mpeg, etc.).

Yes. Evidence.com provides law enforcement with a robust solution for organizing, classifying, managing, viewing, and archiving all of their digital evidence – not just Axon videos.

Online streaming and preview features supported in Evidence.com for the following file types:

- ***Video: DIVX, TS, 3GP, ASF, AVI, FLV, MOV, MP4, RM, VOB, WMV, F4V, MPEG, MPG***
- ***Image: JPEG, JPG, GIF, PNG, BMP***
- ***Audio: MP3, WAV***

Documents and non-supported digital media types can be uploaded and managed in Evidence.com; however, online preview features are not available for unsupported file types. These file types are typically proprietary formats that require custom players.

These file types can be downloaded from Evidence.com and saved to a local drive, burned to a disc, copied to a USB drive, or saved to a PC with the required player. After selecting files for download, the user receives an email with a download link to a single file containing all of their requested evidence. The system supports the following file types for the download file:

- ***ZIP — The system includes the selected evidence files in a ZIP file.***
- ***ISO — The system includes the selected evidence files in an ISO image, which can be used to create a CD-ROM or DVD.***

NHP can also ingest and store video, photos, files and data from other mediums and group them around larger case files — the most common sense way to manage evidence.

3.11.5.8 VMS shall provide remote viewing of the stored video based on the permissions granted by the System Administrator.

Yes. Each Evidence.com user is assigned a role. Roles determine a user permissions, which control levels of access to features and functions in Evidence.com.

Information access via Evidence.com is controlled through a robust "Access Control System" managed by the Administrator and features comprehensive audit trails.

Access to information is governed by the agency-defined access control system built into Evidence.com. Access is controlled according to:

- ***Pre-defined roles,***
- ***Pre-defined individuals (i.e., who has access to what camera feed),***
- ***User account-specific passwords.***

Administrators assign the roles and actions of all users and create individual user accounts with varying degrees of access, i.e. administrative accounts, basic user accounts, etc. Account administrators can customize the roles and authorization levels of each account user, or what they are permitted to do. This functionality was created to preserve chain of custody and to clarify what each user is permitted to do.

Each Evidence.com user is assigned a role; roles determine user permissions, which control access to features and functions. The following table provides information about each permission supported by Evidence.com.

Permissions Supported by Evidence.com	***Description***
Login Access	
Evidence.com	***Allows a user to log in to their agency's Evidence.com agency.***
Evidence Sync	***Allows a user to log in to Evidence Sync in Online mode.***
Evidence Mobile	***Allows a user to log in to the Axon Capture or Evidence Mobile application.***
User Account	

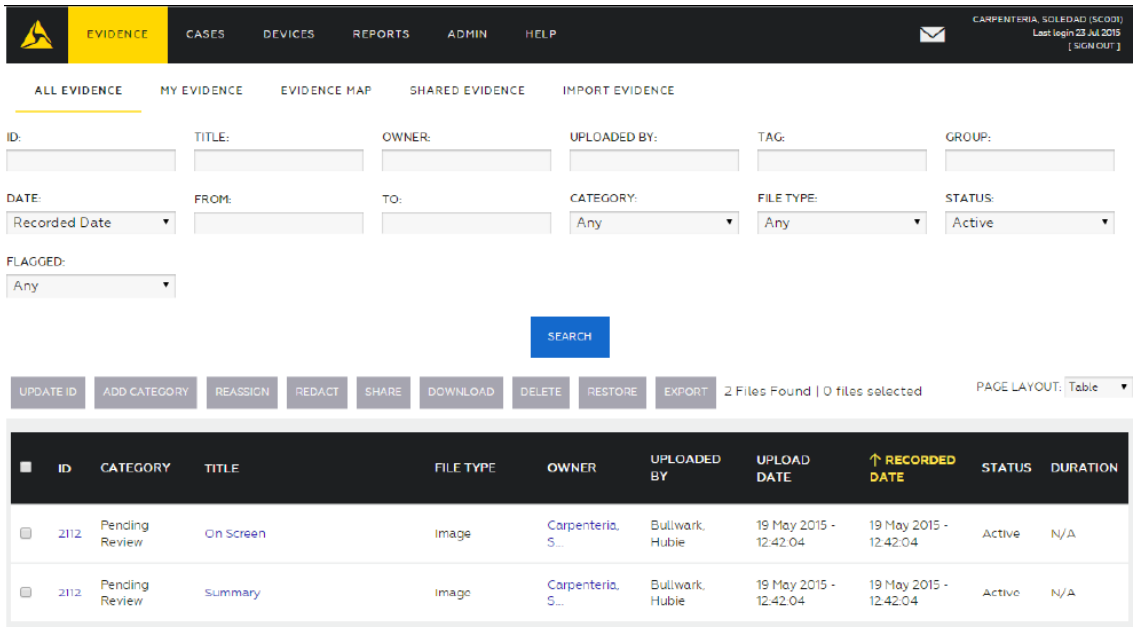
Permissions Supported by Evidence.com	*Description*
Edit Account Information	*Allows a user to change their own account information, including their Name, Badge ID, Phone, Email Address, Password, Security Questions, or Email Settings. If you change the User Administration permission to Allowed, this permission is automatically set to Allowed.*
View & Compose User Messages	*Allows a user to read and send messages to other users.*
Download Sync Software	*Allows a user to download Sync software from their Evidence.com agency.*
Create/Edit Group	*Allows a user to create a group, and edit its monitors and members.*
Group Audit Trail PDF	*Allows a user to view an audit trail of the activities related to a group.*
Admin Access	
Configure Agency Security Settings	*Allows a user to edit the agency's IP Restrictions, authentication method, password configurations, and partner agencies.*
Edit Agency Settings	*Allows a user to configure agency wide settings including Categories and Retention, Video and Camera Settings, Roles and Permissions, and Password Configuration requirements.*
Edit Device Offline & Microphone Settings	*Allows a user to configure the agency-wide settings for the Axon cameras default Microphone Setting and whether or not they can be turned to Offline Mode.*
Device Administration	*Allows a user to reassign all agency devices, change their settings, and upload any CEW logs.*
User Administration	*Allows a user to add, remove and edit the accounts of other users, including their role, personal information, contact information, and reset their credentials (password and security questions).*
Category Administration	*Allows a user to add a Category to the agency's list or edit an existing Category*
Generate Reports	*Allows a user to generate reports.*
Search Access	
User Search	*Allows a user to see what users are in the agency. If disabled the user will be unable to see any evidence or devices assigned to others, assign devices or evidence to others, share evidence or cases, or send messages to others.*
Partner Contact Search	*Allows a user to view members of partner agencies that have been added to your agency's contact list* *Unlocks: Share Externally to Authenticated Users, Share With Partner Agencies*
Evidence Search	*Allows a user to search for all of the Evidence in the agency. Note: the user can only access the Evidence specified under the Evidence Management permissions.*
Device Search	*Allows a user to search for all of the Devices in the agency.*

Permissions Supported by Evidence.com	*Description*
Case Search	*Allows a user to search for all of the Cases in an agency. Note: Their ability to access a Case is determined by the Case Management Permissions.*
Evidence Creation	
Upload External Files	*Allows a user to upload files through Evidence Sync, Axon Capture, Evidence Mobile, and the Import Evidence feature. This does not affect the ability to upload through an ETM or Evidence.com Dock.*
Configure Automatic Upload through Evidence Sync	*Allows a user to configure Automatic Upload through Evidence Sync.*
Evidence Management	
View	*Allows a user to access evidence. Does not include weapon firing logs.*
View CEW Firing Logs	*Allows a user to view weapon firing logs.*
Edit	*Allows a user to change the Title, ID, Flag, Assignment, Category, Tags and Location.*
Add/Remove Pending Review Category	*Allows a user to add or remove the Pending Review Category from a piece of Evidence.*
Redact	*Allows a user to create redactions of video evidence files. This does not alter the original video in any way.*
Reassign	*Allows a user to change the owner of an evidence file.*
Delete Evidence & Edit Date Recorded	*Allows a user to manually initiate the deletion of Evidence before its Category determined date.*
Download	*Allows a user to download Evidence.*
Share	*Allows a user to allow other users to have access to Evidence.*
Share Externally to Authenticated Users	*Allows users to provide individuals outside of your agency with access to evidence. These external users are required to sign in to their Evidence.com account to view the shared evidence, and their actions are shown in your agency's audit logs. If they do not have an Evidence.com account, they can create a free guest account on my.evidence.com.*
Share External Download Links	*Allows users to send an email containing a download link to individuals outside of your agency. This link does not require the recipient to sign in to an Evidence.com account or even to have an Evidence.com account. Only the apparent IP address of the computer downloading the file appears in your agency's audit logs.*
Post Notes	*Allows a user to write messages associated with Evidence.*
Audit Trail PDF	*Allows a user to view and download the record of who has Viewed or Edited Evidence.*
Restricted Category Access	*Allows a user to access Evidence that has been categorized as Restricted Access.*
Case Management	
View	*Allows a user to access a Case*
Edit	*Allows a user to Edit Case ID, Description, Categories, Tags, and Folder Structure.*

Permissions Supported by Evidence.com	*Description*
Reassign	***Allows a user to change the Owner of a piece of a Case.***
Share	***Allows a user to add members to a Case, giving them access to the associated Evidence.***
Share with Partner Agencies	***Allows users to send cases to a partner agency. After the partner agency accepts the case, the evidence in the case is copied to the partner agency and no further actions by the partner agency are shown in your agency's audit logs.***
Share External Download Links	***Allows users to send an email containing a download link to individuals outside of your agency. This link allows recipients to download all of the evidence in the case. Using the link does not require recipients to log in to an Evidence.com account or even to have an Evidence.com account. Only the apparent IP address of the computer downloading the file appears in your agency's audit logs.***
Audit Trail PDF	***Allows a user to view and download the record of who has Viewed or Edited a Case.***
View & Add Case Notes	***Allows a user to write messages associated with a Case.***
Create Case	***Allows a user to create a Case.***
Restricted Category Access	***Allows a user to access Cases that have been categorized as Restricted Access.***
Shared Case	
View	***Allows users to access a Case that has been Shared with them.***
Edit	***Allows users to Edit Case ID, Description, Categories, Tags, and Folder Structure of a Case that has been shared with them.***
Reassign	***Allows a user to reassign a Case that has been Shared with them.***
Share	***Allows users to add members to a Case that has been shared with them, giving access to the associated Evidence.***
View & Add Case Notes	***Allows users to write messages associated with a Case that has been Shared with them.***
Audit Trail PDF	***Allows users to view and download the record of who has Viewed or Edited a Case that has been shared with them.***
Email Notification Preferences	
Account Lockout Notification	***Determines whether or not a user will receive Account Lockout Notifications when any user in the agency is locked out.***
Upcoming Evidence Deletion Notification	***Determines whether or not a user will receive weekly notifications of any upcoming evidence deletions in the agency.***
Evidence Timestamp Notification	***Determines whether or not a user will receive weekly notifications of evidence whose timestamp indicates it is older than 14 days.***

3.11.5.9 VMS shall allow users to search video files by name, date of recording, date of upload, case number (CAD-generated), device number, as well as categorize and add notes to each file within the solution.

Yes. By enabling officers to annotate Axon video with meta-data, Evidence.com turns what was once an overwhelming amount of files and information into a database of highly searchable evidence.



For evidence searches, the ID, Title, and Tag filters provide advanced text matching features.

- ***The text you enter can match any part of the data you are filtering. For example, if you enter 21 in the ID box, any evidence whose ID includes "21" in any portion of the ID is included in search results.***
- ***You can search for more than one text string in a single filter. For example, if you enter 21 78 in the ID box, search results include evidence with the ID 213789 as well as 421278.***
- ***The order of text strings is irrelevant. For example, if you enter 78 21 in the ID box, search results include evidence with the ID 213789.***

Evidence Search Filters

Evidence.com provides a search feature to help you find the evidence you need. In the Evidence area, you can use any of three evidence search pages to narrow your results.

- ***All Evidence — Finds all evidence, including evidence that you do not have permission to view.***
- ***My Evidence — Finds evidence that you own. Under Filter Evidence, the Owner filter is automatically set to your name.***
- ***Shared Evidence — Finds evidence that has been shared with you by the evidence owner.***

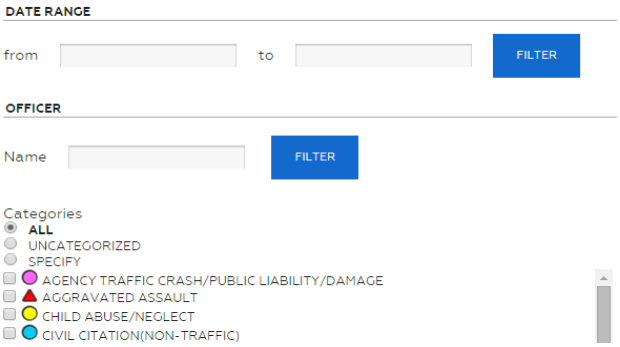
Evidence Search Fields

- ***ID — Limits search results to evidence whose ID includes the characters you enter in the ID box.***
- ***Title — Limits search results to evidence whose title includes the characters you enter in the Title box.***
- ***Category — Limits search results to evidence that is assigned to the category that you select. By default, search results include evidence assigned to any category, including uncategorized evidence.***

- ***Date — Limits search results by either the recorded, uploaded, or deletion date of evidence, as selected. You must also specify a date range by using the From and To boxes, else the search is not limited by date range. Search results are inclusive of the dates specified.***
  - ***From — The start of the date range. If the From box is empty, the date range begins with the earliest possible date.***
  - ***To — The end of the date range. If the To box is empty, the date range ends with today.***
- ***File Type — Limits search results to the file type selected. By default, search results include all file types.***
- ***Owner — Limits search results to evidence owned by the user specified. To specify the user, click in the Owner box, start typing the name of the user, wait for the system to show the matching users, and then click the user you want. On the My Evidence page, the Owner filter is set to your name by default.***
- ***Uploaded By — Limits search results to evidence uploaded by the user specified. To specify the user, click in the Uploaded By box, start typing the name of the user, wait for the system to show the matching users, and then click the user you want.***
- ***Status — Limits search results to evidence whose status matches the status selected. By default, evidence searches are limited to evidence with a status of Active.***
- ***Tag — Limits search results to evidence whose tags includes the characters you enter in the Tag box.***
- ***Group — Limits search results to evidence owned by members of the group specified. To specify the group, click in the Group box, start typing the name of the group, wait for the system to show the matching groups, and then click the group you want.***
- ***Flagged — Limits search results to evidence whose flag status matches the flag status selected.***

Evidence Map Search Feature

GPS tagging is available when one of TASER's free mobile applications, Axon View and Axon Capture, is installed on an officer's smart device and paired to his camera via Bluetooth.



The Axon will source GPS location information from the mobile device and video files are automatically tagged with GPS locations. When a new coordinate is received, the coordinates are sent to the camera system. The metadata is pulled directly from the smart device's GPS coordinates and the location is then geotagged in Evidence.com.

If the NHP's Records Management System or Computer-Aided Dispatch System is integrated with Evidence.com, GEO-tagging will be available using the address sourced from the RMS or CAD system. This integration effectively automates the process of tagging videos with complete, correct metadata.

The Evidence Map feature shows pin icons for any evidence with associated location information and basic features for finding and viewing a location on the map. The map pin style used for an evidence file is determined by the category assigned to the evidence.

3.11.5.10 VMS must allow System Administrators the ability to grant access of specific files to specified persons for a specific period of time.

Yes. When an officer wishes to share the video, he or she simply selects the share option adjacent to the video, and then enters the first or last name, or the badge number of their superior. The user can also assign a time limit, limiting the parties' ability to watch the video to a specified amount of days.

3.11.5.11 VMS shall have the ability to share files internally and externally via secure links over the Internet.

There are several options for sharing evidence with interested parties.

<u>Internal Sharing</u> allows for intra-agency sharing of evidence, ideally from an officer to a superior. When an officer wishes to share the video, they simply select the share option adjacent to their video, and then enter the First or last name, or the badge number of their superior. By default, users or patrol officers are limited to this feature.

<u>External sharing</u> allows for inter-agency sharing, or sharing with organizations like City and District Attorneys. In the same way an officer can share a video with a superior, an employee with Administrative rights on Evidence.com can share a video outside of the Agency. This is particularly useful for FOIA requests and public records requests.

The collaboration function is focused on the inter-agency aspect of sharing. If two agencies choose to collaborate, they no longer have to enter an entire e-mail address, as they would normally when externally sharing. If your Administrator wanted to share a video with another Agency, rather than specifying the recipient's email address, they would simply be able to type in their name. The feature is at the discretion of the Agency administrator. And agencies that you collaborate with do not have visibility to your Agency's content. It's simply designed to make sharing a bit easier.

When all of the evidence pertaining to an incident has been grouped together in a Case, you can transfer that package to your trusted Partner Agencies. When they accept the case, they will have their own copy of the files to manage independently. They can then control their own retention policies and access rights without affecting yours.

Another option is to create an account for the external party that is highly restricted only to videos that are shared with them by the Agency. The Agency can also assign a time limit, limiting the external parties' ability to watch the video to a specified amount of days.

An administrator can also access a file on Evidence.com, download the file, and then burn or copy the file to CD, DVD or a flash/USB drive.

Bulk Share by Unauthenticated Download Link

Bulk sharing enables the agency to share more than one evidence file at a time. Sharing by download link makes the shared evidence available through a web link, or URL, for downloading a ZIP file of the evidence from Evidence.com—without requiring the person downloading the evidence to sign in to Evidence.com.

Bulk Share Evidence by Authenticated Sharing

Bulk sharing enables the agency to share more than one evidence file at a time. Authenticated sharing enables you to share evidence with other users of Evidence.com. The agency should use authenticated sharing when it is required that evidence is available only to users who sign in to Evidence.com. The agency can control whether users with whom evidence is shared can view the evidence, download the evidence, view the audit trail of evidence, and share the evidence with others. Bulk sharing evidence

grants each user the same permissions to the shared evidence. If the agency needs to grant different permissions to different users, this procedure is performed once for each set of users granted the same permissions. These permissions can be revoked at any time based on a certain time limit the agency sets or through a manual revoking of the permissions granted.

Receiving Shared Cases from Partner Agencies

The NHP can enable a group to receive cases shared by partner agencies. When a partner agency shares a case, they can send it to groups permitted to receive shared cases. All members of the group receive a message notifying them of the invitation to receive the shared evidence.

The user who accepts the case shared with the group becomes the owner of the evidence. While accepting the case, the user can add or remove evidence access for other group members. A group that is monitoring a group that receives a shared case from a partner agency can view the evidence of the shared case.

External and Interagency Sharing

Evidence.com makes it easy to send evidence to organizations like City and District Attorneys. Users can share a single file, multiple files, or, when all of the evidence pertaining to an incident has been grouped together in a case, a copy of the case and its evidence can be sent to trusted Partner Agencies. When they accept the case, the system creates a copy of the files, which they can manage independent of the original case and evidence. Likewise, they can then control their own retention policies and access rights without affecting any agency's evidence.

Collaborating with another Evidence.com agency makes sharing evidence with that agency as simple as if they were part of your own agency, while still maintaining the agency's data security. Collaborating agencies have access only to that data specifically share with them. All unshared data belonging to an agency will remain unavailable to partner agencies.

Evidence.com for Prosecutors

Managing Evidence from Capture to Courtroom

The same end-to-end evidence management solutions of Evidence.com now allow prosecutors to manage evidence of any type, from any agency, all in one place. Files can be shared during discovery, complete chain of custody is maintained, and all evidence is encrypted. Prosecuting attorneys working with agencies already using Evidence.com, standard licenses are provided at no cost.

3.11.5.12 When videos are exported to a portable media device, all metadata shall transfer over without compromising its authenticity.

Yes. The Axon Body 2 will export all recorded footage to the Application in the original file format, without loss of quality of associated metadata.

Metadata will be maintained if the footage is exported into another media form (DVD, streaming, etc.)

3.11.5.13 VMS shall grant System Administrators the ability to set variable retention rules per DPS/HPD preferences.

Yes. Retention periods are determined by the evidentiary category assigned to a file. Categories are customizable and can be unique to your agency; the category or categories assigned to a file populate as a metadata field.

Categorizing Evidence Simplified

Categorizing evidence simplifies searching for videos in Evidence.com and facilitates seamless database management by ensuring only relevant evidence is retained in the system. The administrator creates evidence categories with corresponding retention times and can configure and delete categories. While any evidence can be kept indefinitely, departments often store critical incidents such as homicides, felonies, etc. for many years (if not indefinitely) and less significant events (i.e. routine traffic stops or training videos) for a few months.

While there is no limit to the number of retention categories that can be created, we recommend no more than 10 for your department's most utilized categories. Many agencies using Evidence.com have found that using no more than 10 categories is ideal because it simplifies the categorization process and facilitates use of the mobile device (if applicable) by not requiring officers to scroll through a long list of different options.

Evidence Retention Policy

For proper management, NHP should create a set of agency-specific categories large enough to properly segregate evidence by type for retention setting and search functionality. This list should not be so large that it becomes an impediment to efficient field use by Users. Agencies are encouraged to consult their State Retention Schedules, City/County or State Attorneys or other legal counsel for guidance on proper retention setting.

