

## EDGEWOOD POLICE DEPARTMENT

5565 S. ORANGE AVE  
EDGEWOOD, FLORIDA 32809

Chris Francisco  
Chief of Police

Police Department 407.851.2820  
City Hall 407.851.2920  
Emergency 911

---

### *Interoffice Memorandum*

---

January 14, 2016

To: City Council

Via: Chain of Command

From: Chief Chris Francisco

Subject: Body Worn Cameras

During last month's city council meeting, the Council requested a list of pro's & con's in regards to body worn cameras. Attached to this memo is a report prepared by Sgt. Jackson in reference to the Council's request. In addition I have added a few comments listed below;

- Our Code Enforcement Officer has been using a body worn camera for approximately 9 months with only one complaint. The 9 months prior we had several complaints that she was unfair and rude. It has certainly increased transparency for the Code Enforcement Officer as well as the Public
- Research has shown that Law Enforcement Officers are open and supportive of the program. It has further indicated that the camera program has improved citizen and officer behaviors.
- Several forums from around the Country have shown that the public perception of Law Enforcement Officers increases in a positive direction when body worn cameras have been implemented.
- The financial impact to the City of Edgewood will be the service and maintenance of the cameras as well as the yearly storage costs associated with the program. The yearly cost will be approximately \$2,500.00 beginning February 2017.
- The total cost of implementation is \$11,238.44. We have been awarded two grants which will cover \$11,000.00, (one grant for \$10,000.00 & one for \$1,000.00). Our out of pocket expense will be \$238.44. This price includes evidence storage until February 2017.

Please feel free to contact myself or Sgt. Jackson if you have additional questions.



C. F.

# EDGEWOOD POLICE DEPARTMENT

## Body Camera Project

---

### Pro's and Con's

Sgt. Vince Jackson

1/14/2016

## Recording of all encounters

### *Pros*

The officer does not have to remember which situation to turn the camera on. If a situation deteriorates there is a record of the incident.

### *Cons*

- A. It can undermine community members' privacy rights (i.e. crime victims, witnesses, and non-law enforcement interactions)
- B. Damage police-community relationships (see Impact on Community Relations below).
- C. More data storage needed.

## Limited recording

### *Pros*

- A. Gives officers the discretion not to record if they feel that it would infringe on a citizens' individual privacy rights.
- B. Less data storage needed.

### *Cons*

Not all interaction with officers are recorded. Written documentation and justification should be required for incidents that are not recorded.

## Accountability Benefits

- A. Accountability and transparency
- B. Reducing complaints and resolving officer-involved incidents
- C. Identifying and correcting internal agency problems

## Evidence documentation

- A. Retained Recordings
- B. View and no tampering of videos
- C. Total recall before redaction

## Impact on community relationships

Some law enforcement executives have found that body-worn cameras have a negative impact on their intelligence gathering activities, especially if officers do not have the discretion to turn them off. However, others have found that the cameras actually improve their police community relations by defusing tensions that may arise during an encounter. Most law enforcement agencies have found that it is helpful to engage the community before the camera is rolled out to mitigate a community's concerns. Transparency about the agency's camera policies and practices, before and after the roll out, can help increase the public acceptance

## **POV (Point of View)**

### ***Pro***

**The Point of View from which the camera captures images may be the most critical single element of a new body-worn solution for law enforcement.**

### ***Con***

**Limited view of the law enforcement officer from the surrounding areas.**

## **Financial considerations**

In addition to the initial purchasing cost of the cameras, an agency will need to commit to funding and staffing resources toward storing recorded data, managing videos, disclosing copies of videos to the public, providing training to officers, and administering the program (i.e., ensuring the cameras are properly maintained, fix technical problems and address any issues of officer noncompliance). Data storage is the most expensive aspect of the body-worn cameras. This cost will depend on how many videos are produced, how long they are kept, and where they will be stored.