The evidence retention policy determines:

1. **Whether the system will initiate automatic deletion of evidence assigned to the category.**
2. **How long the system waits before initiating the deletion of evidence that is not included in a case. Axon video deletions are based on the recording date. Deletion of all other evidence is based on the upload date.**

	NAME	RETENTION DURATION
1.	Uncategorized	Until manually deleted
2.	Intelligence	Until manually deleted
3.	No Event	31 Days
4.	Offence	10 Years
5.	Pending Review	Until manually deleted
6.	Person of Interest	1 Year
7.	Work Health	10 Years

Cases

Retention policies apply to evidence only. Cases are never deleted automatically. Evidence included in a case is exempt from deletion until it is removed from the case. If evidence is assigned multiple retention categories, the longest retention time will be used.

Special Categories

The system includes two special categories:

- **Uncategorized — Any evidence that is not assigned to another category is automatically assigned to the Uncategorized category. When you assign a category to evidence, it is automatically removed from the Uncategorized category.**

You cannot change the evidence retention policy for this category. Evidence assigned to this category must be manually deleted.

- **Pending Review — Files are automatically added to this category when they encounter errors during creation or upload that may prevent them from functioning properly. These files should be periodically reviewed and the following actions taken:**
  - **If the file appears to be functioning properly within Evidence.com, it can be removed from this category and added to its correct one per agency policy.**
  - **If the file is not functioning properly, please contact Help@evidence.com or visit the Contact Us page to request service to help recover the files.**
  - **You cannot make the Pending Review category a restricted category.**
  - **You cannot delete the Uncategorized or Pending Review category.**

New Evidence.com agencies are provided with four additional categories that you can edit and delete as needed:

- **Officer Injury**
- **Traffic Stop**
- **Training Demo**
- **Use of Force**

3.11.5.14 VMS shall have the ability to set time tables for automatic deletions of files.

Yes. Every event that is captured and uploaded to Evidence.com can be assigned a category to determine how long it is retained in the system. Proper categorization is important to ensure that incidents remain in the system for the appropriate amount of time.

Automated deletion is reliant on the NHP establishing retention categories that will be associated with a retention period. Evidence.com will automatically trigger the deletion of a file according to the retention period associated with the category. If no retention period is specified, then video will remain on the system until manually deleted.

Retention periods can always be adjusted for individual files after they are uploaded to Evidence.com, which will be useful if a particularly critical incident is captured and must be stored on file indefinitely. If recently deleted files are still needed, a "remorse period" ensures that those files can still be retrieved within a seven-day timeframe.

Manual Deletion

The System Administrator can also delete evidence as necessary manually. The evidentiary Audit Trail will be retained after the evidence is purged for the purpose of accountability. The Audit Trail will indicate if the file was removed manually or through retention via categories. Administrators can run reports on Evidence Created and Evidence Deleted within a specified time range.

3.11.5.15 VMS should have the ability to recover deleted evidence within a minimum of seven (7) days of deletion. The State would prefer a recovery period of 30 days.

To protect against accidental deletions, administrators can recover files up to 7 days after they are queued for deletion. This policy applies to evidence only. Cases are never deleted automatically. Evidence included in a case is exempt from deletion until it is removed from the case. If evidence is in multiple categories, the longest retention time will be used. This 7-day remorse/recovery period and approval workflow is designed to protect evidence and chain of custody. After the remorse period, the event is expunged.

3.11.5.16 The VMS will maintain a log/audit trail illustrating users who have viewed and copied video to an external source (e.g. DVD/ long term storage).

Yes. The detailed Evidence Audit Trail can be used to determine compliance with chain of custody regulations. All content uploaded to Evidence.com is paired with an audit trail indicating every action applied to that evidence and its metadata. Information such as viewed by, downloaded by, and deleted by, is all included in the audit trail, in addition to the source IP Address of the person who made the change. All audit trails can be exported to a PDF document.

To ensure a robust chain of custody, evidence can be verified for authenticity by matching the SHA hash of original file ingested in Evidence.com with the copy. The original data associated with a video is never changed. All modifications are handled by creating new, derivative files. Detailed audit logs track all evidence access.

3.11.5.17 VMS must have the ability to preserve the raw file without editing.

Yes. The best way to describe how Evidence.com manages video is through layers. The two bottom layers are the original video and audio. Those two layers are never tampered with or manipulated. When we apply markers, clips, or redaction they exist in layers above the original content. The best way to imagine this would be to picture a translucent sheet over a picture or painting. Editing is simply drawing on the sheet, and then removing the sheet. This leaves you with an un-altered original image. When a user applies redaction to a video, all of their actions are saved to an XML file, much like the translucent sheet. When the video is played back the sheet is layered back over the video. Even when a redacted video is exported from Evidence.com, the video is created (encoded) on the fly and saved to the local hard drive.

3.11.5.18 VMS must securely store all videos and recordings in a way that only State-authorized users and users authorized by DPS/HPD can view.

Yes. In order to access recordings housed on the Agency's Evidence.com account, a person would require a user login, including an email address and password. Access to information stored on Evidence.com governed by the City/Agency-defined access control system built into Evidence.com. Access is controlled according to:

- ***Pre-defined roles***
- ***Pre-defined individuals (i.e., who has access to what camera feed)***
- ***User account-specific passwords.***

3.11.5.19 VMS must provide redundant, security back-up of all data.

Yes. The Axon solution will provide maximum security against data loss using industry best practices and minimize, if not eliminate any possible interruption to service:

- ***Multiple Locations - Each Evidence.com region is comprised of multiple, isolated locations and all Evidence.com application components are duplicated across all these locations for a fully redundant, Hot/Hot failover, infrastructure***

- ***Highly Available - Evidence.com is spread across isolated locations, and all components (e.g. databases, web servers) are further backed up daily to a highly available and durable storage location to support a Hot/Cold failover and recovery objective.***

- ***Automatic Failover - No human intervention is required in the event of a primary data center failure.***

- ***Active-Active Topology - Because the solution was designed from the start to run as a highly-available application, it is equipped to handle a wide range of failures in the underlying infrastructure. The active-active design means that computing resources are efficiently utilized, no resources are wasted on "standby" servers.***

- ***Commodity Hardware - No special systems required for high-availability.***

- ***Local Replication – the application also makes its easy, should the NHP wish, to keep local copies of certain content. The application provides "Bulk Download" functionality.***

3.11.5.20 VMS should offer redaction capabilities.

Yes. Evidence.com features a full redaction suite natively within the application. This functionality is available to all licensed users, subject to your agency's role-based access controls.

Evidence.com offers both automated and manual options for redacting an evidence file (or multiple evidence files). A full description of the comprehensive redaction capabilities within Evidence.com follows.

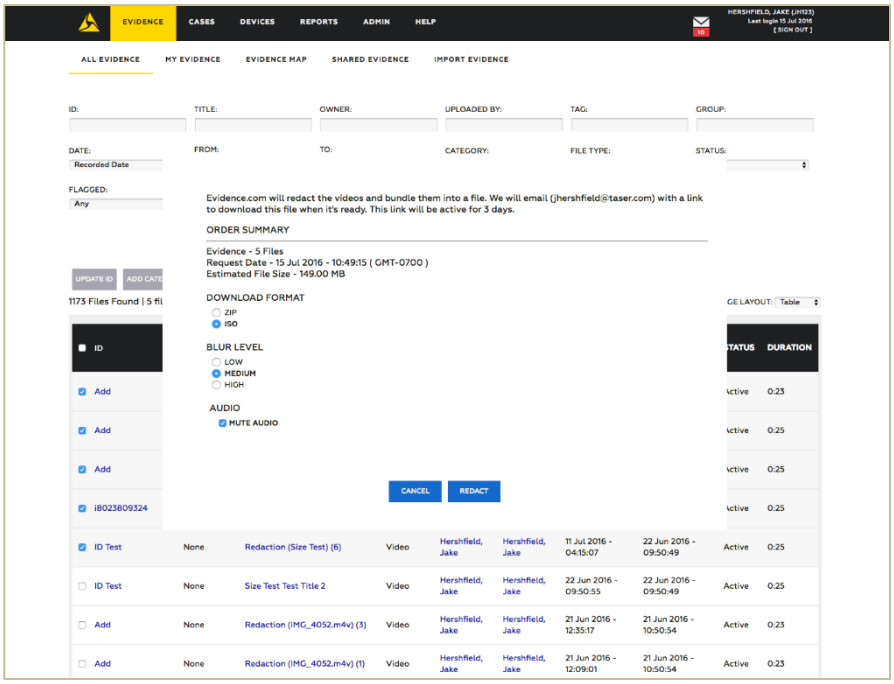
EVIDENCE.COM REDACTION SUITE OVERVIEW

Evidence.com offers users three options to redact videos, each to be used in a different scenario: Bulk Redaction, Smart Tracker Redaction and Manual Redaction. Both Bulk and Smart Tracker Redaction options are automated. Each of these options are simple and easy to use, allowing the NHP personnel to manage public information requests quickly.

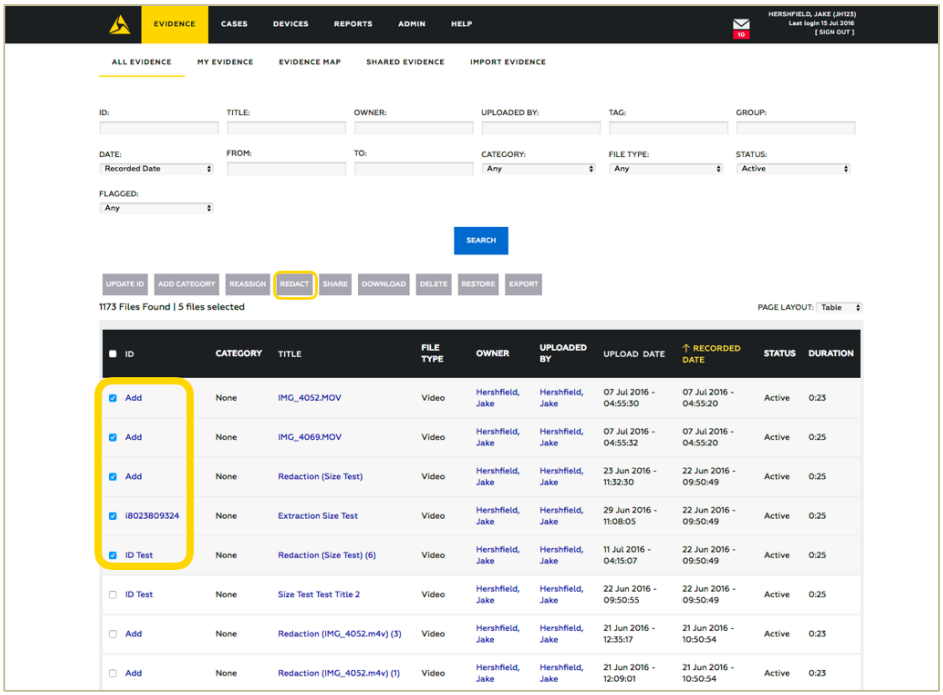
Bulk Redaction

To aid with large public disclosure requests, the Bulk Redaction feature allows a user to queue video evidence for bulk redaction. Bulk redaction creates a copy of the original video and a blur filter over the entire video automatically. It can also remove audio for the duration of that copy. The blur over the

entire video allows requestors to see what happened in the video without potentially revealing personally identifiable details such as faces, addresses, or license plates. This presents an opportunity for agencies to fulfill the public disclosure request in the least amount of time.



It is recommended that a user verifies bulk-redacted videos to ensure the proper level of blur is applied to each file prior to releasing the redacted version. If a user needs to redact a video more precisely, such as redacting only a portion of each video frame, they can redact a single video.



Smart Tracker Redaction

Smart Tracker Technology within Evidence.com brings intelligent, automated support to agency video redaction workload. Using the Smart Tracker technology, users can easily create a redaction that tracks up to 10 objects in a video. For each object, specify a start and end frame. On each start frame, place and size a redaction mask.

Once a user is done preparing assisted redaction, Evidence.com's technology tracks the redacted objects automatically and sends a notification email when it has finished creating the redaction.

It is recommended that users closely verify redacted clips created using assisted redaction. If corrections are necessary, Evidence.com allows for manual edits to redacted clips.

Smart Tracker Technology Concepts

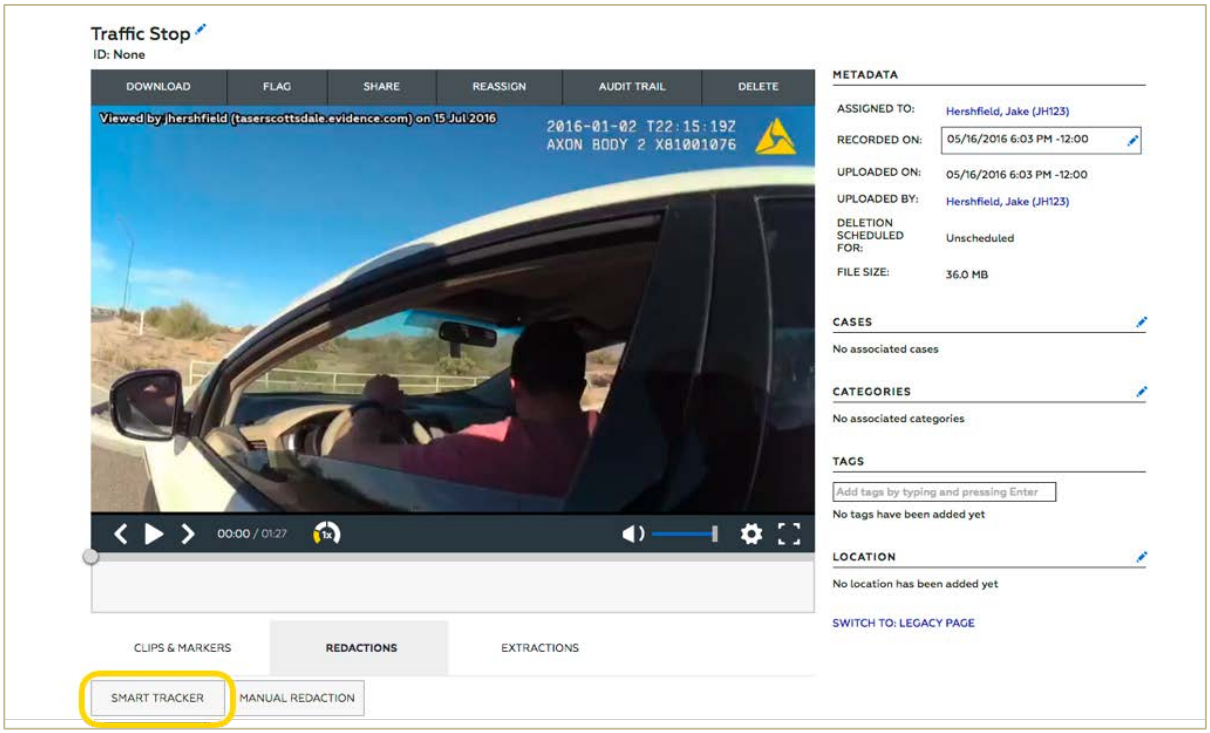
Using Smart Tracker technology to create a redaction shares many concepts with manual redaction. Because Smart Tracker technology automatically tracks objects in the video file, the Smart Tracker feature represents an object and its timeline with one control, eliminating the need to create multiple mask timelines per object.

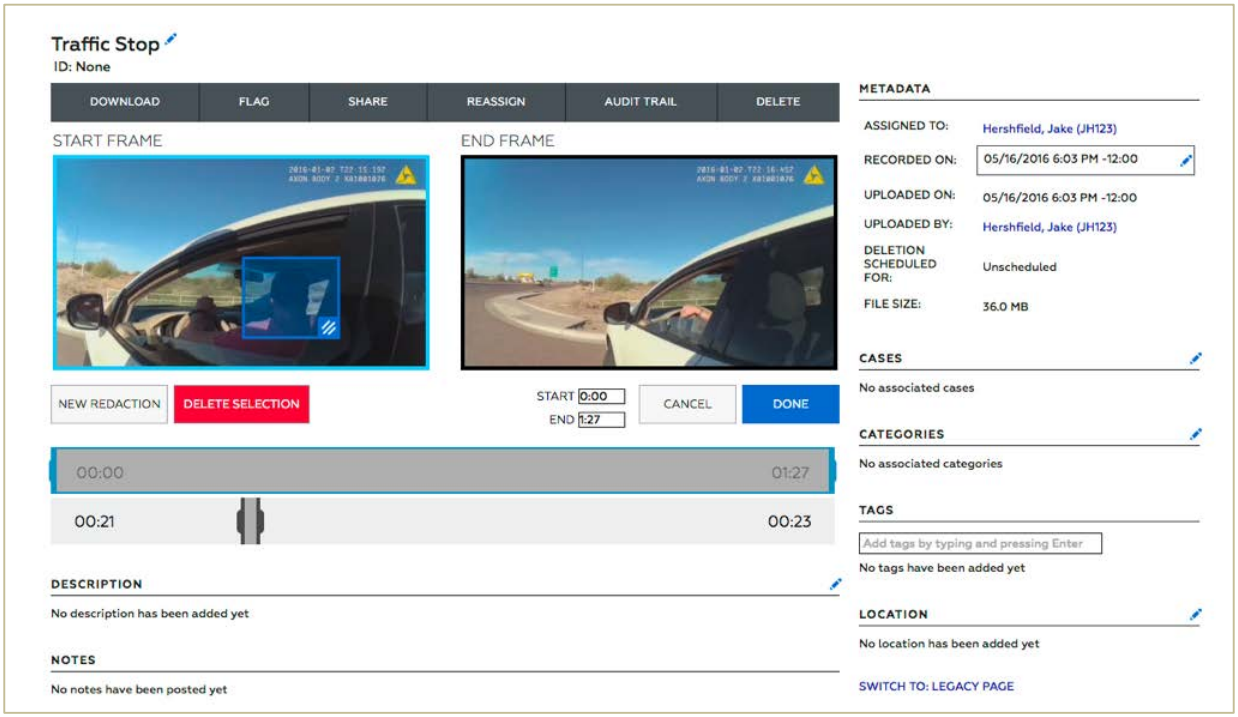
- ***Object—Enables users to redact one actual object in the video. An assisted redaction object contains only one object timeline. Smart Tracker supports up to 10 objects.***

- ***Object Timeline—Represents all frames in the video and enables users to place the mask segment precisely where it is needed. Each Smart Tracker object timeline has one mask segment.***

Smart Tracker Technology Controls

On each start frame, position the redaction mask and when preparation of assisted redaction is complete, Evidence.com tracks the redacted objects automatically and notifies the user when tracking is complete. A user can then verify the redaction as closely as needed. If corrections are needed, Evidence.com allows manual adjustments.





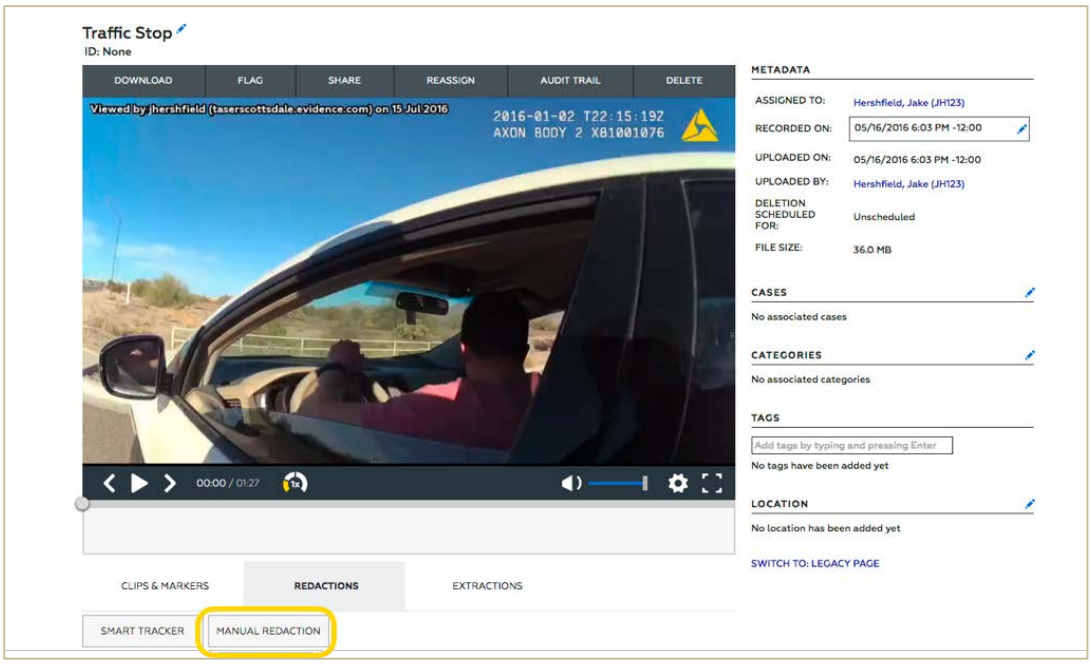
Manual Redaction

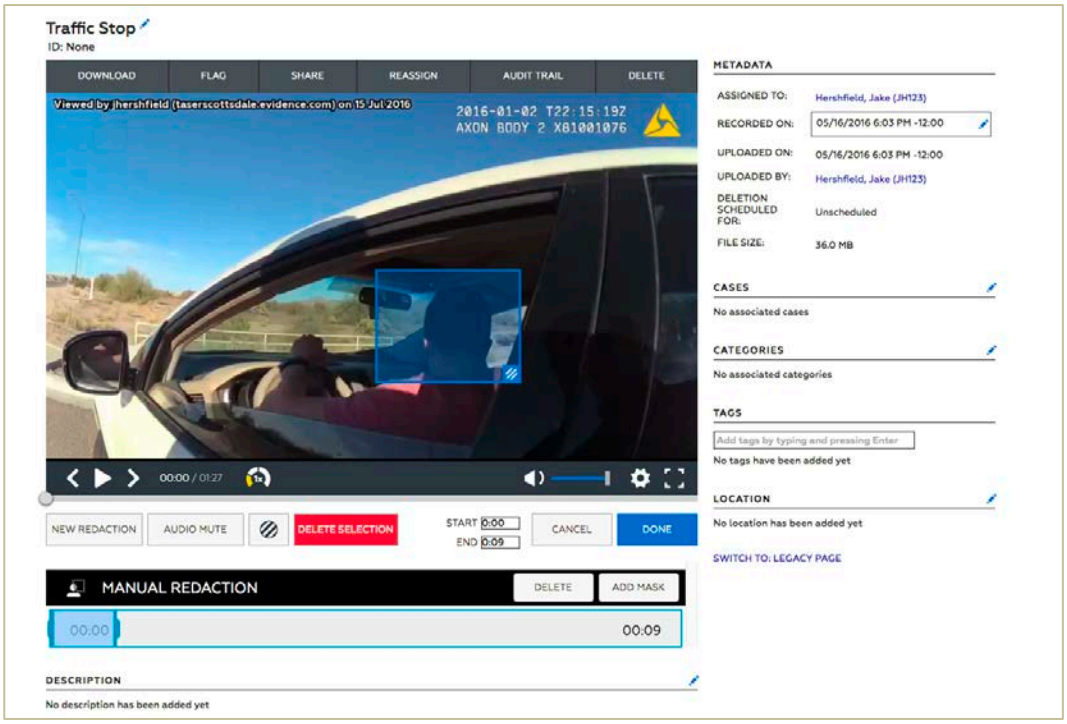
Manual redaction allows the user to control size, shape, and placement of redaction masks precisely, frame by frame.

Manual Redaction Concepts

Creating a redaction manually involves working with several important concepts.

- ***Object—Organizes the mask segments that redact one actual object in the video. A redaction contains one or more objects. An object contains one or more mask timelines.***
- ***Mask—Defines a rectangular area in a continuous segment of video frames that are redacted. A mask has three dimensions:***
  - ***Height, defined by the mask frame***
  - ***Width, defined by the mask frame***
  - ***Duration, defined by the start and end handles of the mask segment.***
- ***Mask Timeline—Represents all frames in the video and enables you to place the mask segment precisely where you need it. Each mask timeline has one mask segment.***
- ***Mask Segment—Defines the continuous series of frames that the mask redacts. A mask segment has a start and an end handle.***
- ***Mask Segment Handle—Defines the start or end frames of a mask segment.***
- ***Mask Frame—Defines the rectangular area redacted by a mask.***
- ***Mask Frame Handle—Enables you to change the size and shape of the mask frame.***


Traffic Stop
ID: None
DOWNLOAD
FLAG
SHARE
REASSIGN
AUDIT TRAIL
DELETE
Viewed by jhershfield (taserscottsdale.evidence.com) on 15 Jul 2016
2016-01-02 T22:15:19Z
AXON BODY 2 X81001076
00:00 / 01:27
CLIPS & MARKERS
REDACTIONS
EXTRACTIONS
SMART TRACKER
MANUAL REDACTION
METADATA
ASSIGNED TO: Hershfield, Jake (JH123)
RECORDED ON: 05/16/2016 6:03 PM -12:00
UPLOADED ON: 05/16/2016 6:03 PM -12:00
UPLOADED BY: Hershfield, Jake (JH123)
DELETION SCHEDULED FOR: Unscheduled
FILE SIZE: 36.0 MB
CASES
No associated cases
CATEGORIES
No associated categories
TAGS
Add tags by typing and pressing Enter
No tags have been added yet
LOCATION
No location has been added yet
SWITCH TO: LEGACY PAGE


Traffic Stop
ID: None
DOWNLOAD
FLAG
SHARE
REASSIGN
AUDIT TRAIL
DELETE
Viewed by jhershfield (taserscottsdale.evidence.com) on 15 Jul 2016
2016-01-02 T22:15:19Z
AXON BODY 2 X81001076
00:00 / 01:27
NEW REDACTION
AUDIO MUTE
DELETE SELECTION
START 0:00
END 0:09
CANCEL
DONE
MANUAL REDACTION
DELETE
ADD MASK
00:00
00:09
DESCRIPTION
No description has been added yet
METADATA
ASSIGNED TO: Hershfield, Jake (JH123)
RECORDED ON: 05/16/2016 6:03 PM -12:00
UPLOADED ON: 05/16/2016 6:03 PM -12:00
UPLOADED BY: Hershfield, Jake (JH123)
DELETION SCHEDULED FOR: Unscheduled
FILE SIZE: 36.0 MB
CASES
No associated cases
CATEGORIES
No associated categories
TAGS
Add tags by typing and pressing Enter
No tags have been added yet
LOCATION
No location has been added yet
SWITCH TO: LEGACY PAGE

Additional Functionality

Blur Levels

Users can toggle the blur level of the redaction masks from low, medium, high, and blackout blur.

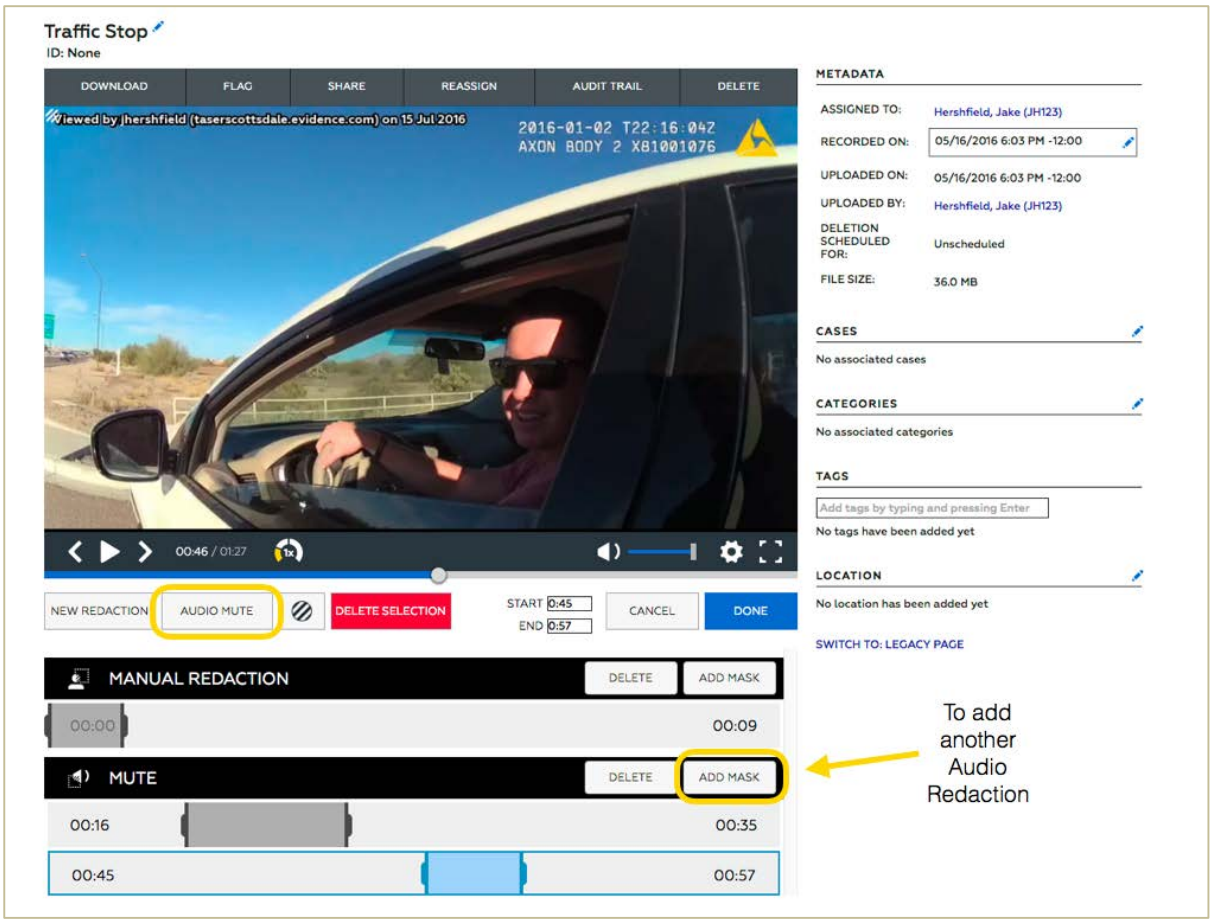
Keyboard Shortcuts

For users who redact a large volume of video, keyboard shortcuts are a simplified way to navigate throughout the video.

When selected on a redaction segment, the "A and S" keys move the start handle back and forth, respectively, and the left and right arrow keys move the end hand back and forth, respectively. These shortcuts allow users to complete frame-by-frame redaction in an intuitive way.

Audio Redaction

Users can redact audio just as they redact video, resulting in a complete removal of the audio track for the duration specified. Users can also redact the audio or different portions of the same video by pressing the "Add Mask" button.



Filters

Evidence.com offers complete application of various image-processing filters for the duration specified. Optionally audio redaction can be enabled during video segments that have been blackout redacted. Examples of filters are as follows:

- ***Light Blur***
- ***Normal Blur***
- ***Heavy Blur***
- ***Blackout***

Light Blur

Normal Blur

Heavy Blur

Blackout

3.11.5.21 VMS must be compatible with at least Windows 7 Professional Operating System or more recent versions) and Internet Explorer Version 11 web browser or more recent version(s).

Yes. Evidence.com can be accessed from any computer. Users can access Evidence.com with the following web browsers:

- ***Internet Explorer version 10 and above***

Note: If you use Internet Explorer, ensure that Compatibility View is disabled. Evidence.com does not support the use of the Compatibility View feature. To verify your Internet Explorer settings, go to Tools > Compatibility View settings and ensure that Evidence.com is not included in the list of websites added to Compatibility View and that the "Display all websites in Compatibility View" check box is cleared.

- ***Chrome version 40 and above***
- ***Firefox version 30 and above***
- ***Safari version 8 and above***

Additionally, TASER supports the media player and related tools, introduced in Evidence.com release 1.27, with the following web browsers:

- ***Internet Explorer version 10 and above***
- ***Chrome version 43 and above***
- ***Firefox version 38 and above***
- ***Safari version 8 and above***

If you use an unsupported browser to access media-evidence files, Evidence.com provides the traditional media player.

It is strongly recommended that you always use the latest release of Adobe Flash.

Evidence Sync Minimum System Requirements

- ***Windows XP or 7***
- ***Microsoft Direct X (Version 7.0 or greater for exported incident video processing)***
- ***Adobe Reader***
- ***Apple QuickTime or VLC Media Player***
- ***Pentium 4 or AMD Athlon Processor***
- ***128 MB of RAM***
- ***Audio Card***
- ***Video Card (1024 x 768 Resolution or Better, with 24-bit Color)***
- ***PATA Hard Drive with At Least 2 GB of Available Disk Space***
- ***Internet Access (Recommended)***
- ***2.0 Self-Powered USE BUS or HUB***

3.11.5.22 Provide the minimum required memory (RAM), if applicable.

Not applicable. Because Evidence.com is a cloud-based solution launched through a Web browser, the only memory requirement would be that of the device from which a user is accessing Evidence.com, as computers require RAM when accessing any website.

3.11.5.23 Provide the minimum required processor speed, if applicable.

Not applicable. Because Evidence.com is a cloud-based solution launched through a Web browser, the only requirement would be that of the device from which a user is accessing Evidence.com, as computers require processor speed when accessing any website.

3.11.5.24 Provide the minimum network speed to upload videos, if cloud based.

Yes. Restrictions on uploading data from cameras is only limited by the bandwidth available to the Agency.

3.11.5.25 Upload times to the VMS will be defined in per hour or thirty-minute increments of video files.

Yes. Single events spanning longer than 30 minutes are recorded as multiple segments in 30 minute increments. Breaking up a single event into smaller sections allows for ease of uploading video evidence to Evidence.com. Segmented videos of a single event will be exported as multiple files in the same 30 minute increments captured at the time of the event recording. Timestamps and metadata associated with the videos make it easy to identify multiple files associated with a singular event.

3.11.5.26 Any required or expected 'buffering' times before video files are accessible in cloud storage (for view or adding metadata) will be clearly defined.

Yes. Videos cannot be viewed until the file is uploaded successfully to Evidence.com. Upload time is dependent on agency bandwidth.

3.11.5.27 Describe System compatibility with mobile devices (iPhones and Android).

Yes. Using a compatible browser installed on the tablet etc. Evidence.com is written in HTML5 to allow mobile devices to display the site and can be accessed with the following web browsers:

- ***Internet Explorer version 10 and above***

Note: If you use Internet Explorer, ensure that Compatibility View is disabled. Evidence.com does not support the use of the Compatibility View feature. To verify your Internet Explorer settings, go to Tools > Compatibility View settings and ensure that Evidence.com is not included in the list of websites added to Compatibility View and that the "Display all websites in Compatibility View" check box is cleared.

- ***Chrome version 40 and above***
- ***Firefox version 30 and above***
- ***Safari version 8 and above***

Additionally, TASER supports the media player and related tools, introduced in Evidence.com release 1.27, with the following web browsers:

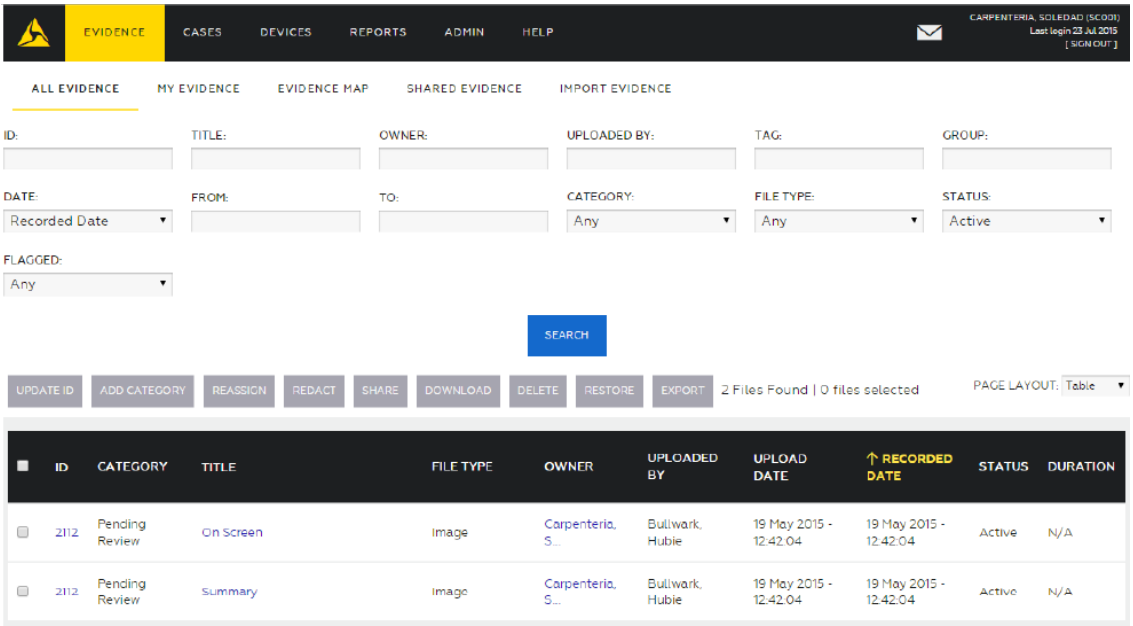
- ***Internet Explorer version 10 and above***
- ***Chrome version 43 and above***
- ***Firefox version 38 and above***
- ***Safari version 8 and above***

The Axon Capture Mobile Application requires iOS 8.0 or later for Apple products and Android 4.1 and up.

The Axon View Mobile Application requires iOS 8.0 or later for Apple products and Android versions vary by device.

3.11.5.28 Vendor shall indicate the number of searchable fields in storage system and any 'wild card' searches that can be done to locate stored data.

Yes. By enabling officers to annotate Axon video with metadata, Evidence.com turns what was once an overwhelming amount of files and information into a database of highly searchable evidence using 13 fields and text searches. Users can also search by location..



For evidence searches, the ID, Title, and Tag filters provide advanced text matching features.

- ***The text you enter can match any part of the data you are filtering. For example, if you enter 21 in the ID box, any evidence whose ID includes "21" in any portion of the ID is included in search results.***
- ***You can search for more than one text string in a single filter. For example, if you enter 21 78 in the ID box, search results include evidence with the ID 213789 as well as 421278.***
- ***The order of text strings is irrelevant. For example, if you enter 78 21 in the ID box, search results include evidence with the ID 213789.***

Evidence Search Filters
Evidence.com provides a search feature to help you find the evidence you need. In the Evidence area, you can use any of three evidence search pages to narrow your results.

- ***All Evidence — Finds all evidence, including evidence that you do not have permission to view.***
- ***My Evidence — Finds evidence that you own. Under Filter Evidence, the Owner filter is automatically set to your name.***
- ***Shared Evidence — Finds evidence that has been shared with you by the evidence owner.***

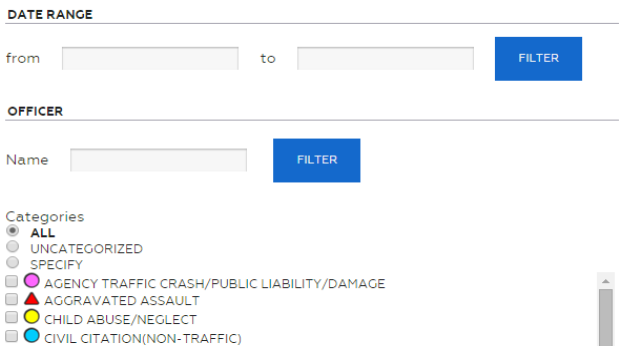
Evidence Search Fields

- ***ID — Limits search results to evidence whose ID includes the characters you enter in the ID box.***
- ***Title — Limits search results to evidence whose title includes the characters you enter in the Title box.***
- ***Category — Limits search results to evidence that is assigned to the category that you select. By default, search results include evidence assigned to any category, including uncategorized evidence.***
- ***Date — Limits search results by either the recorded, uploaded, or deletion date of evidence, as selected. You must also specify a date range by using the From and To boxes, else the search is not limited by date range. Search results are inclusive of the dates specified.***
  - ***From — The start of the date range. If the From box is empty, the date range begins with the earliest possible date.***
  - ***To — The end of the date range. If the To box is empty, the date range ends with today.***
- ***File Type — Limits search results to the file type selected. By default, search results include all file types.***
- ***Owner — Limits search results to evidence owned by the user specified. To specify the user, click in the Owner box, start typing the name of the user, wait for the system to show the matching users, and then click the user you want. On the My Evidence page, the Owner filter is set to your name by default.***
- ***Uploaded By — Limits search results to evidence uploaded by the user specified. To specify the user, click in the Uploaded By box, start typing the name of the user, wait for the system to show the matching users, and then click the user you want.***
- ***Status — Limits search results to evidence whose status matches the status selected. By default, evidence searches are limited to evidence with a status of Active.***
- ***Tag — Limits search results to evidence whose tags includes the characters you enter in the Tag box.***
- ***Group — Limits search results to evidence owned by members of the group specified. To specify the group, click in the Group box, start typing the name of the group, wait for the system to show the matching groups, and then click the group you want.***
- ***Flagged — Limits search results to evidence whose flag status matches the flag status selected.***

Evidence Map Search Feature

GPS tagging is available when one of TASER's free mobile applications, Axon View and Axon Capture, is installed on an officer's smart device and paired to his camera via Bluetooth.

The Axon will source GPS location information from the mobile device and video files are automatically tagged with GPS locations. When a new coordinate is received, the coordinates are sent to the camera system. The metadata is pulled directly from the smart device's GPS coordinates and the location is then geo-tagged in Evidence.com.



If the NHP's Records Management System or Computer-Aided Dispatch System is integrated with Evidence.com, GEO-tagging will be available using the address sourced from the RMS or CAD system. This integration effectively automates the process of tagging videos with complete, correct metadata.

The Evidence Map feature shows pin icons for any evidence with associated location information and basic features for finding and viewing a location on the map. The map pin style used for an evidence file is determined by the category assigned to the evidence.

3.11.5.29 Users should have the ability to send email messages from hosted solution interface to end users.

Yes. You can set personal preferences for email notifications. The email notifications that are available to you are determined by the role assigned to your user account. The agency logo appears on audit trail PDFs and system-generated emails.

Evidence.com supports the following email notification settings:

- ***Account Lockout Notification — Turn on to receive an email if Evidence.com locks your account because you exceeded the maximum number of incorrect login attempts.***
- ***External Agency Collaboration Notifications — Turn on to receive notifications regarding other agencies that would like to collaborate with you and share evidence.***
- ***Upcoming Evidence Deletion Notification — Turn on to receive an email about the upcoming evidence deletions summary for the next week in your Evidence.com Inbox.***
- ***Evidence Timestamp Notification — Turn on to receive an email informing you about any evidence uploaded by your agency that appears to be recorded more than 14 days ago, which could be indicative of a device with a system clock in need of synchronization with Evidence.com.***
- ***Category Assignment Notification — Turn on to receive an email when evidence uploaded is also assigned to at least one category that is in the process of being deleted. This notification helps ensure that no evidence is unintentionally deleted during system-initiated evidence deletions.***

Editing a Role

If you edit a role to change any of the Login Access permissions, all users assigned to the role receive a notification email about the change.