# AXON Flex™ helps agencies with Legal Benefits



## Department Profile



<b>Agency</b>	Aberdeen, SD
<b>Industry</b>	Law Enforcement
<b>Country</b>	United States
<b>Personnel</b>	42 sworn & 8 civilian
<b>Web site</b>	<a href="http://www.aberdeen.sd.us/index.aspx?nid=21">www.aberdeen.sd.us/index.aspx?nid=21</a>

## Captures POV

Aberdeen Officers found that the AXON™ eliminated the ambiguity of what the officers actually saw during the conflict. Also, the previous 30 seconds of looped record was able to be retrieved when the officer activated the system. Because of this capability, Aberdeen officers were able to present in the court of law critical evidence that conventional recording systems would have missed.

## Less Litigations and Lawsuits

With the exact recording of the incident, the video evidence from the AXON has been used by Aberdeen PD to prove that the officer is of no legal fault against false citizen complaints.<sup>1</sup>

## More Time in the Field

Because of the AXON, Aberdeen officers are spending less time filing paperwork or testifying in drawn-out court cases and more time on patrol. The AXON and EVIDENCE.com significantly increased the efficiency of the Aberdeen officers wearing the device and the Aberdeen PD as a whole.

"You get less complaints filed, you get less lawsuits filed, so you are saving money that way. You get better prosecutions, so you are saving money that way. Less court time, you are saving money that way."

Don Lanpher Jr., Chief,  
Aberdeen Police Department, SD

"I can just put on my reports 'See AXON recording' and I'm good to go."

Mike Law, Officer,  
Aberdeen Police Department, SD

<sup>1</sup> UK pilot project using 300 officers over a six-month period using a head camera setup found an increase of 9.2% increase in officer time on patrol. Guidance for the Police Use of Body Worn Video Devices. On May 14th 2011, Burnsville PD conducted an After Action Review of the AXON and EVIDENCE.com systems and produced the above findings (Interviewees include Chief Robert Hawkins, Officer Bryan Rychner, IT Systems Administrator Jarek St. Michaels, City of Burnsville Lynn Lembke, Officer Shaun Anselment). AXON™ and AXON Flex™ are trademarks of TASER International, Inc., and TASER® and © are registered trademarks of TASER International, Inc., registered in the U.S. © 2012 TASER International, Inc. All rights reserved.



# City of Rialto Case Study



Rialto PD's comprehensive, randomized experiment proves that TASER's AXON cameras reduced citizen complaints by 87.5% and reduced use of force by 59%.

## Agency

Rialto PD serves the family-friendly City of Rialto with 115 Sworn Officers and 42 non-sworn Officers. The PD covers 28.5 square miles and serves a population of 100,000. The City of Rialto retains its small-town atmosphere amidst quickly developing areas nearby and prioritizes Public Safety in order to maintain the City's safe, small-town feel.

### Department Profile



<b>Agency</b>	Rialto, CA
<b>Industry</b>	Law Enforcement
<b>Country</b>	United States
<b>Personnel</b>	115 sworn & 42 non-sworn
<b>Tech Solution</b>	AXON flex and EVIDENCE.com
<b>Web site</b>	<a href="http://www.rialtopd.com">www.rialtopd.com</a>

## Challenge

When facing the public, Rialto PD found two main areas for improvement: Use of Force, and Officer Complaints. These issues cost the department valuable time and resources. Rialto PD believed that improving oversight, gathering more video evidence, and improving trust within the community would decrease the frequency of these issues.

## Solution

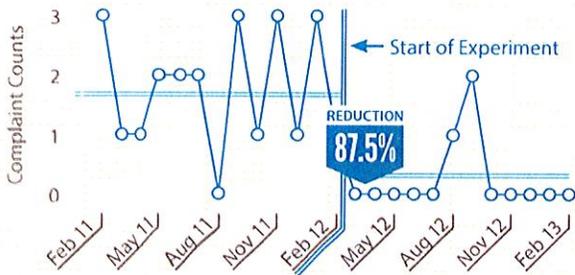
Rialto PD invested in TASER's Digital Evidence Ecosystem, AXON flex and EVIDENCE.com. After purchasing 66 cameras and licenses to EVIDENCE.com, the PD began a scientific research study to determine the effects of TASER's AXON flex and EVIDENCE.com solution.

To protect the integrity of data gathered during the experiment, Rialto PD used the "Cambridge Randomizer" and followed a strict scientific process. This strategy shaped a sophisticated, web-based experiment with data protected

from outside influences. Officers, shifts, and days were randomly assigned to experiment or control assignments. During the experiment, there were 498 experimental uses of AXON Flex and 499 control instances. The Study reached its 1-year mark in February 2013.