Invite an Agency to Share with Your Agency

Administrators of agencies that you add to your Agencies with My Contacts list receive a notification email. Before you can share a case with the partner agency, an administrator from the partner agency must accept the invitation to collaborate with your agency.

Request Access to Evidence

If you wish to view a file to which you do not have access, Evidence.com sends the owner a notification email about your request.

After the owner grants you access, Evidence.com sends you a notification email. You can access the evidence from the All Evidence page and the Shared Evidence page.

Sharing Evidence (Internally and Externally)

Evidence.com emails each user who you shared the evidence with, notifying them that the evidence is available to them.

3.11.5.30 VMS should send System Administrators administrative notifications when evidence files are about to be deleted.

Yes. You can set personal preferences for email notifications. The email notifications that are available to you are determined by the role assigned to your user account. Turn on Upcoming Evidence Deletion Notification to receive an email about the upcoming evidence deletions summary for the next week in your Evidence.com Inbox.

3.11.5.31 VMS should send System Administrators administrative notifications when users need their credentials reset due to failed log on attempts.

Yes. Administrators will receive the following email notification any time a user is locked out as a result of too many failed login attempts.

AXON Evidence.com

TASER AGENCY PRO

Dear Tom Smith (Badge ID: 1122),

User Williams, Matthew (matt@test.com) has just been locked out of his/her Evidence.com account because they exceeded the maximum number of incorrect login attempts.

User Login Details:

User	Williams, Matthew
Badge ID	matt@test.com
IP	89.123.456.789
Region	N/A
Country Code	N/A

They will need to wait 1 minutes, check their login and password and try again later, or reset their password by visiting [Forgot your username or password?]

Sincerely,
The Axon Team

When a user attempts and fails to sign in to Evidence.com more times than are allowed by the agency's security settings, the user is locked out of Evidence.com and receives the message, "Too many failed login attempts. Account temporarily suspended."

3.11.5.32 VMS should offer auto-redaction capabilities, to include high-movement and low light video; preferred to minimize the amount of time to redact 30 fps for the entire length of video.

Yes. Evidence.com provides the ability to redact video evidence files as needed, such as to protect the identity of persons in a video. The redaction tools enable you to create redacted versions of video

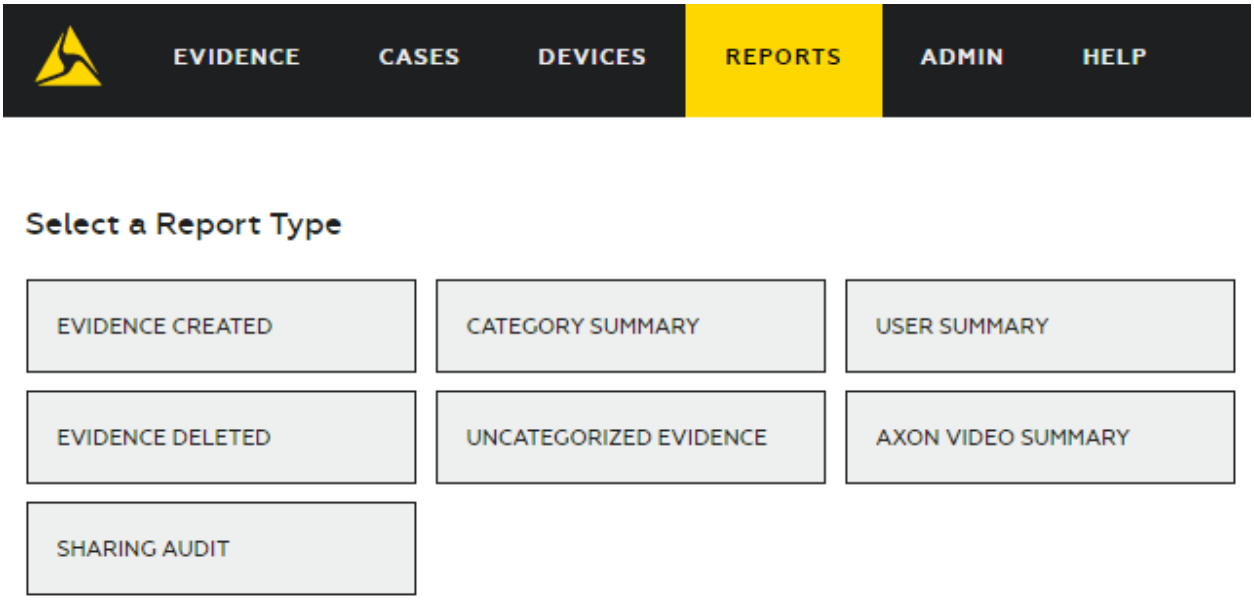
evidence files without affecting the original file. In Evidence.com, a redaction is a set of information that tells Evidence.com; what to redact in a video. When you have completed creating or editing a redaction, you can extract a redacted video. You can create and maintain many redactions for each video evidence file. This enables you to create different redacted videos for different audiences or different purposes.

Assisted redaction brings intelligent, automated support to your agency's video redaction workload. Using assisted redaction, you can easily create a redaction that tracks up to 10 objects in a video. For each object, you specify a start and end frame. On each start frame, you place and size a redaction mask. When you are done preparing an assisted redaction, Evidence.com tracks the redacted objects automatically and sends you a notification email when it has finished creating the redaction. It is recommended that you closely verify redactions created by assisted redaction. If you need to make corrections, Evidence.com enables you to edit the redaction manually.

Bulk redaction creates a copy of the original video and applies a blur filter over the entire copied video. It can also remove audio for the duration of that copy as well. The blur over the entire video allows requestors to see what happened in the video without potentially revealing personally identifiable details such as faces, addresses, or license plates.

3.11.5.33 VMS should have the ability to capture data, report on video statistics and provide custom reports.

Yes. Evidence.com allows administrators and those with the reporting permission to generate reports showing Evidence.com utilization. These options can help your agency turn that data into valuable answers to ensure your Evidence.com account is providing you with the flexibility and utility your agency deserves. Evidence.com has pre-set categories; however, agencies can add customized categories based on Agency guidelines and protocols.



Report Types

- ***Evidence Created — Lists all evidence on your agency's account in order of when the data was created. It also lists all associated metadata attached to those pieces of evidence.***

- ***Evidence Deleted — Lists all evidence deleted and associated metadata on your agency's account in order of when the data was deleted. This report will give better monitoring of automated deletions and help ensure a proper retention policy is in place.***
- ***Category Summary — Lists the current count of total files and file size in megabytes (MB) for each category as well as the percent of files assigned to that category.***
- ***Uncategorized Evidence — Lists users with uncategorized evidence assigned to them. A second tab on the export lists every piece of uncategorized evidence and includes the owner information, evidence title, date recorded, and link to the evidence.***
- ***User Summary — Lists total files and file size in MB, broken out by owner of the evidence. The counts are further broken out by evidence type, active, and deleted evidence.***
- ***Axon Video Summary — Lists usage metrics on Axon videos uploaded to your agency. The first tab is a summary of Number of videos, hours, and MB uploaded. The second tab breaks out uploads by the specified grouping: Day, Month, or Year.***
- ***Sharing Audit Report — The Sharing Audit report exports a list of all user actions related to sharing evidence and cases to a CSV file. You can specify the date range for the report.***

A report can take minutes to several hours to generate, depending on the size of the report. To run a report, you must be allowed the Generate Reports permission. You can download reports either by visiting the Reports page or by the download link in a notification email. Completed reports are available from the Download Queue section of the Reports page. If you have permission to run reports, you can download reports that any user has run.

Evidence.com reports are spreadsheets in an XLSX file format, which can be opened by many spreadsheet applications. Reports include all relevant metadata for the items included in the report. Using the Microsoft Excel pivot table function, you can group evidence by any of the fields, such as owner or badge ID, to get a better understanding of individual officer usage or certain category retentions over a given period of time.

Exporting Evidence Search Results for Reports

You can export the results of an evidence search as a list in PDF, Excel, text, or CSV format using data from the following search filters.

Evidence Search Filters

- ***ID — Limits search results to evidence whose ID includes the characters you enter in the ID box. For more information, see Text Search Details.***
- ***Title — Limits search results to evidence whose title includes the characters you enter in the Title box. For more information, see Text Search Details.***
- ***Category — Limits search results to evidence that is assigned to the category that you select. By default, search results include evidence assigned to any category, including uncategorized evidence.***
- ***Date — Limits search results by either the recorded, uploaded, or deletion date of evidence, as selected. You must also specify a date range by using the From and To boxes, else the search is not limited by date range. Search results are inclusive of the dates specified.***
  - ***From — The start of the date range. If the From box is empty, the date range begins with the earliest possible date.***
  - ***To — The end of the date range. If the To box is empty, the date range ends with today.***
  - ***File Type — Limits search results to the file type selected. By default, search results include all file types.***
  - ***Owner — Limits search results to evidence owned by the user specified. To specify the user, click in the Owner box, start typing the name of the user, wait for the system to show the matching users, and then click the user you want.***

- ***Uploaded By — Limits search results to evidence uploaded by the user specified. To specify the user, click in the Uploaded By box, start typing the name of the user, wait for the system to show the matching users, and then click the user you want.***

Status — Limits search results to evidence whose status matches the status selected. By default, evidence searches are limited to evidence with a status of Active.

- ***Tag — Limits search results to evidence whose tags includes the characters you enter in the Tag box. For more information, see Text Search Details.***
- ***Group — Limits search results to evidence owned by members of the group specified. To specify the group, click in the Group box, start typing the name of the group, wait for the system to show the matching groups, and then click the group you want.***
- ***Flagged — Limits search results to evidence whose flag status matches the flag status selected.***

Export Device Search Results

An agency administrator can easily search and manage the TASER devices assigned to their agencies. You can sort the search results based on column headings. For example, click the Error Status heading to sort the list based on the device's error status.

Users can generate reports using the current version of the following browsers:

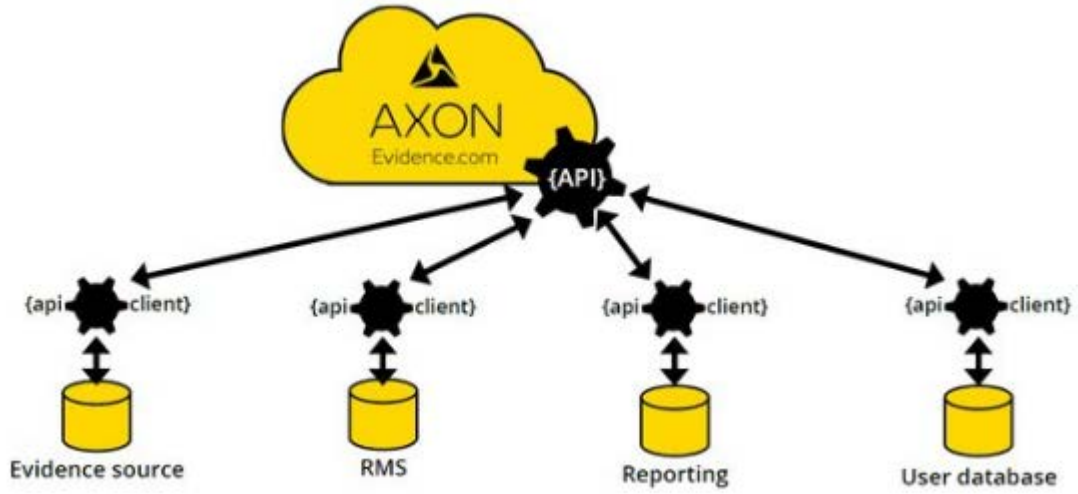
- ***Microsoft Internet Explorer***
- ***Google Chrome***
- ***Mozilla Firefox***
- ***Apple Safari***

<u>Evidence.com Application Program Interface</u>

The Evidence.com Partner API provides a programmatic means to access the data in your Evidence.com agency. By developing API-compliant client software or using third-party client software, you can use the Partner API to integrate your Evidence.com agency with other systems. An API client can request create, read, update, and delete operations on a variety of data resources:

- ***Users***
- ***Groups***
- ***Cases***
- ***Evidence***
- ***Devices***
- ***Reports***

By using the Partner API, you can address your agency's specific operational needs.



The API provides the means to achieve customized ends, such as the following scenarios:

- ***Integrate with New Technology — As law-enforcement and prosecutorial technology evolves and new digital evidence sources arise, agencies need assurance that their digital evidence management system (DEMS) can receive evidence and cases, regardless of the source. Facial and license-plate recognition, transcription services, and closed-circuit television integration are impending market demands. With the Partner API, you can add evidence from all these sources and others, manage evidence ownership, assign evidence to cases, and link to evidence from a records management system (RMS).***

- ***Integrate with Old Technology -- Even the best body-worn cameras and in-car systems require upgrades, maintenance, and eventually, replacements. Video evidence recorded on aging hardware must still be managed even as you roll out new hardware. The Partner API enables you to transition to an Axon solution with Evidence.com as your DEMS while continuing to use older hardware to the end of its lifespan.***

- ***Customize Reporting — When your agency needs to audit user behavior for policy compliance, such as timely application of critical metadata, the Evidence.com dashboard and reports may not***

support the precise need. Through the Partner API, you can retrieve the necessary user and evidence data and provide it to the application or system that will perform custom analysis in support of your policies.

Evidence.com allows users to fully customize reports through an API or through existing reports using services found in Microsoft Excel or other spreadsheet applications. Administrators can use the Reports API to retrieve report data, which they then can provide to other applications or systems as needed for reporting, analysis, or other needs. For example, you could provide the reporting data that you retrieve from the Reports API to a Tableau instance, Microsoft Excel, or a local database.

- ***Manage Users and Groups — When Evidence.com user accounts and their group memberships need to match those in another system, agencies need an automated synchronization method. Using the Partner API, you can create, update, and inactivate user accounts and groups, ensuring that your Evidence.com agency user and group configuration is in lockstep with your preferred central user repository.***

3.11.6 Video Storage

If cloud based, the storage facility must be located within the continental United States.

Yes. All primary servers and failover sites will be located in the United States.

3.11.6.1 Does your storage solution have the ability to upload video from multiple camera units simultaneously?

Yes. Evidence.com is a cloud-hosted digital evidence management solution provided as a service (SaaS) application. It is horizontally scalable and can elastically adapt to accommodate any traffic volumes. Internally, the solution uses a service oriented architecture where functionality is provided by discrete compassable services that can run on one or many servers. This allows individual components to scale to handle changes in traffic volumes.

The application is designed to support uploads from multiple users, devices, and locations, simultaneously from thousands of agencies across the United States. It is also possible for concurrent users to access the same video at the same time.

3.11.6.2 Storage solution should have the ability to view multiple linked videos simultaneously.

Yes. You can view multiple pages using separate browser sessions from within Evidence.com. Multi-video playback is available in the next firmware update and Evidence.com already supports it.

3.11.6.3 Solution should have two tier storage capacity for active video and long term storage needs as defined by the State.

Yes. As part of the Axon commitment to provide our customers a true SaaS offering, TASER is leveraging the cloud platform to offer your agency unlimited, highly available storage for Axon captured assets. This allows your agency instantaneous access to all of your body- worn camera evidence for a low, predictable cost without having to manage archived data.

<u>Evidence Retention Policy</u>
For proper management, NHP should create a set of agency-specific categories large enough to properly segregate evidence by type for retention setting and search functionality. This list should not be so large that it becomes an impediment to efficient field use by Users. Agencies are encouraged to consult their State Retention Schedules, City/County or State Attorneys or other legal counsel for guidance on proper retention setting.

The evidence retention policy determines:

1. ***Whether the system will initiate automatic deletion of evidence assigned to the category.***
2. ***How long the system waits before initiating the deletion of evidence that is not included in a case. Axon video deletions are based on the recording date. Deletion of all other evidence is based on the upload date.***

3.11.6.4 Does proposed solution offer storage options for 'unlimited storage' of body camera video evidence?

Yes. Unlimited storage is included in the proposed pricing.

3.11.6.5 Does your system provide a method to upload videos, via an access point? Please describe your process.

The Axon Body 2 is equipped with Wi-Fi 802.11n at 5 GHz and 2.4 GHz. In 2017, this connectivity will be enhanced to enable the Axon Body 2 to automatically offload videos when pre-configured Wi-Fi network are available.

3.11.6.6 Is your system compatible with an EnGenius ENS500EXT access point?

Yes, our Axon Fleet solution meets this requirement since our preferred band is 5GHz. The Axon Body 2 is equipped with Wi-Fi 802.11n at 5 GHz and 2.4 GHz. In 2017, this connectivity will be enhanced to enable the Axon Body 2 to automatically offload videos when pre-configured Wi-Fi network are available.

3.11.6.7 Does solution have the ability to maintain and export audit trail along with video?

Yes. The detailed Evidence Audit Trail can be used to determine compliance with chain of custody regulations. All content uploaded to Evidence.com is paired with an audit trail indicating every action applied to that evidence and its metadata. Information such as viewed by, downloaded by, and deleted by, is all included in the audit trail, in addition to the source IP Address of the person who made the change. All audit trails can be exported to a PDF document.

To ensure a robust chain of custody, evidence can be verified for authenticity by matching the SHA hash of original file ingested in Evidence.com with the copy. The original data associated with a video is never changed. All modifications are handled by creating new, derivative files. Detailed audit logs track all evidence access.

A detailed audit trail for every action in Evidence.com is retained in perpetuity even after the asset has been purged from the system. Even if evidence is deleted, or a user is deactivated, all audit trails/user information are retained intact and indefinitely.

3.11.6.8 Define maximum storage capacity, if any.

Not applicable. Unlimited storage is available through Evidence.com.

3.11.6.9 Describe the capability of proposed solution to provide the State with the ability to export/download and migrate original recordings with all metadata to other storage media or, local storage inclusive of all metadata and chain of custody information.

Users can download multiple evidence files at a time. After selecting files for download, the user receives an email with a download link to a single file containing all of their requested evidence. Metadata will be maintained if the footage is exported into another media form (DVD, streaming, etc.) The system supports the following file types for the download file:

- ***ZIP — The system includes the selected evidence files in a ZIP file.***
- ***ISO — The system includes the selected evidence files in an ISO image, which can be used to create a CD-ROM or DVD.***

Once downloaded, users can store the files in the location of their choosing (DVD, CD, flash drive, storage media, local storage, etc.).

3.11.6.10 Describe archival, hot and cold cloud storage solutions.

Not applicable. Evidence.com is a cloud-based repository offering unlimited storage.

3.11.6.11 Describe archival solutions for server storage, if applicable.

Not applicable. Evidence.com is a cloud-based repository.

3.11.6.12 Discuss different cost savings as defined by various storage solutions (active vs. long-term storage of files).

As part of the Axon commitment to provide our customers a true SaaS offering, TASER is leveraging the cloud platform to offer your agency unlimited, highly available storage for Axon captured assets. This allows your agency instantaneous access to all of your body- worn camera evidence for a low, predictable cost without having to manage archived data.

3.11.6.13 Describe capability to respond to requests to pull video from 'cold cloud storage', including time required to download video from storage.

Not applicable. As part of the Axon commitment to provide our customers a true SaaS offering, TASER is leveraging the cloud platform to offer your agency unlimited, highly available storage for Axon captured assets. This allows your agency instantaneous access to all of your body- worn camera evidence for a low, predictable cost without having to manage archived data.

3.11.6.14 Describe your solution to upload video in the rural areas that only have a maximum broadband speed of 1.5 Mbps

We provide multiple ways to upload videos: direct via LTE, Wi-Fi at the station, or removing the camera and placing it in a dock. These methods of offloading can be mixed and matched to resolve

bandwidth challenges. The videos can be offloaded via LTE as the vehicle is in the field as long as there is an LTE connection. For Wi-Fi offload at the station, we will allow the videos to be offloaded rapidly from the vehicle to a local server. That server will then upload video to Evidence.com via the allotted broadband speed over time.

3.11.7 System Security

3.11.7.1 The VMS shall meet the minimal security requirements for the Criminal Justice Information Services (CJIS) Policy. In particular, the VMS shall comply with Policy Areas 2 through 13 in Section 5 of the CJIS Policy. The CJIS Policy can be viewed by accessing the following link: https://www.fbi.gov/about-us/cjis/cjis-security-policy-resource-center

Complies. Please see Tab IX, B. Axon CJIS Compliance.

A. Will access to Criminal Justice Information (CJI) within a cloud environment fall within the category of remote access? (Section 5.5.6 Remote Access found in the above link)

Complies. Please see Tab IX, B. Axon CJIS Compliance.

5.5 - Policy Area 5: Access Control

5.5.1 – Account Management	***TASER International maintains account management policies and practices for Evidence.com, including quarterly account validation.***
5.5.2 – Access Enforcement	***TASER International maintains account management practices and access control policies for Evidence.com to ensure access is limited to authorized accounts.***
5.5.2.1 – Least Privilege	***TASER International access controls for Evidence.com are designed according to the principle of least privilege.***
5.5.2.2 – 5.5.5: System Access Control; Access Control Criteria; Access Control Mechanisms; Unsuccessful Login Attempts; System User Notification; Session Lock	***Evidence.com access control mechanisms are maintained in compliance with the specific CJIS security requirements.***
5.5.6 – Remote Access	***TASER International maintains policies and practices for Evidence.com that limit remote access to only required individuals, via managed VPN connections requiring 2-factor authentication.***
5.5.6.1 – Personally Owned Information Systems	***TASER International maintains requirements for the use of personally owned devices.***
5.5.6.2 – Publically Accessible Computers	***Evidence.com back-end system administration is prohibited from public access computers.***

3.11.7.2 Will advanced authentication (AA) be required for access to CJI within a cloud environment (Section 5.6.2.2 Advanced

Authentication, 5.5.2.2.1 Advanced Authentication Policy and Rationale found in the link under 3.11.7.1)

Complies. Please see Tab IX, B. Axon CJIS Compliance.

5.6 - Policy Area 6: Identification and Authentication

5.6.1 – Identification Policy and Procedures	***TASER International maintains policies and practices for Evidence.com for identifying and authenticating users before allowing access.***
5.6.1.1 – 5.6.2: Use of Originating Identifiers in Transactions and Information Exchanges; Authentication Policy and Procedures	***Not applicable to Evidence.com security practices.***
5.6.2.1 – 5.6.2.1.2: Standard Authenticators; Password; Personal Identification Number (PIN)	***Evidence.com authentication mechanisms are maintained in compliance with the specific CJIS security requirements.***
5.6.2.2 – 5.6.2.2.2: Advanced Authentication; Advanced Authentication Policy and Rational; Advanced Authentication Decision Tree	***Evidence.com requires at least 2-factor authentication for all system administration access. Additionally, advanced authentication is available for customer accounts.***
5.6.3 – 5.6.3.2: Identifier and Authenticator Management; Identifier Management; Authenticator Management; Assertions	***TASER International maintains policies and practices for Evidence.com for Identifier and Authenticator management.***
5.6.4 - Assertions	***TASER International utilizes a combination of internal and trusted external certification authorities for validating individual identities. Certificates are issued internally through an internal trusted authority. For external access, commercial CA's are used. Private keys and certificates are stored and distributed securely.***

3.11.7.3 Does your cloud service provider's datacenter(s) used in the transmission or storage of CJI meet all the requirements of a physically secure location? (Section5.9.1 Physical Secure Location found in the link under 3.11.7.1)

Complies. Please see Tab IX, B. Axon CJIS Compliance.

5.9 - Policy Area 9: Physical Protection

5.9.1.1 – Security Perimeter	***Evidence.com defines and controls the physically secure perimeter.***
5.9.1.2 – Physical Access Authorizations	***TASER International ensures physical access is limited to authorized personnel.***
5.9.1.3 – Physical Access Control	***TASER International ensures physical access is limited to authorized personnel, including the use of Iris and RFID access control systems at TASER facilities.***
5.9.1.4 – Access Control for Transmission Medium	***TASER International protects access to transmission lines.***
5.9.1.5 – Access Control for Display Medium	***TASER International controls display medium to prevent unauthorized viewing of CJI.***

5.9.1.6 – Monitor Physical Access	***TASER International maintains policies and practices for monitoring physical access, and responding to suspicious events.***
5.9.1.7 – Visitor Control	***TASER International maintains policies and practices for controlling visitor access.***
5.9.1.8 – Delivery and Removal	***TASER International maintains policies and practices for controlling information system-related items.***
5.9.2 – Controlled Area	***TASER International maintains policies and practices for Evidence.com related to physical protection.***

3.11.7.4 Are the encryption requirements being met? (Section 5.10.1.2 Encryption found in the link under 3.11.7.1)

Please. Please see Tab IX, B. Axon CJIS Compliance.

5.10.1.2 – Encryption	***Evidence data transmitted and stored in Evidence.com is encrypted with 128 bits or stronger. FIPS 140-2 approved encryption ciphers (or stronger) are used, including AES 256, and RSA 2048.*** ***TASER International maintains policies and practices for Evidence.com for encryption key and certificate management.***

3.11.7.5 Who will be providing the encryption as required in the CJIS Security Policy? (Client or cloud service provider)

TASER International maintains policies and practices for Evidence.com for encryption key and certificate management Please see Tab IX, B. Axon CJIS Compliance.

3.11.7.6 Is the data encrypted while at rest and in transit?

Yes. Evidence.com uses strong encryption to protect evidence data in transit and at rest.

- ***Data in Transit - Evidence data is encrypted during transfer: SSL with RSA 2048 bit key, 256 bit ciphers, TLS 1.0-1.2, Perfect Forward Secrecy***
- ***Data at Rest - Evidence data is encrypted in storage: 256-bit Advanced Encryption Standard (AES-256)***

3.11.7.7 What are the cloud service provider's incident response procedures? (Section 5.3 Policy Area 3: Incident Response found in the link under 3.11.7.1)

5.3.1 – Reporting Information Security Events	***TASER International maintains comprehensive security incident response plans for Evidence.com include reporting to appropriate parties.***

5.3.2 – Management of Information Security Incidents	***TASER International maintains security incident response policies and practices for Evidence.com.***
5.3.2.1 – Incident Handling	***TASER International maintains security incident response procedures and capabilities for Evidence.com.***
5.3.2.2 – Collection of Evidence	***The TASER International security incident response practices for Evidence.com include requirements to collect and maintain appropriate evidence, when necessary.***
5.3.3 – Incident Response Training	***The TASER International security awareness training for Evidence.com includes security incident response roles and responsibilities, including reporting expectations.***
5.3.4 – Incident Monitoring	***TASER International documents and tracks security incidents for Evidence.com and maintains such documentation to meet this requirement.***

3.11.7.8 Will the cloud subscriber be notified of any incident?

Yes, TASER International maintains comprehensive security incident response plans for Evidence.com including reporting to appropriate parties.

3.11.7.9 If CJI is compromised, what are the notification and response procedures?

TASER International maintains comprehensive security incident response plans for Evidence.com including reporting to appropriate parties.

3.11.7.10 Is the cloud service provider a private contractor/vendor?

TASER acknowledges and abides by all aspects of the CJIS Security Addendum. The CJIS Security Addendum is included by reference in the TASER MSPA which contractually commits TASER to the CJIS Security Policy requirements. CJIS Security Addendum Certification pages are maintained for each authorized TASER employee and are available to customers.

TASER International maintains policies and practices for ensuring all Evidence.com personnel are trustworthy and competent to handle sensitive data and systems. Authorized TASER personnel are available for state of residence and national fingerprint-based record checks at either the state or local level.

3.11.7.11 If so, they are subject to the same screening and agreement requirements as any other private contractors hired to handle CJI. (Section 5.1.1.5 Private Contractor User Agreements and CJIS Security Addendum; 5.12.1.2 Personnel Screening for Contractors and Vendors found in the link under 3.11.7.1)

TASER acknowledges and abides by all aspects of the CJIS Security Addendum. The CJIS Security Addendum is included by reference in the TASER MSPA which contractually commits TASER to the CJIS Security Policy requirements. CJIS Security Addendum Certification pages are maintained for each authorized TASER employee and are available to customers.

TASER International maintains policies and practices for ensuring all Evidence.com personnel are trustworthy and competent to handle sensitive data and systems. Authorized TASER personnel are available for state of residence and national fingerprint-based record checks at either the state or local level.

3.11.7.12 Will the cloud service provider allow the CSA and FBI to conduct compliance and security audits? (Section 5.11.1 Audits by the FBI CJIS Division; 5.11.2 Audits by the CSA found in the link under 3.11.7.1)

Yes. TASER International adheres to the audit requirements of the FBI CJIS Security Policy.

3.11.7.13 The State may verify that Contractor is in compliance with CJIS by requesting a compliance audit of Contractor's technology deployment through the CJIS Systems Agency to the Federal Bureau of Investigation (FBI). The FBI CJIS Division shall perform the requested audit to verify compliance. 140-2.

TASER International adheres to the audit requirements of the FBI CJIS Security Policy.

3.11.7.14 System shall provide full conformance to Federal Information Processing Standards (FIPS) Publication.

Evidence data transmitted and stored in Evidence.com is encrypted with 128 bits or stronger. FIPS 140-2 approved encryption ciphers (or stronger) are used, including AES 256, and RSA 2048. TASER International maintains policies and practices for Evidence.com for encryption key and certificate management.

3.11.7.15 VMS shall provide user authentication with a unique username and password.

Yes. Each agency has a unique URL. All users in your Evidence.com agency must have unique email accounts and each user should have a unique Evidence.com account.

Password settings for all users in the agency are defined and configured within Evidence.com.

- ***Password Length — Determines how short passwords can be. [default 8, min 6]***
- ***Passwords Complexity — System and application administration requires 9 character passwords and contain at least three of the four character categories (Upper letter, Lower letter, Number, Symbol).***
  Step-up authentication is performed using a one-time, six-character code delivered out-of-band to a previously authenticated device.
- ***Password History — Unique new passwords a user must use before an old password can be reused. [default 10, min 1, max 25]***
- ***Password Aging — Determines how many days a password can be used before the user is required to change it. [default 90, min 7, max 365]***
- ***Customizable Failed Login Limit — Number of failed login attempts before the account is locked out. [default 5, min 1, max 25]***
- ***Failed Login Limit Lockout duration — Number of minutes a user is locked out of their account due to failed login attempts. [default 60, min 1, max 720]***
- ***Lockouts occur for increasingly longer periods of time starting with five minutes after five unsuccessful log in attempts.***

Evidence.com also includes the following features to provide robust access control.

- ***Enforced session timeout settings during idle periods***
- ***Mandatory challenge questions when authenticating from new locations***
- ***Multi-factor authentication options for user login and prior to administrative actions (one time code via SMS or phone call-back)***
- ***Role-based permission management***
- ***Device-level permission management (for example, allow specific users to use the web-based interface, but not the mobile application)***
- ***Restrict access to defined IP ranges (limit access to approved office locations)***
- ***Detailed, tamper-proof administrator and user activity logging***

3.11.7.16 VMS will allow for authorized users to be established based on various roles and permissions by the System Administrator.

Yes. Each Evidence.com user is assigned a role. Roles determine a user's permissions, which control levels of access to features and functions in Evidence.com. Information access via Evidence.com is controlled through a robust "Access Control System" managed by the Administrator and that features comprehensive audit trails. Access to information is governed by the agency-defined access control system built into Evidence.com. Access is controlled according to:

- ***Pre-defined roles***
- ***Pre-defined individuals (i.e., who has access to what data feed)***
- ***User account-specific passwords***

Each Evidence.com user is assigned a role; roles determine user permissions, which control access to features and functions. The following table provides information about each permission supported by Evidence.com.

Permissions Supported by Evidence.com	***Description***
Login Access	
Evidence.com	***Allows a user to log in to their agency's Evidence.com agency.***
Evidence Sync	***Allows a user to log in to Evidence Sync in Online mode.***
Evidence Mobile	***Allows a user to log in to the Axon Capture or Evidence Mobile application.***
User Account	
Edit Account Information	***Allows a user to change their own account information, including their Name, Badge ID, Phone, Email Address, Password, Security Questions, or Email Settings. If you change the User Administration permission to Allowed, this permission is automatically set to Allowed.***
View & Compose User Messages	***Allows a user to read and send messages to other users.***
Download Sync Software	***Allows a user to download Sync software from their Evidence.com agency.***
Create/Edit Group	***Allows a user to create a group, and edit its monitors and members.***
Group Audit Trail PDF	***Allows a user to view an audit trail of the activities related to a group.***
Admin Access	
Configure Agency Security Settings	***Allows a user to edit the agency's IP Restrictions, authentication method, password configurations, and partner agencies.***
Edit Agency Settings	***Allows a user to configure agency wide settings including Categories and Retention, Video and Camera Settings, Roles and Permissions, and Password Configuration requirements.***
Edit Device Offline & Microphone Settings	***Allows a user to configure the agency-wide settings for the Axon cameras default Microphone Setting and whether or not they can be turned to Offline Mode.***
Device Administration	***Allows a user to reassign all agency devices, change their settings, and upload any CEW logs.***
User Administration	***Allows a user to add, remove and edit the accounts of other users, including their role, personal information, contact information, and reset their credentials (password and security questions).***
Category Administration	***Allows a user to add a Category to the agency's list or edit an existing Category***
Generate Reports	***Allows a user to generate reports.***
Search Access	
User Search	***Allows a user to see what users are in the agency. If disabled the user will be unable to see any evidence or devices assigned to others, assign devices or evidence to others, share evidence or cases, or send messages to others.***

Permissions Supported by Evidence.com	*Description*
Partner Contact Search	*Allows a user to view members of partner agencies that have been added to your agency's contact list* *Unlocks: Share Externally to Authenticated Users, Share With Partner Agencies*
Evidence Search	*Allows a user to search for all of the Evidence in the agency. Note: the user can only access the Evidence specified under the Evidence Management permissions.*
Device Search	*Allows a user to search for all of the Devices in the agency.*
Case Search	*Allows a user to search for all of the Cases in an agency. Note: Their ability to access a Case is determined by the Case Management Permissions.*
Evidence Creation	
Upload External Files	*Allows a user to upload files through Evidence Sync, Axon Capture, Evidence Mobile, and the Import Evidence feature. This does not affect the ability to upload through an ETM or Evidence.com Dock.*
Configure Automatic Upload through Evidence Sync	*Allows a user to configure Automatic Upload through Evidence Sync.*
Evidence Management	
View	*Allows a user to access evidence. Does not include weapon firing logs.*
View CEW Firing Logs	*Allows a user to view weapon firing logs.*
Edit	*Allows a user to change the Title, ID, Flag, Assignment, Category, Tags and Location.*
Add/Remove Pending Review Category	*Allows a user to add or remove the Pending Review Category from a piece of Evidence.*
Redact	*Allows a user to create redactions of video evidence files. This does not alter the original video in any way.*
Reassign	*Allows a user to change the owner of an evidence file.*
Delete Evidence & Edit Date Recorded	*Allows a user to manually initiate the deletion of Evidence before its Category determined date.*
Download	*Allows a user to download Evidence.*
Share	*Allows a user to allow other users to have access to Evidence.*
Share Externally to Authenticated Users	*Allows users to provide individuals outside of your agency with access to evidence. These external users are required to sign in to their Evidence.com account to view the shared evidence, and their actions are shown in your agency's audit logs. If they do not have an Evidence.com account, they can create a free guest account on my.evidence.com.*
Share External Download Links	*Allows users to send an email containing a download link to individuals outside of your agency. This link does not require the recipient to sign in to an Evidence.com account or even to have an Evidence.com account. Only the apparent IP address of the computer downloading the file appears in your agency's audit logs.*

Permissions Supported by Evidence.com	*Description*
Post Notes	*Allows a user to write messages associated with Evidence.*
Audit Trail PDF	*Allows a user to view and download the record of who has Viewed or Edited Evidence.*
Restricted Category Access	*Allows a user to access Evidence that has been categorized as Restricted Access.*
Case Management	
View	*Allows a user to access a Case*
Edit	*Allows a user to Edit Case ID, Description, Categories, Tags, and Folder Structure.*
Reassign	*Allows a user to change the Owner of a piece of a Case.*
Share	*Allows a user to add members to a Case, giving them access to the associated Evidence.*
Share with Partner Agencies	*Allows users to send cases to a partner agency. After the partner agency accepts the case, the evidence in the case is copied to the partner agency and no further actions by the partner agency are shown in your agency's audit logs.*
Share External Download Links	*Allows users to send an email containing a download link to individuals outside of your agency. This link allows recipients to download all of the evidence in the case. Using the link does not require recipients to log in to an Evidence.com account or even to have an Evidence.com account. Only the apparent IP address of the computer downloading the file appears in your agency's audit logs.*
Audit Trail PDF	*Allows a user to view and download the record of who has Viewed or Edited a Case.*
View & Add Case Notes	*Allows a user to write messages associated with a Case.*
Create Case	*Allows a user to create a Case.*
Restricted Category Access	*Allows a user to access Cases that have been categorized as Restricted Access.*
Shared Case	
View	*Allows users to access a Case that has been Shared with them.*
Edit	*Allows users to Edit Case ID, Description, Categories, Tags, and Folder Structure of a Case that has been shared with them.*
Reassign	*Allows a user to reassign a Case that has been Shared with them.*
Share	*Allows users to add members to a Case that has been shared with them, giving access to the associated Evidence.*
View & Add Case Notes	*Allows users to write messages associated with a Case that has been Shared with them.*
Audit Trail PDF	*Allows users to view and download the record of who has Viewed or Edited a Case that has been shared with them.*
Email Notification Preferences	
Account Lockout Notification	*Determines whether or not a user will receive Account Lockout Notifications when any user in the agency is locked out.*
Upcoming Evidence Deletion Notification	*Determines whether or not a user will receive weekly notifications of any upcoming evidence deletions in the agency.*

Permissions Supported by Evidence.com	*Description*
Evidence Timestamp Notification	*Determines whether or not a user will receive weekly notifications of evidence whose timestamp indicates it is older than 14 days.*

3.11.7.17 VMS will offer optional IP access restriction and security challenge questions upon access from an unknown or previously used location.

Yes. Multi-factor authentication options can be enabled for user login and prior to administrative actions (via a SMS to the user's cell phone, or a call back to authenticating from new locations).

Access can also be restricted to defined IP ranges. Security challenge questions are required when authenticating from new locations. Access can be restricted to defined IP ranges (i.e. limiting access to approved office locations). These options are agency configurable, so a NHP administrator can enable and configure per agency policy.

<u>Reset Passwords and Security Questions</u>
When you reset a user's password and security questions, Evidence.com sends the user an email with information about the change and a temporary password that allows the user to sign in, change the password, and specify new security questions.

<u>Mobile Phone Advanced Authentication</u>
By enabling Mobile Phone Advanced Authentication, agency administrators can add a layer of security to their Evidence.com agencies.

This requires users to have access to their mobile phone as well as their username and password when they sign in. This means that if someone steals or guesses their password, the potential hijacker still cannot sign in to their account because they do not have their phone.
This authentication is also required for critical actions. For example, you are prompted to answer your security questions when you attempt any of the following actions:

- ***Deleting evidence***
- ***Assigning evidence to a category with a lower retention policy***
- ***Deleting a case***
- ***Assigning a case to a category with a lower retention policy***
- ***Changing a category retention policy***
- ***Deactivating a user***
- ***Changing a user's role***
- ***Changing a role's permission***
- ***Adding or deleting IP addresses or IP address ranges***
- ***Disabling IP restrictions***
- ***Disabling Dual Factor Authentication***
- ***Enabling or disabling any of the Security Settings***
- ***Creating categories***

When you answer the questions, the authentication is not required for the number of minutes specified in the Code Request Frequency field on trying any of the above actions.

3.11.7.18 Any access to stored video shall be maintained in an automatic log or audit trail showing users that have viewed, shared or copied video to an external source (e.g. CD/DVD, local storage, etc.), and the audit trail should be capable of being exported.

Yes. The detailed Evidence Audit Trail can be used to determine compliance with chain of custody regulations. All content uploaded to Evidence.com is paired with an audit trail indicating every action applied to that evidence and its metadata. Information such as viewed by, downloaded by, and deleted by, is all included in the audit trail, in addition to the source IP Address of the person who made the change. All audit trails can be exported to a PDF document.

To ensure a robust chain of custody, evidence can be verified for authenticity by matching the SHA hash of original file ingested in Evidence.com with the copy. The original data associated with a video is never changed. All modifications are handled by creating new, derivative files. Detailed audit logs track all evidence access.

3.11.7.19 Log activities performed by specific user ID, IP address and time/date stamp all activities.

Yes. The User Audit Trail shows many of the actions taken by a user in addition to changes to the user's account. It does not show activities related to devices, evidence, or cases.

User Audit Trails are available in the following formats.

1. ***PDF format — Well suited for use in court.***
2. ***Comma-separated values (CSV) format — Supported by spreadsheet applications such as Microsoft Excel and helpful for simplifying reporting and integration with other systems.***

The Evidence.com auditing functionality provides the source IP Address of all actions. Location can be associated with uploaded content, and can be viewed on Evidence.com. In addition to evidence-related user actions, the User Audit Trail provides the following information:

- ***Failed login attempts will be entered into the user's individual audit trail and show the IP address.***
- ***When a user is locked out of their account due to multiple failed login attempts the user's audit trail will show the IP address of the computer that attempted logging in.***
- ***When a user's password has been reset or their account has been unlocked the audit trail will show the username, first and last name, and badge ID of user who has taken that respective action.***

Evidence-related user actions that appear in user audit trails include the following:
- ***View evidence***
- ***Watch video evidence***
- ***Initiate evidence deletion***
- ***Restore deleted evidence***
- ***Upload evidence***
- ***Add or edit evidence title***
- ***Add or edit evidence ID***
- ***Add or edit categories assigned to evidence***
- ***Add or edit evidence location***
- ***Edit evidence recorded date and time***

- ***Extend evidence retention period***
- ***Flag or un-flag evidence***
- ***Share evidence internally (with users in your Evidence.com agency)***
- ***Share evidence externally (with users outside your Evidence.com agency)***
- ***Add or edit evidence tags***
- ***Add or edit evidence description***
- ***Add, edit, or remove evidence notes***
- ***Reassign evidence***
- ***Add evidence to a case***
- ***Add a marker***
- ***Download a marker***
- ***Add a video clip***
- ***Add video redaction***

Case-related user actions that appear in user audit trails include the following:

- ***Create case***
- ***Viewed case***
- ***Add evidence to a case***
- ***Remove evidence from a case***
- ***Share case by download link***
- ***Share case with partner agency***
- ***Share case with user in your agency (add member to case)***
- ***Download case***
- ***Add or remove folder***
- ***Add or edit categories assigned to case***
- ***Edit case title***
- ***Add or edit case description***
- ***Add, edit, or delete case notes***
- ***Add or remove case tags***

3.11.7.20 System Administrators shall have the ability to administratively manage accounts and assign rights and permissions to system users.