Because of Rialto PD's extensive data gathering and controlled study, the data is compelling. Over the course of 1 year, **officer complaints fell by 87.5%** in the experimental group. The data shows the officers increased interactions with the public compared to the previous year, and still complaints fell dramatically.

## Monthly Complaints Received

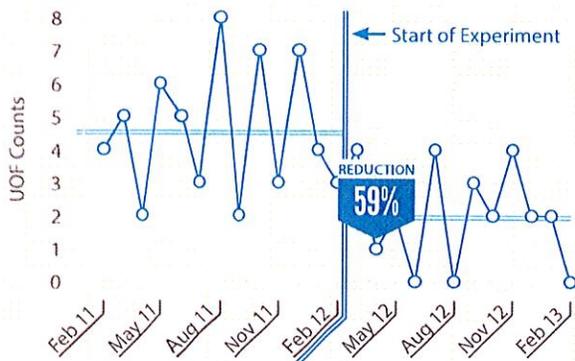


Decrease in Complaints



Rialto PD also focused on their Officer use-of-force data. During the experiment, individuals wearing an AXON flex **reduced use-of-force by 59%**. This data indicates that the presence of the camera not only encouraged compliance from the public but it also reduced instances of use of force by officers.

## Patrol Officer's Use-of-Force



Reduced Use-of-Force



## Conclusion

Rialto PD addressed their biggest areas for improvement with one system: TASER's Digital Evidence Ecosystem. Rialto PD justified the purchase of additional AXON flex and EVIDENCE.com licenses using their data. In the future, they'll use the study to educate other agencies on the benefits of on-officer video and cloud-based evidence management.



**TASER**

This document outlines the specific security features for Evidence.com, as well as the general security policies and practices related to TASER International's management of Evidence.com

TASER International recognizes the need for law enforcement agencies to adhere to their regulatory obligations when using Evidence.com. Knowing this key requirement, Evidence.com was designed and is operated to ensure that it aligns with the FBI's CJIS Security Policy. TASER International can provide additional documentation to demonstrate how Evidence.com is aligned with the CJIS Security Policy. Contact your TASER sales representative for more details.

TASER International has partnered with Amazon Web Services (AWS) to provide a secure, extremely scalable and highly reliable

infrastructure to operate Evidence.com. This partnership includes a shared commitment to ensure the infrastructure operating Evidence.com is aligned with the CJIS Security Policy. Additionally, AWS complies with many security assurance and certification programs and undergoes regular security audits. These include SOC 1/SSAE 16, SOC 2 & 3, CJIS, ISO 27001, FedRAMP, PCI, FISMA, and FIPS 140-2. TASER International regularly reviews the specific security practices and audit results documented by AWS to ensure the highest standards are met.

More details on AWS security and compliance practices and assurance programs can be found here <http://aws.amazon.com/security> and here <http://aws.amazon.com/compliance>.

## **Evidence.com: Security Features**

Evidence.com provides many security features and capabilities to enable customers to securely manage digital evidence. Evidence.com customers have varying risk profiles, and different security needs. Many of the following security features can be enabled or disabled by customers as needed, or can be changed to meet a specific level of risk. The default settings for these security features were chosen to provide a strong level of security, while still maintaining flexibility and convenience. Customers are encouraged to evaluate these features and align them with their own unique needs.

### **Access Control**

Evidence.com includes many features to provide robust access control.

- Customizable password length and complex password requirements
- Customizable failed login limit and lockout duration
- Enforced session timeout settings
- 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