Yes. Each Evidence.com user is assigned a role. Roles determine a user permissions, which control levels of access to features and functions in Evidence.com.

Information access via Evidence.com is controlled through a robust "Access Control System" managed by the Administrator and features comprehensive audit trails.

Access to information is governed by the agency-defined access control system built into Evidence.com. Access is controlled according to:
- ***Pre-defined roles,***
- ***Pre-defined individuals (i.e., who has access to what camera feed),***
- ***User account-specific passwords.***

Administrators assign the roles and actions of all users and create individual user accounts with varying degrees of access, i.e. administrative accounts, basic user accounts, etc. Account administrators can customize the roles and authorization levels of each account user, or what they are

permitted to do. This functionality was created to preserve chain of custody and to clarify what each user is permitted to do.

Administrators can allow or prohibit a user access to specific features and functions depending on the level of access granted to the user(s). You can restrict access to the following functions, but this is not a complete list:

- ***Edit Account Information***
- ***View & Compose User Messages***
- ***Download Evidence Sync Software***
- ***Configure IP Restrictions***
- ***Edit Agency Settings***
- ***Edit Device Offline & Microphone Settings***
- ***Device Administration***
- ***User Administration***
- ***Category Administration***
- ***Generate Reports***
- ***User Search***
- ***Evidence Search***
- ***Device Search***
- ***Case Search***
- ***Upload External Files***

Agencies can create a unique role for those who will have sole access to highly sensitive event recordings. Typically this role will be reserved for the Agency head, executive or command staff or professional standards/internal affairs staff. If you choose to create a restricted category, consider the workflow instruction for who will be responsible and when your field supervisory staff will be required to categorize evidence as "Restricted".

3.11.7.21 VMS shall provide ability to set an unsuccessful access attempt limit and suspend IDs after reaching the unsuccessful access threshold.

Yes. When a user attempts and fails to sign in to Evidence.com more times than are allowed by the agency's security settings, the user is locked out of Evidence.com. Configuring password settings allows Administrators to select a failed login limit.

3.11.7.22 VMS shall provide ability to send alerts to System Administrators for unauthorized access attempts.

Yes. When a user attempts and fails to sign in to Evidence.com more times than are allowed by the agency's security settings, the user and the administrator is locked out of Evidence.com and receives the message, "Too many failed login attempts. Account temporarily suspended."

3.11.7.23 VMS shall enable automatic logoff of ID after a defined period of session inactivity, and perform subsequent re-log-on password authentication.

Yes. An administrator can set up a timeout or suspend users after an idle period. The user will then be required to re-enter their password before continuing.

3.11.7.24 VMS shall provide ability to configure password parameters such as password lengths, user access to expiration settings and other behaviors, enabling alphanumeric characters, etc.

Yes. Using the configure password settings feature in Evidence.com. This feature enables administrators to define password settings for all users in the agency.

- ***Password History — Unique new passwords a user must use before an old password can be reused. [default 10, min 1, max 25]***
- ***Password Aging — Determines how many days a password can be used before the user is required to change it. [default 90, min 7, max 365]***
- ***Password Length — Determines how short passwords can be. [default 8, min 6]***
- ***Failed Login Limit — Number of failed login attempts before the account is locked out. [default 5, min 1, max 25]***
- ***Lockout Duration — Number of minutes a user is locked out of their account due to failed login attempts. [default 60, min 1, max 720]***

3.11.7.25 VMS shall provide ability to lock out user or group ID.

Yes. An administrator can lock out a user or group.

3.11.7.26 Vendor will provide a detailed explanation of data security standards, to include but not limited to: defining the physical environment, location of all host servers; protections against natural and man-made disasters; encryption; transfer; storage; redundancy and recovery of files.

Yes. For customers residing in the, United States TASER will ensure that all content stored in Evidence.com remains within the United States including any backup data, replication sites, and disaster recovery sites.

Evidence.com customer data is stored within Microsoft Azure Government data centers located in Boydton, VA and Des Moines, IA. Each data center offers world-class security and system protection. Data centers employ backup power, climate control, alarms, and seismic bracing.

In the event of a disaster, the system will failover automatically to the secondary site and provide uninterrupted service to customers, providing uninterrupted access during disaster events.

The Axon solution will provide maximum security against data loss using industry best practices and minimize, if not eliminate any possible interruption to service:

- ***Multiple Locations - Each Evidence.com region is comprised of multiple, isolated locations and all Evidence.com application components are duplicated across all these locations for a fully redundant, Hot/Hot failover, infrastructure***

- ***Highly Available - Evidence.com is spread across isolated locations, and all components (e.g. databases, web servers) are further backed up daily to a highly available and durable storage location to support a Hot/Cold failover and recovery objective.***

- ***Automatic Failover - No human intervention is required in the event of a primary data center failure.***

- ***Active-Active Topology - Because the solution was designed from the start to run as a highly-available application, it is equipped to handle a wide range of failures in the underlying infrastructure. The active-active design means that computing resources are efficiently utilized, no resources are wasted on "standby" servers.***

- ***Commodity Hardware - No special systems required for high-availability.***

- ***Local Replication – the application also makes its easy, should the NHP wish, to keep local copies of certain content. The application provides "Bulk Download" functionality.***

3.11.7.27 Describe security standards for hardware (cameras) in place to prevent data from being accessed in the event a camera is lost or stolen.

Video content encoded onto the camera is not encrypted since the storage card is non-removable. An officer cannot delete, alter or edit, the videos; he or she can only change the metadata. The integrity of the original data can never be altered.

For example, the user can edit an hour-long video into the 10-minute portion needed, but the hour long video retains its original integrity. Encryption only takes place when video content is uploaded to Evidence.com.

Evidence.com uses strong encryption to protect Evidence data in transit and at rest.

- ***FIPS 140--2 approved encryption ciphers (or stronger)***
- ***Robust SSL/TLS implementation for data in transit.***
  - ***RSA 2048 bit key***
  - ***TLS 1.2 with 256 bit connection***
  - ***Perfect Forward Secrecy***
- ***256 bit AES encryption for evidence data in storage***

All Axon video data is securely stored on a solid-state, non-removable, embedded Multimedia Card (eMMC) inside the Axon device. Rather than using an SD card, the media is populated directly on the circuit board, providing several levels of physical and virtual security.

Level 1: Non-standard connection & sealed compartment
The Axon Body 2 uses a non-standard connection, thus preventing access to the storage without destruction of the device.

Level 2: eMMC Storage
eMMC storage is populated on the circuit board rather than using an SD card. Accessing and reading eMMC is difficult and would require destruction and/or modification of the circuit board.

Level 3: No Partition Table
The storage media does not have a partition table and will show as an unreadable drive/card (under any operating system).

Level 4: Encryption

The data stored on the camera is secure and can be encrypted by means of 256-bit AES encryption. The camera does not allow any footage to be deleted, overwritten, or otherwise modified.

While the camera does not have an internal tracking device, the status of all devices can be seen while logged into an administrator account.

Device Searches index the following eight fields:

- ***Model - All Axon Cameras, Docks and CEWs***
- ***Serial Number***
- ***Device Status - Any, Active, Inactive, Stolen, RMA, Lost***
- ***Error Status - Any, Good, Minor, Major, Critical***
- ***Last Upload Data From***
- ***Last Upload Data To***
- ***Device Name***
- ***Device Assigned to***

3.11.7.28 Vendor will describe any previous loss of data occurring from criminal actions, as well as other issues that impact data integrity, such as unauthorized data access by contract personnel.

Not applicable. Please see Tab IX, B. Axon CJIS Compliance.

3.11.7.29 Provide a non-technical means for field personnel to remotely view stored video without altering original file (other than applying metadata to file).

For body worn video, officers can use Axon Mobile or Evidence Sync to view video that is still stored on the camera. Remote viewing is not currently available.

We allow field personnel and field officers to use the Axon View XL MDC application to play back videos before it is uploaded.

Evidence.com can also be accessed from the MDC as long as there is internet connectivity to view videos that have already been uploaded.

3.11.7.30 Describe ability of system to enforce password expiration.

Yes. Using the configure password settings feature in Evidence.com. This feature enables administrators to define password settings for all users in the agency.

- ***Password Aging — Determines how many days a password can be used before the user is required to change it. [default 90, min 7, max 365]***

3.11.7.31 Describe ability of system to limit concurrent sessions.

If a user successfully signs in from a different location while he or she is already signed in from one location, Evidence.com will display a message that the original session will be terminated.

3.11.7.32 Describe ability of system to log changes to administrative functions.

The Agency Audit Trail shows agency-wide changes to your Evidence.com account. This report helps provide transparency on administrative actions across Evidence.com. By displaying each action in detail, your agency is able to review who changed a setting, in order to understand the purpose and provide better accountability to each user. Only users with the "Edit Agency Settings permission" enabled can view the Agency Audit Trail. The audit trail logs the following Evidence.com changes:

- ***Device Default Ownership Policy Updated***
- ***Address Added***
- ***Address Updated***
- ***Admin Added***
- ***Admin Changed***
- ***Authentication Policy Updated***
- ***Partner Created***
- ***Default Retention Level Updated***
- ***Axon Body 2 Settings Updated***
- ***Axon Flex Settings Updated***
- ***Axon ATC Settings Updated***
- ***Device Settings Updated***
- ***X2 CEW Settings Updated***
- ***Dual Factor Authentication Policy Updated***
- ***Expire All Subscriber Passwords of Partner Agency***
- ***Partner Federation Entity Removed***
- ***Partner Federation Entity Updated***
- ***Federation Group Updated***
- ***Partner Federation Updated***
- ***Partner Federation Disabled***
- ***IP Address Policy Updated***
- ***IP Range Restriction Updated***
- ***IP Address Session Security Policy Updated***
- ***Password Policy Updated***
- ***Agency Deactivated***
- ***Agency Reactivated***

3.11.8 Information Security

3.11.8.1 Vendor shall encrypt transmission of confidential data when transferred through publicly accessible networks such as the Internet.

Complies.

3.11.8.2 Vendor shall ensure all transmission of information data files are transferred through a Secure Socket Layer (SSL), which creates a 128 bit encrypted connection which is password protected. All data files that are on Vendor's servers are encrypted once they have completed the upload and pre-process procedures.

Complies.

3.11.8.3 All input data transmitted across public networks (all networks other than the State's) shall be encrypted during transit and decrypted electronically during processing to produce non-confidential output data. The decrypted data shall not be accessible by vendor's employees unless otherwise limited on a "need to know" basis as determined by the Nevada Highway Patrol's designee.

Complies.

3.11.8.4 The System shall have a host-based firewall technology preventing inappropriate/ unauthorized access. Vendor shall provide the following:

A. All intrusion detection system monitoring for unauthorized access attempts.

Complies.

B. Must run anti-virus software.

Complies.

C. Monitor daily logs for potential intrusions, file integrity.

Complies.

D. Only allow access by uniquely assigned and auditable IDs.

Complies.

E. All data transfers and administrative access must be in an encrypted format.

Complies.

3.11.9 In-Car Video Integration

3.11.9.1 BWC must have the ability to record audio for the In-car video system.

Complies.

3.11.9.2 BWC must have the ability to activate recording off the In-Car video systems automatic triggers.

Complies.

3.12 IN-CAR VIDEO

The In-Car Video portion of this RFP is contingent upon funding anticipated to be approximately one (1) year from contract award. Vendors proposing In-Car Video must be compatible with proposed Body Worn Cameras.

3.12.1 Standard Specifications

3.12.1.1 All mobile video systems and related audio equipment must conform to the applicable minimum standards as set by the following: Electronic Industries Association (EIA);

Yes. Per the component based standards as set by EIA, Axon Fleet utilizes industry standard components, which meet all necessary standards for sale and use in the United States.

3.12.1.2 Federal Communications Commission (FCC) rules/ regulations;

Yes. The Axon Fleet solution is wholly FCC certified, the Axon Fleet camera FCC ID is X4GS00947.

3.12.1.3 Institute of Electrical and Electronic Engineers (IEEE);

Yes. Axon Fleet's communication interfaces are designed to IEEE 802.15.1 and IEEE 802.11 guidelines.

3.12.1.4 International Electro-technical Commission (IEC);

Yes. Axon Fleet is IEC 60529 and IEC55022 compliant.

3.12.1.5 International Organization for Standardization (ISO);

Yes. TASER products and services are ISO 9001:2008, ISO 27001:2013 ensuring the quality control and information security of the solution as a whole. Axon Fleet has been tested to and meets ISO 16750-2:2012, ISO 17215-1:2014, and ISO 13766:2006.

3.12.1.6 National Fire Protection International (NFPA);

Yes. The Axon Fleet solution meets the standards of safety for sale in the United States.

3.12.1.7 National Highway Transportation Safety Administration (NHTSA);

Yes. The Axon Fleet solution is engineered for safety and meets all the necessary standards for implementation in police vehicles. Please see the attached installation guide detailing the equipment that will be provided and installation instructions that are all in accordance with the current Federal Motor Vehicle Safety Standards (FMVSS).

3.12.1.8 Society of Automotive Engineers (SAE);

Yes. These standards will apply to vehicles themselves. Axon Fleet fully supports utilization in vehicles meeting these standards.

3.12.1.9 Underwriters Laboratories Inc. (UL); and

Yes. Axon Fleet batteries are UL 1642 compliant.

3.12.1.10 Vendors must provide documentation that validates that their systems adhere to the minimum specifications in the International Association of Chief of Police (IACP) Specifications for In-Car Video (dated 11/21/2008), and that the technology used is generally accepted in the relevant field.

The solution is still in beta and as such is undergoing the proper validation testing. The fleet solution will meet all necessary standards to ensure evidentiary integrity and admissibility in court.

3.12.2 Video System Specifications

3.12.2.1 The minimum acceptable components consist of the following parts:

A. Front camera;

Yes.

B. Back seat camera;

Yes.

C. Color LED monitor with audio;

Yes. If the vehicle doesn't have an MDT/MDC, Axon Fleet is still operational, but cannot be controlled with a visual interface.

D. Body worn camera must act as a wireless transmitter for audio with in-car & home charger;

Yes, however, the Axon Fleet system works in a different way. BWCs capture audio for in-car camera system and audio and video are synched automatically on evidence.com.

E. Covert secondary hard-wired microphone;

Yes. The microphones are contained within the cameras themselves.

F. Digital Video Recorder- DVR;

Yes. The camera contains the DVR.

G. Integrated GPS receiver and antenna;

No. We provide GPS and we will integrate with NHP's Feeney Wireless SkyusX in-car routers as long as the router has GPS data.

H. Collision sensor;
I. Controller center;
J. Means to transfer media data from In-car to storage solution;
K. Video viewer capability;
L. Hardware/software necessary to submit videos as evidence;
M. All mounts and cables for power, interfaces, cameras, and antennas;
N. Documentation;

O. Warranty and maintenance;
P. Training; and
Q. Shipping and handling.

Yes.

3.12.2.2 The digital video recorder (DVR) offered shall be in full commercial production. Prototypes will not be considered.

Yes.

3.12.2.3 Programming of the in-car recording system shall be restricted to authorized personnel only.

Yes.

3.12.2.4 All controls and indicators shall have adjustable backlighting.

Yes.

3.12.2.5 The officer shall have the option of recording primary, rear-facing, or both cameras simultaneously.

Yes.

3.12.2.6 A collision sensor covering 360 degrees, to trigger recordings, without requiring connection to the vehicles airbag system, shall be included. If a collision is detected, the video recorder (including pre-event memory) shall be automatically activated so the collision and video leading up to the collision is recorded.

Yes. We use the accelerometer in the cameras themselves to trigger recordings in the case of a crash.

3.12.2.7 The in-car digital video system shall be provided with all necessary cables and hardware (e.g. fuse holders, mounting brackets) required for installation.

Yes.

3.12.2.8 Each digital video recording system shall be supplied with a comprehensive installation/ programming/ operations manual. The

manual shall specify all brackets, hardware and mounting locations for installing camera systems.

Yes.

3.12.3 Digital Video Recorder (DVR)

3.12.3.1 The DVR shall mount in standard equipment consoles between the seats, or overhead.

Yes.

3.12.3.2 No permanent modifications shall be required to install the DVR system.

Yes.

3.12.3.3 The DVR system shall be capable of being installed as to not hinder the operation of the police unit.

Yes.

3.12.3.4 The DVR shall be capable of recording two video inputs from a powerful zoom, forward-facing camera, and a wide-angle rear-facing camera.

Yes. Axon Fleet offers two cameras per vehicle, one forward-facing and one rear-facing. Both cameras offer a 143 degree FOV.

The larger form factor of a zoom camera can obstruct visibility for the officer.

HD video allows for license plate legibility at approximately 20' - 30' from the vehicle.

When surveyed, many officers do not use the zoom function and would prefer a smaller camera that does not obstruct their line of sight out of the vehicle over a zoom camera.

3.12.3.5 The DVR shall provide a choice of at least one of the following upload options.

A. Wireless Ethernet- provided 802.11n base station includes encryption, supports multiple simultaneous uploads and is upwardly scalable. The system should be capable of comfortably uploading from multiple vehicles in the regional command centers (depicted in the scope of work section of this RFP) simultaneously. In addition, a backup upload system must be provided, should the wireless transfer system fail.

Yes.

B. Removable Hard Disc Drive (HDD) with provided hard drive docking stations that support plug and play hard drive insertion.

Yes, by removing cameras from the car since the cameras are the DVR.

C. Removable Compact Flash Device-Device with provided docking stations that support plug-and-play flash card insertion.

Yes, using TASER's Dock and Walk workflow. Storage is on the camera therefore it replaces the need for any additional hardware. Axon Fleet does not support plug-and-play, a user must upload to Evidence.com or he or she can playback video stored on the camera using the Axon Fleet XL MDT Application in the vehicle.

D. Cellular - Upload media via LTE connectivity that is compatible with the Feeney Wireless Skyus-X modem.

Yes.

E. If necessary, itemize and include the cost of media needed to allow officers the ability to rotate media between their vehicles and evidence technicians.

Not applicable. Each camera houses 64GB of non-removable storage.

3.12.3.6 The DVR shall have the ability to record up to 8 hours of video before reaching the capacity of the storage media at maximum resolution. For the recording media available, specify the recording and playback times, resolution, and MB per second.

Yes. The Axon Fleet video camera has a minimum video resolution of 480P and a maximum video resolution of 1080P. It utilizes an aspect ratio of 16:9 at 1080P and 720P and a 4:3 aspect ratio at 480P. The video resolution, the encoding bitrate, the frame rate and the video encoding format impact the size of the files captured at each setting. The Axon Fleet has 64GB of non-removable storage.

The Axon Fleet video camera has four video quality settings, Low SD, High SD, Low HD, High HD spanning 480P, 720P and 1080P video resolutions.

- ***The Low SD setting captures video at a 480P video resolution at a rate of .81 GB per 60 minutes of video. This allows for over 70 hours of recording***
- ***The High SD setting captures video at a 480P video resolution at a rate of 1.8 GB per 60 minutes of video. This allows for over 35 hours of recording***
- ***The Low HD setting captures video at 720P video resolution at a rate of 2.7 GB per 60 minutes of video. This allows for over 23 hours of recording***
- ***The High HD setting captures video at 1080P video resolution at a rate of 5.4 GB per 60 minutes of video. This allows for 11.3 hours of recording***

3.12.3.7 Video resolution, frame rates, and quality on the DVR shall be preset but can be changed by an administrator. These settings shall be independently configurable for recording modes of both video cameras. Please specify levels for:

A. video resolution

Yes. See response to question 3.12.3.6.

B. video frame rate

Yes. Axon Fleet records at 30 FPS; in policing situations, officers often deal with objects in motion. The higher frame rate results in smoother video, resulting in a clearer, more functional piece of evidence.

C. video quality

Yes. See response to question 3.12.3.6.

3.12.3.8 The DVR shall require a security feature (key, admin software rights) to prevent unauthorized users from accessing the on-screen menus to adjust video settings and perform file management functions.

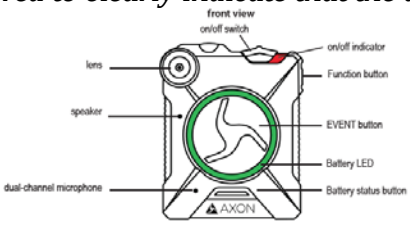
Yes. Officers must log in to the Axon View XL MDT Application to prevent unauthorized users from accessing the on-screen menus to adjust video settings and perform file management functions.

3.12.3.9 The DVR shall include a GPS receiver to provide vehicle position, course and speed information. The GPS receiver shall also be used to set the internal DVR clock to the proper time and date so that all vehicles display and record proper time.

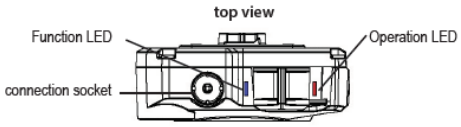
Yes. The camera can pull GPS from the in-car wireless router, as well as course. Speed can be calculated as long as GPS is included in the file metadata.

3.12.3.10 The DVR shall include indicators visible outside of the vehicle to confirm that the system is recording and that the wireless audio transmitter is activated. This indicator does not need to be visible to occupants inside the vehicle.

Yes. The LED lights and the audible beeps emitted from the device serve as recording awareness features. The Axon Fleet provides a clear visual recording indicator in the form of a large LED ring (around the perimeter of the Event Button). While recording, the forward facing LED ring will flash red to clearly indicate that the device is recording. This LED is configurable.



- ***Operational LED - The device also features a visible indicator light at the top of the device (clearly visible to the officer). This LED will flash green during buffering mode and flash red when recording.***



- ***Audible Alert - The device will also emit an audible beep every two minutes when recording is taking place.***

3.12.3.11 The DVR shall be capable of initiating a recording by both automatic and manual means. The DVR shall begin recording automatically when any of the following are activated:

A. Vehicle's emergency/pursuit lights;
B. Siren, and
C. The systems integrated crash sensor. (This activation shall include capturing the "look back" buffer memory to video-record the collision, should it be in view of the active camera.

Yes. Axon Signal is a system for secure activation of Axon camera devices. It is protocol, which operates over Bluetooth Low Energy. The effective range of Axon Signal is 30ft (~10 meters). The Axon Signal protocol is implemented by all Axon cameras, by the Axon Signal box and by an upcoming battery module for TASER conductive electric weapons.

Signal can convey specific telemetry messages that describe the state of the environment. Axon cameras capture these messages and store them as metadata within the video. Depending on the specific telemetry contained within the message, Axon cameras can decide to start or stop recording.

Specific activation criteria are listed below:

- ***Binary triggers: on-off triggers for 1 - 24V inputs. These inputs include door switches, light-bar, shotgun/patrol rifle release, brake switches or dedicated on-off switches.***
- ***ECU speed trigger: this input measures the time between speed pulses from the vehicle ECU. The period between pulses is changes in proportion to the vehicle speed. The Signal Box can be configured to match the time between pulses at 60 MPH to provide a highly accurate representation of vehicle speed. On the receiving side, Axon cameras can be configured to activate at a specific speed, such as 90mph.***
- ***Accelerometer: All Axon cameras include an accelerometer and can be configured to activate based on a high-G event, such as that of a crash.***
- ***MDT GPS: Should the MDT laptop or tablet contain a GPS receiver, the solution can utilize that source of GPS data. This data is used to store location and vehicle speed data within the video files.***
- ***Mobile Application: mobile apps can send activation events. These events will allow future functionality such as real-time CAD activation where an officers cameras are activated as soon as they are assigned to a call.***
- ***Another Wearer's Axon Camera: Axon cameras can be configured to broadcast Signal messages when activated. Thus Fleet cameras will activate when a nearby Axon Body 2 begins recording.***
- ***TASER CEW: TASER is producing a retrofit battery for existing TASER weapons. This battery will activate Axon cameras when the CEW safety is disabled.***
- ***External GPS: Axon Signal will accept a NMEA-format serial input from external GPS devices, such as those used for AVL systems. This GPS data can be added to the video as the definitive source of GPS data.***

3.12.3.12 The audio input associated with the forward-facing camera shall record audio using the internal microphone inside the vehicle. When the wireless audio transmitter/BWC is activated, the audio input shall be automatically switched to the wireless audio transmitter's

microphone. The system shall automatically revert to the internal microphone when the wireless audio transmitter/BWC is deactivated.

Yes. Users can choose which audio stream they wish to playback. Audio is captured by both the BWC microphone and the in-car camera microphone.

3.12.3.13 The DVR shall include a programmable pre-event recording mode allowing it to capture images a minimum of 30 seconds prior to the activation of the RECORD mode. Specify pre-event recording capability of proposed DVR.

Yes. The pre-event buffer is configurable from 0-120 seconds.

3.12.3.14 The DVR shall be capable of capturing date/time, user identification information, emergency light indication, siren indication, speed indication (w/ radar interface), braking indication, and whether the microphone is activated. The information shall not be overlaid on the recorded video, and should be stored as secured metadata.

- ***capturing date/time - Yes***
- ***user identification information- Yes***
- ***emergency light indication - No. These activation triggers are available, however, there will be no indication if it was on/off at any given time.***
- ***siren indication - No – These activation triggers are available, however, there will be no indication if it was on/off at any given time.***
- ***speed indication (w/ radar interface)- Yes - As long the file has associated GPS data speed can be calculated (with radar interface).***
- ***braking indication, and - No – These activation triggers are available, however, there will be no indication if it was on/off at any given time.***
- ***whether the microphone is activated - Yes***
- ***The information shall not be overlaid on the recorded video, and should be stored as secured metadata. - Confirmed***

3.12.3.15 The DVR shall allow video to be played back in the vehicle. When the DVR PLAY button is pressed a list of all prior recordings shall appear on the display screen provided.

Yes. This is accomplished using Axon View XL.

3.12.3.16 The DVR shall record video in a format that allows playback on multiple devices.

Yes. Video and audio are recorded and exported to the application in a standard, open, and non-proprietary format, including both codec and container.

Audio and video are recorded as the same MP4 encoded file ensuring perfect synchronization. The video format is MPEG4 using the H.264 compression standard. Sound is recorded via the Advanced Audio Coding (AAC) coding standard for lossy digital audio compression. The MP4 files can be played using all freely available standard software (i.e. Windows Media player, Real player, QuickTime, VLC, etc.).

3.12.3.17 The DVR shall provide a means to ensure the integrity of the recorded video has not been compromised. The video must be able to be authenticated at any time, including when it is played back outside of the police vehicle.

Yes. Officers cannot delete, alter or edit the videos stored on their camera. Using Axon View in the field, an officer can update the evidence title, ID and assign a category, however; the integrity of the original data can never be changed.

The device uses a non-standard connection to access data on the camera and a granular device-level audit trail will be available in a future release.

Content on the device is only deleted once it has been successfully transferred to the system, and once in the system can only be deleted in accordance with the NHP's retention or Role Based Access Control (RBAC) policies as defined and applied in the categorization of the video content.

A cryptographic SHA hash is automatically created by the camera every time a video is finished recording. This SHA is sent to the application to verify the integrity of the file and is used for auditing purposes. The hash can be used to demonstrate that the recording has not been modified, down to the last bit.

By the end of 2016 the solution will fully migrate to SHA-2.

3.12.3.18 The DVR shall provide a means to ensure the integrity of the recorded video has not been compromised. The video must be able to be authenticated at any time, including when it is played back outside of the police vehicle.

Yes. Officers cannot delete, alter or edit the videos stored on their camera. Using Axon View in the field, an officer can update the evidence title, ID and assign a category, however; the integrity of the original data can never be changed.

The device uses a non-standard connection to access data on the camera and a granular device-level audit trail will be available in a future release.

Content on the device is only deleted once it has been successfully transferred to the system, and once in the system can only be deleted in accordance with the NHP's retention or Role Based Access Control (RBAC) policies as defined and applied in the categorization of the video content.

A cryptographic SHA hash is automatically created by the camera every time a video is finished recording. This SHA is sent to the application to verify the integrity of the file and is used for auditing purposes. The hash can be used to demonstrate that the recording has not been modified, down to the last bit.

By the end of 2016 the solution will fully migrate to SHA-2.

3.12.3.19 The Control Center/DVR firmware shall allow in-system programming for future updates. Please describe how updates are made.

Yes. Updates to Axon View XL are pushed over the air. This happens automatically as long as the NHP approves updates. MDTs must have an internet connection. This process also pushes firmware updates to cameras.

3.12.3.20 The DVR or related display (Mobile Data Computer, tablet etc.) shall have backlit controls for record; stop; play/pause; forward/reverse, fast forward/ reverse; trace, and lighted indicators for power on; record; and play.

Yes. The Axon Fleet solution includes Axon View XL, a Microsoft Windows-based MDT software application to manage the in-car camera system. The MDT software supports Windows 7/8/10 and can run on a Windows 10 tablet. It can be remotely installed and upgraded using traditional Windows automation tooling. The MDT software presents a user interface that is equally optimized for mouse or touch-panel usage.

Officers will be able to view a live stream of their Axon Fleet camera through their MDT, review videos captured, and add additional labels and categories to videos from the MDT. Categories and configurations are pulled from the agency's Evidence.com. When officers share cars, the MDT app is also used to assign the recordings to a specific officer by having the officer log into the MDT app at the beginning of the shift.

The MDT application provides the following capabilities:

- ***Before recording, the officer is able to provide their identity. This allows Axon Evidence.com to index the video by both car number and by officer. This reduces time spent looking for video evidence.***
- ***Before recording, the officer is able to run a system check and preview the video and audio being captured by both the front and rear camera. They can also check that the different triggers are operating as expected.***
- ***The officer can control the recording of the cameras. One or both cameras can be commanded to start/stop recording.***
- ***The officer can view the video from both cameras as it is being captured.***
- ***The officer can enter metadata for a video during or at the conclusion of a recording.***
- ***The officer can monitor storage capacity of both cameras.***
- ***The officer can monitor Wi-Fi off-load status of the camera.***

3.12.3.21 The power control switch shall allow the DVR to automatically power on after the vehicle's ignition is switched on.

Yes. Power management is built in to the device's firmware and inline battery. The system can remain powered without pulling power from the car, using the Fleet power unit for up to 4 hours.

3.12.3.22 The DVR shall automatically power down after the vehicle's ignition is turned off provided the DVR is not in "Record" and is not in the process of downloading files or other type of file save.

Yes. Power management is built in to the device's firmware and inline battery. The system can remain powered without pulling power from the car, using the Fleet power unit for up to 4 hours.

3.12.3.23 The DVR should provide a means to tag an incident at the time it is recorded with a priority designation. Once a recording is stopped, the DVR should automatically prompt the officer to select from the pre-defined drop-down list(s).

Yes. Officers can review recorded video and associated metadata, as well as add annotations like incident numbers, case categories, etc. through Axon Fleet's MDT application, Axon View XL. The application has an intuitive interface designed for officers to quickly access the functions they need, so they can focus on their jobs in the field.

Officers will only be able to review and annotate video currently stored on their Fleet camera through the Axon View XL application. Video that has already been offloaded can be accessed by logging into Evidence.com. Evidence.com is accessible on any device with an internet connection via a standard web browser, subject to IP restrictions and security settings configurable at the agency level.

Pre-configured Axon Signal triggers like light-bar activation will initiate recording even if the officer is using the MDT application at the time.

3.12.3.24 The DVR shall be capable of operating within the range of interior temperatures found within a law enforcement vehicle in Nevada without the need for supplemental heating or cooling. Specify your DVR's operating range and acceptability for the extreme temperature range in Nevada

Yes. The Axon Fleet camera is a rugged piece of equipment designed to withstand extreme temperature found in the interior of a law enforcement vehicle. The Fleet system can withstand exposure to extreme temperatures ranging from −35 °F to 122 °F [−37 °C to 50 °C] and up to 80% relative humidity.

3.12.4 Compact CCD Color Camera

3.12.4.1 The low-light CCD color camera shall use a Sony EXview® HAD CCD or equivalent image sensor to provide high quality nighttime images while minimizing blooming and glaring from bright sources of light. Proof of "equal" shall be the responsibility of the bidder and shall be submitted with the bid if not using the Sony EX VIEW chipset.

We have a wide angle lens + 1/3.2" image sensor, we can do 480p -1080p resolution.

3.12.4.2 The forward-facing camera shall be a solid state imaging system that is not subject to burn in, or interference by magnetic fields.

Complies - Axon Fleet have passed EMC immunity testing for EM radiation and ETSI EN 301 489 RF Electromagnetic field testing, with no degradation of performance.

3.12.4.3 The forward-facing camera shall operate within the range of temperatures from 0 to 120 degrees Fahrenheit or between -17.8 and 48.9 degrees Celsius.

Yes. The Axon Fleet camera is a rugged piece of equipment designed to withstand extreme temperature found in the interior of a law enforcement vehicle. The Fleet system can withstand exposure to extreme temperatures ranging from −35 °F to 122 °F [−37 °C to 50 °C] and up to 80% relative humidity.

3.12.4.4 The camera shall be compact so as not to obstruct the driver's forward or peripheral view thru the windshield, or provide any obstruction of factory installed airbags or mirrors.

Yes. The Axon Fleet camera will not obstruct the vision of the driver. The entire system is smaller by volume than the camera component of most competitors alone. The small design offers flexibility in mounting locations allowing agencies to choose a camera position that will optimize officer visibility and safety. The Axon team is happy to assist NHP with determining the best mounting option for each model vehicle.

3.12.4.5 The camera shall be a single unit, including power lens, mounted on the windshield or roof of the vehicle and operate on 12 VDC power source.

Yes. The unit runs off of the car battery.

3.12.4.6 The camera shall provide a minimum field of view of 24 feet width at distance of 35 feet (40 degrees).

Yes. The Axon Fleet's 143° wide-angle lens was designed to record a wide field of view (FOV) to capture accurate evidence, even when the device is mounted on an officer's beltline. Axon Fleet's diagonal field of view is 107° horizontal and 78° vertical.

A wide FOV provides a better representation of what the officer is seeing and provides a record of the officer's environment.

Distortion Correction

In order to achieve an ultra-wide FOV, most cameras use an ultra-wide angle lens or 'fisheye' lens. Fisheye lenses result in distortion of the image. The Axon Fleet automatically corrects for this distortion. Correcting for this distortion results in an overall better quality video. This difference is especially noticeable when dealing with still images generated from wide FOV video.

Distortion Correction via Software

Unlike many competitors' cameras, TASER's Axon Fleet camera automatically corrects for fisheye on the camera. TASER's backend software (Evidence.com) currently provides the NHP the ability to correct for wide-angle distortion through Evidence.com.

3.12.4.7 The camera shall have manual and automatic focus capabilities, which are user selectable.

Yes (automatic focus). Axon Fleet does not have manual focus.

3.12.4.8 The front camera should have a minimum 120X zoom (10x optical zoom with 12x digital zoom). Specify mode.

No. The camera doesn't have zoom functionality; however, zoom can be accomplished in post-production from within Evidence.com.

3.12.4.9 The minimum LUX rating of the forward facing camera shall be rated at less than 1 LUX at full shutter speeds and 0.05 LUX in night view mode.

Yes. Axon Fleet cameras utilize high quality lenses with "Retina Low-Light" Imaging Technology of ≤ 0.1 lux. The human eye has a lux rating of approximately 0.1 lux. By matching that sensitivity, the camera is able to more accurately capture and portray the experience of the user. In order to achieve outstanding reproduction in low light, cameras can either utilize electronics (amplification) or optics (lenses). With amplification, video footage may be grainy and inaccurately reproduce the event.

3.12.4.10 The camera shall automatically adjust for varying light levels from day to night. The camera and lens will be equipped with auto focus, automatic exposure, and automatic white balance.

Yes.

3.12.4.11 The camera shall have a minimum color resolution of 450 horizontal lines.

We encode in a progressive format 480P, 720P and 1080P. So our system supports 1080 lines of resolution.

3.12.4.12 All cameras shall default to auto focus. An override system should be configurable to prevent operation while the vehicle is in motion.

Yes. All focus is auto-focus. The cameras do not utilize manual focus.

3.12.4.13 The camera shall offer a signal-to-noise ratio of at least 46db.

We do not offer signal-to-noise ratio for Axon Fleet. The camera is the recording device for both audio and video; the dual-channel microphone is built into the device. The camera can pick up multiple conversations within its audio range and can detect audio up to 15-20 feet when spoken at a normal conversational volume.

A single channel is specifically designed to focus on the audible frequency band associated with voice. The second channel has been developed to filter out low and high frequency noise that is beyond the audible range of the human ear. The camera system also employs a codec with digital filters and automatic gain control to manage excessively high and low audible sounds. This is immensely valuable when dealing with environments with significant ambient noise.

3.12.4.14 The camera shall have backlight compensation setting.

Axon Fleet cameras are equipped with automatic focus, exposure, and white balance.

The Axon Fleet offers 3-axis image stabilization. The electronic image stabilization algorithm takes inputs from the lens driver (focal length) and the accelerometer (movement of the device). The algorithm uses this information to calculate an accurate motion vector. With the motion vector, the processor inside the device is able to shift the electronic image from frame to frame, counteracting motion and stabilizing the video.

In the future, it is possible that TASER could add further stabilization capabilities using post processing in the Application, similar to what TASER has done with regard to Redaction and Assisted Redaction. The TASER solution facilitates efficient handling of complex post processing via the system design structure.

3.12.4.15 The camera shall be compact. List the size and weight of the proposed CCD camera.

Yes. Width: 2.76 in [7 cm]
Height (fully extended): 7.37 in [18.7 cm]
Depth: 1.58 in [4 cm]
Weight: 5.0 oz [142 g]

Please see the attached Axon Fleet Specification Sheet, included in Tab IX.

3.12.4.16 The camera shall mount with a heavy-duty controlled pivot mount that does not obstruct the driver's field of view. Camera shall be able to be rotated 360 degrees and can pan and tilt to +/- 90 degrees. Adjustment shall require no tools.

No. The Axon Fleet mount rotates 210 horizontally in 30 degree increments and has a 110 degree vertical rotation.

3.12.4.17 An optional rear view camera shall be available.

Yes. NHP can purchase either a one camera or two camera bundle. Officers can also turn off the rear-facing camera and record only front-facing camera footage.

3.12.5 Back Seat Cameras

3.12.5.1 The back-seat camera shall utilize a micro compact with wide angle 1/3" Super HAD image device (or equivalent) with approximately 420 lines of resolution. Proof of "equal" shall be the responsibility of the bidder and shall be submitted with the bid. This must be included in the system at no charge.

TASER offers a wide angle lens + 1/3.2" image sensor, we can do 480p resolution.

3.12.5.2 The rear-facing camera shall be capable of being mounted covertly in the cab.

No. The rear-facing camera is mounted on the officer side of the partition, but is not intended to be covert.

3.12.5.3 The rear facing camera shall be capable of recording the entire rear seat area of the police vehicle.

Yes.

3.12.5.4 The rear-facing camera shall have a minimum lux rating of .03. Specify the rating.

Yes. Axon Fleet cameras utilize high quality lenses with "Retina Low-Light" Imaging Technology of ≤ 0.1 lux. The human eye has a lux rating of approximately 0.1 lux. By matching that sensitivity, the camera is able to more accurately capture and portray the experience of the user.

3.12.5.5 The rear-facing camera shall utilize infrared illumination to capture video in no-light conditions.

No. In order to achieve outstanding reproduction in low light, cameras can either utilize electronics (amplification) or optics (lenses). With amplification, video footage may be grainy and inaccurately reproduce the event.

3.12.6 Compact Color LCD Monitor

3.12.6.1 The monitor shall be a full color high quality LCD, active matrix (TFT) screen that measures at least 3.0" measured diagonally.

Yes. Compliance with this requirement is dependent upon the specifications of the MDT/MDC used by NHP. Axon View XL is installed on existing devices. If the vehicle doesn't have an MDT/MDC, Axon Fleet is still operational, but cannot be controlled with a visual interface.

3.12.6.2 The monitor shall be capable of displaying a live picture from the camera when powered, even if recording is not in progress.

Yes. The Axon View XL MDT Application allows officers to live view both cameras.

3.12.6.3 The monitor shall operate between 32 and 120 degrees Fahrenheit.

Yes. Compliance with this requirement is dependent upon the specifications of the MDT/MDC used by NHP. Axon View XL is installed on existing devices.

3.12.6.4 The monitor shall include a system speaker, with volume control, to provide monitoring of live audio or playback from all system microphones.

Yes. Officers will be able to playback body-worn camera video in Q1 2017. Live streaming of audio is not available but we will be able to support live stream of BWC video on MDT application by Q1 2017.

3.12.6.5 The monitor shall have controls/indicators that mimic the DVR and include record; stop; play/pause; forward/reverse; brightness; volume; and power. The monitor should also include a button for

disabling the monitor when the system in standby, and accessing a menu for programming.

Yes. These actions can be accomplished using Axon View XL.

3.12.6.6 The monitor should have the capability to display: date/time, user identification information, emergency light indication, siren indication, latitude and longitude, speed (w/ radar interface), braking indicator and microphone activation indicator. The information shall not be overlaid on the recorded video; rather, it should be stored as external secure meta-data (or equivalent) in the video file.

No. Axon Fleet metadata will display the time the cameras are activated.

3.12.6.7 The monitor should support a full-screen video mode (without the auxiliary data) using a single key press on the control center.

Yes. Video can be played back in full-screen mode.

3.12.6.8 The monitor shall operate independently from the recording device. For covert operation it should possible to operate the DVR in RECORD mode with the monitor turned off.

Yes.

3.12.6.9 The monitor shall be provided with an adjustable mounting bracket that will allow it to be mounted in a variety of locations within the law enforcement vehicle.

No. Axon Fleet's Axon View XL Application will use NHP's existing MDTs, so no additional mounts needed.

3.12.6.10 The monitor shall have the capability to display the approximate amount of storage remaining on the media in an HH:MM format. An audible beep or other form of tone shall warn operator prior to or when there is 10%, or less, time remaining on the media.

Yes. The device's internal firmware is constantly checking the remaining storage capacity. Should recording capacity drop below 6 GB of available storage - the device will emit three quick successive beeps, these beeps will repeat every 15 minutes. In addition, the "Function LED" will blink yellow. When recording capacity has been reached, the device will beep three times and every time the user attempts to start a new event, will beep three times and not enter recording mode.

The device will never overwrite over any previously recorded footage. It is not possible to delete, modify or overwrite any video content on the device; it can only deleted once it has been successfully transferred to Evidence.com. This ensures that no data is accidentally deleted or modified on the device.