<b>Encryption</b>
<p>Evidence.com uses strong encryption to protect evidence data in transit and at rest.</p> <ul style="list-style-type: none"> <li>• FIPS 140-2 approved encryption ciphers (or stronger)</li> <li>• Robust SSL/TLS implementation for data in transit.               <ul style="list-style-type: none"> <li>○ RSA 2048 bit key</li> <li>○ TLS 1.2 with 256 bit connection</li> <li>○ Perfect Forward Secrecy</li> </ul> </li> <li>• 256 bit AES encryption for evidence data in storage</li> </ul>
<b>Evidence Integrity</b>
<p>Evidence.com includes features to ensure the integrity and authenticity of digital evidence. These features ensure the evidence meets chain-of-custody requirements and can be proven to be authentic and free from tampering.</p> <ul style="list-style-type: none"> <li>• Forensic fingerprint of each evidence file using industry standard SHA-1 hash function. Integrity is validated before and after upload to ensure no changes occurred during transmission.</li> <li>• Full tamper-proof evidence audit records. Logs the <i>when</i>, <i>who</i>, and <i>what</i> for each evidence file. These records cannot be edited or changed, even by account administrators.</li> <li>• Original evidence files are never altered; even when derivative works (video segments) are created.</li> <li>• Deletion protection, including deletion approval workflows, deletions notification emails, and a deletion remorse period to recover accidentally deleted evidence files.</li> </ul>

## **Evidence.com: General Security Practices**

<b>Access Management</b>
<p>TASER International maintains account management policies and practices for Evidence.com. These include access control standards, account management procedures, regular account and permission validation, the principle of least privilege, and remote access policies that include 2-factor authentication for all administrative activities.</p>
<b>Security Monitoring &amp; Response</b>
<p>TASER International maintains security monitoring and incident response policies and practices for Evidence.com. These include robust attack detection, incident response procedures, logging and monitoring standards, and reporting to appropriate parties.</p>
<b>Vulnerability Management</b>
<p>TASER International maintains vulnerability management policies and practices for Evidence.com. These include regular vulnerability scans and penetration tests, awareness of newly disclosed vulnerabilities and security patches, and vulnerability remediation procedures.</p>
<b>Configuration Management</b>
<p>TASER International maintains configuration management policies and practices for Evidence.com. These include system configuration standards, patch management procedures, malicious software protection, and secure architecture standards.</p>



**Data Protection**

TASER International maintains policies and practices to protect data stored in Evidence.com. These include a data classification standard, data handling and transfer practices, encryption standards, and key management procedures.

**Personnel**

TASER International maintains policies and practices to ensure trustworthy and competent people are working with Evidence.com. These include criminal background checks, and regular security training that includes recognizing and defending against the latest threats.

**Physical Protection**

TASER International maintains policies and practices for physical protection of Evidence.com. These include biometric access controls for TASER facilities, physical access management procedures, and identification badge standards.

The Evidence.com data centers are managed by Amazon Web Services (AWS). TASER regularly validates audit results of AWS security practices to ensure the data center physical security practices are robust and effective. AWS provides many layers of physical security for their data centers. AWS data centers are housed in nondescript facilities. Physical access is strictly controlled both at the perimeter and at building ingress points by professional security staff utilizing video surveillance, intrusion detection systems, and other electronic means. Authorized staff must pass two-factor authentication a minimum of two times to access data center floors. AWS only provides data center access and information to employees and contractors who have a legitimate business need for such privileges. When an employee no longer has a business need for these privileges, his or her access is immediately revoked, even if they continue to be an employee of Amazon or AWS. All physical access to data centers by AWS employees is logged and audited routinely. See the AWS Security Whitepaper for more details: <http://aws.amazon.com/security/>

**Risk Management**

TASER International maintains policies and practices for risk management of Evidence.com. These include various types of risk assessments, practices to identify and address high-risk issues, regular assessments to test security control effectiveness, and security metrics for continuous monitoring.

**Third-Party Security Management**

TASER International maintains policies and practices for vendor security management related to Evidence.com. These include vendor security evaluations and review of audit reports to ensure security and compliance expectations are being met.

**Cyber Insurance**

TASER International has a comprehensive cyber insurance policy which provides insurance coverage for a breach of Evidence.com and covers professional services liability, privacy liability, privacy regulatory liability, regulatory fines and penalties, and security liability. TASER International is able to issue an insurance certificate to its customers naming them as additional insureds under our cyber insurance policy for added protection.

[Version 3.1 - Released May 14th, 2015]

Ⓞ is a trademark of TASER International, Inc., and TASER is a registered trademark of TASER International, Inc., registered in the U.S. All rights reserved.  
© 2015 TASER International, Inc.