The device features 64GB of storage capacity. The device features sufficient storage for 11-70 hours of recording. It is only under extreme circumstances that the device would have low remaining capacity.

3.12.7 Microphones

3.12.7.1 The system shall come equipped with a digital wireless microphone that is incorporated into the BWC and an in-car microphone. The in-car microphone shall be mountable anywhere within the vehicle.

Yes. The in-car microphone is in the Axon Fleet camera. Axon body-worn camera microphones also serve as additional audio recorders.

3.12.7.2 Audio from the interior microphone and the wireless microphone/BWC shall record on separate audio channels.

Yes.

3.12.7.3 The wireless microphone/BWC shall be self-contained and include a re-chargeable battery; mountable charger/docking station; internal microphone; internal antenna. Transmitters that rely on the microphone cable for an antenna, or which utilize an external antenna shall not be permitted.

Yes.

3.12.7.4 The wireless microphone/BWC system shall be FCC type accepted.

Yes.

3.12.7.5 The wireless microphone/BWC shall have a minimum effective operating range 1,000 feet under line-of-sight conditions.

Yes. Axon Fleet cameras aren't transmitted so they're not tethered to the vehicle; however, audio is recorded on the officer's BWC.

3.12.7.6 The wireless microphone/BWC must have a minimum stand-by battery life of ten (10) hours without recharging or additional batteries, with pre-record on.

Yes.

3.12.7.7 The wireless microphone/BWC should be capable of automatically activating the DVR system; additionally, the wireless audio transmitter/BWC shall be capable of being activated by the DVR system when a recording is started.

Partial yes. Body-worn cameras do not activate Fleet in-car cameras, however; pre-configured Axon Signal triggers will activate both Axon Fleet and Axon Body 2 cameras.

3.12.8 Control Center

3.12.8.1 The control center shall be compact in design and mounted overhead, or in the equipment console between the seats.

Yes. Axon View XL is installed on existing MDT/MDCs.

3.12.8.2 The control center shall not obstruct the driver's forward or peripheral view or provide any obstruction of factory installed airbags or mirrors.

Yes. Axon View XL is installed on existing MDT/MDCs.

3.12.8.3 The control center shall not require any permanent modifications to the police vehicle.

Yes. Axon View XL is installed on existing MDT/MDCs.

3.12.8.4 The control center shall accommodate the mounting of the front and rear-facing cameras, the monitor and keypad.

Yes. Axon View XL is installed on existing MDT/MDCs.

3.12.9 Video Viewing Software/Hardware

3.12.9.1 A video viewer/software shall be provided to allow recorded video files to be played on any computer and display date/time, user identification, emergency light indication, siren indication, latitude and longitude, speed (w/ radar interface), braking indication and the microphone activation indicator. This information shall not be overlaid on the recorded video; it shall be displayed outside the video frame.

Partial yes. Axon Fleet metadata capture date/time, user, emergency lights, activation and speed (as long as GPS data is recorded). Microphone activation will be available.

3.12.9.2 Support for this software shall include version updates provided free of charge for the lifetime of the system.

Yes. TASER releases software patches on both scheduled and nonscheduled basis as required. Updates to firmware supporting Axon cameras and Axon Docks are "pushed" from the internet the local devices though the Axon Docks without the need for Agency interaction.

Evidence.com software upgrades are handled in a similar way. TASER will release a software update to Evidence.com during a period of low traffic usage. Software upgrades are "pushed" to Evidence.com and are immediately available to you as soon as you log on, eliminating the need to perform manual software updates. The Evidence.com operations team at TASER applies these upgrades remotely, eliminating any worries about properly integrating or updating your systems. The latest product features and enhancements are included as part of your investment in Evidence.com. Evidence.com software is updated regularly throughout the year, and these updates are included in the price of your software licenses.

TASER releases software patches on both scheduled and nonscheduled basis as required. Patches contain fixes to known issues reported by internal resources or by users at police agencies. There are no additional costs for any software patch or fix deployed. Patch deployment involves minimal or no downtime for the customer's solution.

Scheduled maintenance will take place according to our monthly routine maintenance schedule. Routine maintenance is currently scheduled on the fourth Tuesday of each month from 7:00 PM to 8:00 PM Pacific Time. When possible, you will be informed one week prior to any changes to the maintenance schedule.

Software updates, patches and fixes are included in the purchase of Evidence.com licenses.

Release Notes and Documentation

A detailed email is sent to system administrators when new releases, updates or upgrades are made to Evidence.com, Evidence Sync or Axon hardware.

The Release Notes page in Evidence.com displays links to the release notes containing a summary of features and enhancements for the current and previous releases.

The User Guides page displays links to guides that provide detailed information on Evidence.com features. Release notes and user guides are in PDF format.

As updates and features are released, your Regional Support Manager will troubleshoot all changes to ensure a successful experience for customers.

3.12.9.3 Vendors shall provide all hardware (media readers/drives) and software necessary duplicate, share and present digital video in a court acceptable format. Please describe transfer steps needed to convert captured video to court acceptable evidence without the need for a server based infrastructure.

Yes. Evidence.com ensures a reliable chain of custody for all video files by providing a high level of security, reliability, and expandability. Proper documentation of chain of custody is preserved and can be used to ensure video evidence can be tendered in court as an exhibit. There are also several levels of evidence protection implemented such as, encryption, access control, hashing and other security protocols.

To ensure a robust chain of custody, evidence can be verified for authenticity by matching the SHA hash of original file ingested in Evidence.com with the copy.
Audit trails associated with each and every piece of evidence stored in your agency's account will be able to demonstrate:

- ***how the video was taken***
- ***when the video was taken***
- ***where the video was taken***
- ***how the video was stored***
- ***who had access to the video from the time it was taken through the time it is introduced in court, and***
- ***Details on whether or not it has been altered and how (the original file is never altered, a new copy is created with any changes)***

By the end of 2016 the solution will fully migrate to SHA-2.

An administrator can access a file on Evidence.com, download the file, and then copy it to a CD/DVD or flash/thumb drive. DVDs and CDs can be created using any DVD or CD writing software. Axon cameras record using MP4 format, which is playable without the need for proprietary software.

Users can download individual files and can bulk download files in ISO or ZIP file format, either of which is suitable for removable media. This offers flexibility in packaging depending on NHP requirements.

3.12.9.4 The video management software should be capable of converting a video from the proprietary format to the standard DVD Video format, and authoring a DVD capable of being played in a standard DVD player.

Yes. An administrator can access a file on Evidence.com, download the file, and then copy it to a CD/DVD or flash/thumb drive. DVDs and CDs can be created using any DVD or CD writing software. Axon cameras record using MP4 format, which is playable without the need for proprietary software.

Users can download individual files and can bulk download files in ISO or ZIP file format, either of which is suitable for removable media. This offers flexibility in packaging depending on NHP requirements.

3.12.10 Server Based Video Management System (VMS)

3.12.10.1 VMS shall either be an externally hosted cloud-based data storage solution with the capability of organizing/managing video/digital evidence, server based or consist of a hybrid solution and be accessible via the internet to multiple users simultaneously. The State prefers Cloud or a Hybrid solution.

3.12.10.2 The VMS should include infrastructure in our Northern, Southern, and Central regional command offices to assure downloading of all rural substations into the regional command centers to which they report (see Table 3.8.A).

3.12.10.3 The VMS shall be a turn-key component and fully installed, serviced, warranted, and maintained by the vendor.

3.12.10.4 The VMS should include video storage servers or equivalent for all regional offices to capture video information, workstation(s) for managing and viewing stored video, equipment racks to mount equipment, and uninterruptible power supplies (UPS).

3.12.10.5 The VMS should provide a configurable archive unit that can automatically archive video copies based on set parameters, and copy video files to a DVD-Video or equivalent court acceptable format.

3.12.10.6 Pricing for the VMS shall be provided on the In-Car Video Cost in the vendor's response. Pricing must be included for all proposed hardware (workstations, servers, archiving hardware, video backup systems, access points), wiring, software, installation, configuration,

and training. If proposing a cloud or Hybrid solution, provide this pricing in the ICV cost schedule.

3.12.10.7 If a server based video management back office component is proposed, a schematic of the back end infrastructure shall be included with responses to the RFP.

3.12.10.8 The VMS file storage shall be equipped with sufficient storage to comfortably manage video that would be generated from cars depicted in the scope of work in this RFP. List and itemize the size of proposed storage for each regional command center identified.

3.12.10.9 If wireless downloading capability is proposed for vehicles assigned to each regional office, provide download times for video captured based on the video compression and resolution capabilities of proposed cameras, the proposed number of access points, and the proposed servers/wiring infrastructure or cloud solutions.

3.12.10.10 The VMS shall include a database that contains a record for each recorded video file. The database shall store sufficient information to support the search capabilities and provide chain-of-evidence documentation.

3.12.10.11 The VMS shall be capable of searching stored video files by: department ID, time, date, officer ID, vehicle ID, camera, recording mode, and status (online or archived).

3.12.10.12 The VMS shall be capable of providing custom fields that may be used to store department-defined information (e.g. suspect's name, license plate number, etc.).

3.12.10.13 The VMS should allow videos to be categorized using department-defined drop-down lists. This classification shall be used for searching and to define how long each category of video is to be kept before it is automatically deleted.

3.12.10.14 The VMS shall provide a means to ensure the integrity of the recorded video. Video integrity must be checked when the video is uploaded, anytime it is played back or archived, and shall be verifiable on demand.

3.12.10.15 The VMS shall provide the capability to duplicate, share and present digital video in a court acceptable format. Describe the transfer steps, if any, needed provide video to the courts as acceptable evidence. Describe the way and format the proposed system archives recorded video files, and how these files will be stored and backed up for safeguarding.

3.12.10.16 When a video file is copied or archived to digital media, the Video Management Software shall store a unique archive ID and maintain a virtual directory to recall the archived video file(s).

3.12.10.17 The Video Management Software shall be capable of converting a video from the proprietary format to the standard DVD Video format, and authoring a DVD capable of being played in a standard DVD player.

3.12.10.18 The support for this software shall include version updates and be provided free of charge to the agency for the lifetime of the system.

Not applicable. Evidence.com is a cloud-based digital evidence management system.

3.12.11 Control Center Specifications

3.12.11.1 An optional radar interface shall integrate directly with the Agency Bee III radar equipment. Collected information shall include speed of the target, the "locked" target speed, and the patrol vehicle.

No. Axon Fleet does not provide radar support.

3.12.11.2 The State is interested in a system that can be configured for motorcycle use. All of the specifications described for the DVR and wireless microphone shall be applicable. Is a motorcycle option available for your solution? If so, does the configuration utilize a weatherproofed monitor and camera? Please explain.

No. TASER does not currently have motorcycle mounting, but Axon Signal and Axon Flex cameras can be configured for motorcycle officers.

3.12.12 Officer Safety

3.12.12.1 All equipment shall be capable of installation in the following vehicles while still meeting the other requirements stated herein: Chevrolet Tahoe, Dodge Charger, Ford Interceptor Utility/Sedan and Ford F150 Pick-up.

Yes.

3.12.12.2 Describe dimensions and vehicle mounting options for your camera, recorder, wireless microphone, transmitter/ receiver and any other required equipment.

Yes. Width: 2.76 in [7 cm]
Height (fully extended): 7.37 in [18.7 cm]
Depth: 1.58 in [4 cm]
Weight: 5.0 oz [142 g]

Please see the attached Axon Fleet Specification Sheet, included in Tab IX.

3.12.12.3 Equipment must not be installed in such as manner as to interfere with a passenger in the front passenger seat.

Yes.

3.12.12.4 No part of the system shall interfere in any way with the driver's field of view. The camera shall be a single unit, including power lens, mounted on the windshield or roof of the vehicle and operate on 12 VDC power source All connections to the camera, for power and video, shall be made by a single cable that attaches using a quick release connector.

Yes. The unit runs off of the car battery.

3.12.12.5 The in-car system shall be protected from damage due to input of voltage, reverse polarity, and electrical transients that may be encountered.

Yes. Protective features are built into the camera.

3.12.12.6 No item installed in the interior of the passenger compartment shall increase the risk of injury to occupants during events related to a vehicle crash.

Yes. The Axon Fleet camera will not obstruct the vision of the driver. The entire system is smaller by volume than the camera component of most competitors alone. The small design offers flexibility in mounting locations allowing agencies to choose a camera position that will optimize officer visibility and safety. The Axon team is happy to assist NHP with determining the best mounting option for each model vehicle.

3.12.12.7 Any items installed in the interior of the vehicle shall meet the requirements stated in Federal Motor Vehicle Safety Standard 201 [October 1, 2002] Occupant Protection in Interior Impact as referenced in the In-Car Video Camera Systems Performance Specifications - Digital Video Systems provided by the International Association of Chiefs of Police. (11/21/2008).

The solution is still in beta and as such is undergoing the proper validation testing. The fleet solution will meet all necessary standards to ensure evidentiary integrity and admissibility in court.

3.12.12.8 All controls and components should be located and designed to minimize driver distraction. The control pad should be designed and organized to minimize officer workload. The record button should be readily identifiable by size, color, location and/or other design features. The record button should be easily accessible by officers wearing gloves.

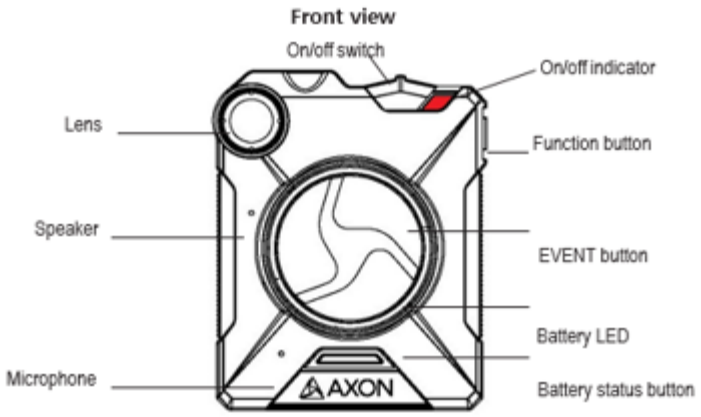
Yes. A complicated activation mechanism is cumbersome in the field and can impede more important duties, especially considering officers often have to start a recording at a moment's notice.

The Axon Fleet was designed specifically for use by law enforcement in tactical policing situations. Activation of event recording is simple and accessible, so officers can operate the device in a high-stress situation. Recordings are initiated with a single "Event Button" located on the front of the device, so an officer can easily reach it with one hand.

The Axon Fleet camera has two operating modes:

5. ***BUFFERING (turning on the camera and starting pre-event buffering)***
6. ***EVENT (event recording)***

To initiate Buffering Mode (turn the camera on) Move the ON/OFF switch on the camera to the ON position. The raised on/off switch is strong enough to prevent accidentally powering the device down, yet can still be switched on if an officer is wearing gloves.



To initiate Event Recording Mode, simply tap the large concave button on the front of the camera two times. While the device is easily activated when worn in a shirt pocket or housed in a case, it is still protected against unintentional event triggering. To end the recording, simply hold down the button for three seconds.

The system can be activated Handsfree using the Axon View XL application, or Axon Signal technology.

3.12.12.9 System components shall be capable of being illuminated for ready identification during periods of darkness. The illumination level shall be capable of being controlled over a range from bright to dark.

Yes.

3.12.12.10 All wiring shall meet industry standards applicable to the wire application including Underwriters Laboratory (UL) as well as the Society of Automotive Engineers (SAE).

Yes.

3.12.12.11 Manufacturers shall provide information in their installer's guide or owner's manual that specifies the proper wiring, fuses, connectors, connection points with the vehicle electrical system and grounding points.

Yes.

3.12.12.12 No parts that can come into contact with human skin shall be allowed to reach a temperature capable of causing a burn injury, Reference UL 60950 "Safety of Information Technology Equipment" as amended December 1, 2000.

Yes.

3.12.12.13 Any system component carried on the officer's person shall meet all Underwriters Laboratory Standards for shock/electrocution and burn

prevention. All batteries used in such devices shall meet Underwriters Laboratory Standards for safety.

The Axon camera and dock are NOT UL listed at the moment, but we are in progress of getting a TUV certification. We should have it in approximately one month.

3.12.12.14 The In-Car Video System shall operate on a power source that is filtered, regulated, and short-circuit protected. The voltage supplied to the In-Car Video System components shall meet the manufacturer's specifications and shall not vary with fluctuations of the vehicle's electrical system of between 9 and 18 volts.

Yes.

3.12.13 Reliability

3.12.13.1 The video systems shall maintain consistent audio/visual recording quality. The in-car recording system shall not be affected by transmissions from the police communication or interference from the following sources: high-powered television stations; other radio frequency interference (e.g. UHF, VHF & HF); automobile alternator, ignition, electrical systems; automobile heaters / air conditioner fan motors; or other patrol vehicle electrical systems.

Yes.

3.12.13.2 All equipment shall have a lifecycle of at least 3 years under law enforcement agency usage, or have replacement coverage under warranty and maintenance. Please provide expected lifecycle for all video system components.

Yes.

3.12.13.3 When in operation, the mobile video system must not generate electromagnetic or radiation that interferes with communications or other electronic equipment found within a police vehicle.

Yes.

3.12.13.4 Loss of power to the system shall not cause loss of any recorded data or result in the unit requiring reprogramming, reloading of software or operating system software.

Yes.

3.12.13.5 The video system shall be able to return to a "ready to record" mode after sudden loss of power without requiring user intervention.

Yes.

3.12.13.6 The system's timekeeping device and the vehicle's identifier shall be protected by a system battery backup to prevent loss of information

in the event the vehicle battery is disconnected for up to a minimum of fourteen (14) days.

Yes. The MDT is protected by system battery backup. This scenario would only cause an issue if an officer doesn't sign in to the Axon View XL application and instead uses Axon Signal.

3.12.13.7 Date and time within video system shall be self-adjusting for daylight savings time and leap years.

Yes. The Axon Body 2 offers the option for a permanent watermark of the time/date. This is configurable, but if it is enabled, the watermark will display time in UTC.

The metadata (EXIF data) associated with the capture footage will be in UTC. This metadata is part of the SHA fingerprint of the file and cannot be altered.

Accurate Local Time – Reflecting the DST Switchover

Evidence.com will never alter the original file (as verified by the SHA fingerprint) – thus, the metadata will always remain in UTC.

However, when displayed in Evidence.com, the Create Date ("Start time") will be displayed in local time (adjusted for DST), based on your agency's time zone preferences.

3.12.13.8 The video system shall have self-charging backup battery that continues recording upon loss of power, and should gracefully shutdown prior to available power being exhausted. The battery backup should power the system for at least 2 minutes following loss of the vehicle's battery power.

Yes.

3.12.14 Training/Documentation

3.12.14.1 The vendor shall offer and provide, at no additional cost, training to all end users on the use of the video system and video viewing software.

Yes.

3.12.14.2 The vendor shall offer and provide, at no additional cost, training to electronic technicians at their Reno, Elko, and Las Vegas shop locations. This training will ensure proper operation, repair, and maintenance of the manufacturer's video system.

Yes.

3.12.14.3 A system administrator class covering all aspects of the system shall be given at all the DPS/HPD Regional Command sites (Reno, Elko, and Las Vegas) upon award.

Yes.

3.12.14.4 Trainers must be experienced instructors who are thoroughly familiar with all technical aspects of the system.

Yes.

3.12.14.5 Provide a course syllabus for training classes to be provided with your RFP response.

Yes. Please see Tab IX.

3.12.14.6 Vendor shall include documentation for procedures on regular maintenance of video system components.

Yes. Not applicable.

3.12.14.7 Vendor shall provide complete service manuals and service bulletins on all electronic components.

Yes. A detailed email is sent to system administrators when new releases, updates or upgrades are made to Evidence.com, Evidence Sync or Axon hardware.

The Release Notes page in Evidence.com displays links to the release notes containing a summary of features and enhancements for the current and previous releases.

The User Guides page displays links to guides that provide detailed information on Evidence.com features. Release notes and user guides are in PDF format.

As updates and features are released, your Regional Support Manager will troubleshoot all changes to ensure a successful experience for customers.

3.12.14.8 Vendor shall provide documentation of system that includes identification of all vehicle equipment and the physical configuration; all configurable system parameters; written installation instructions, user manuals; and system administrator manuals instructions covering the change of all configuration settings.

Yes. Please see Tab IX.

3.12.15 Installation

3.12.15.1 Describe your approach for installing camera systems if this service is requested by the State. The State reserves the right to do such installations either through its fleet shops, or through an accessory installation contract.

TASER directly employs its own certified and qualified Technical Services Managers who are capable of physically installing the in car video solution, training fleet technical staffs and managing installation projects. If the state chooses to perform its installations through its fleet shops then the designated Technical Services Manager(s) will perform installation training for an entire working day,

per site. Each installation training session will include an assisted installation for the first 2 units per location, common troubleshooting practices, customer specific installation diagram and most current installation and support documentation.

3.12.15.2 Provide an installation price per camera unit for each regional office.

If the selects the option for TASER employees to install the in car video system then the cost is $325/per unit. This does not include removal or de-installation of existing hardware. This will also require an on-site, pre-deployment meeting with the fleet management decision makers to review pre-deployment installation requirements, camera placement and installation diagramming.

3.12.15.3 Specify the companies that will provide installation of camera systems in our Reno, Elko and Las Vegas regional offices if requested by the State.

As the prime contractor, TASER will provide installation services and/or installation training services for its customers at Reno, Elko and Las Vegas regional offices if requested by the State.