DOJ, Office of the Inspector General

Privacy Impact Assessment
for the
Inspector General's Field Investigation Support System (IGFIS)

Issued by:
Jonathan M. Malis
Senior Component Official for Privacy

Approved by: Peter Winn
Chief Privacy and Civil Liberties Officer (Acting)
U.S. Department of Justice

Date approved: [March 28, 2022]

Section 1: Executive Summary

Body Worn Cameras (BWC) can build public trust by providing transparency and accountability in circumstances where the use of force may reasonably be anticipated during planned law enforcement operations. Department of Justice, Office of the Inspector General ("OIG") agents do not engage in general policing or public patrol and do not routinely engage with the general public in response to emergency calls. Therefore, the OIG's BWC program focuses on the deployment of BWCs in planned law enforcement operations, where the use of force may reasonably be anticipated, such as the planned execution of a search warrant or arrest.

The IG's Field Investigation Support System (IGFIS) is an implementation of Axon's Body Worn Camera FedRAMP authorized Software as a Service (SaaS) solution. Its mission is to gather and preserve evidence during the specified field operations as outlined in the OIG BWC Policy, such as the execution of search and arrest warrants, including during interviews with arrestees or detainees that take place during enforcement operations, and to use for training purposes in support of OIG investigations.[1] Body worn cameras capture video and audio recordings that are then uploaded to Axon's IT system, to which OIG Special Agents (SAs) and support staff have limited access. Recordings may be used as evidence in OIG investigations as well as for OIG training purposes.

Axon's information system is comprised of a combination of two mobile applications: Axon Capture[2] and Axon View[3]; a software application: Axon View XL[4]; a vendor owned and operated cloud environment; and physical devices, i.e., the body worn cameras and supporting accessories, such as mounts and cables. Data from the body worn cameras may be uploaded via LTE cellular service[5], a docking station, and/or computer to the vendor's cloud environment. OIG has prepared a Privacy Impact Assessment for IGFIS because this system collects, maintains, and disseminates information in identifiable form about individuals. Due to the vested public interest in the use of body worn cameras by law enforcement, this PIA will be published on OIG and OPCL websites.

Section 2: Purpose and Use of the Information Technology

2.1 Explain in more detail than above the purpose of the information technology, why the information is being collected, maintained, or disseminated, and how the information will help achieve the Component's purpose, for example, for criminal or civil law enforcement purposes, intelligence activities, and administrative matters, to conduct analyses to identify

---

[1] OIG BWCs will only be used for criminal law enforcement operations, investigations, interviews, and training; they will not be used for OIG's non-criminal investigative purposes and authorities.
[2] Axon Capture is a mobile application that allows photographs and video to be uploaded from the application to the Axon digital evidence management system.
[3] Axon View is a mobile application that allows the user of an Axon Body Worn Camera to view the video currently on the camera prior to uploading it to the Axon digital evidence management system. The application is password protected and is paired directly with the agent's camera.
[4] Axon View XL is a software application that allows an Axon Body Worn Camera to be connected to a computer in order to upload recordings to the Axon digital evidence management system.
[5] The LTE function can only upload the last video recorded if the video is under one hour in duration and it can only be uploaded to evidence.com. The LTE upload requires a sequence of physical button presses on the camera. Recordings cannot be accessed or uploaded remotely by an external device and they cannot be redirected to a location other than evidence.com.

previously unknown areas of concern or patterns.

As stated above, BWCs can build public trust by providing transparency and accountability in circumstances where the use of force may reasonably be anticipated during planned law enforcement operations, as well as provide a means to gather and preserve evidence. In a memorandum issued by the Deputy Attorney General on June 7, 2021, entitled "Body Worn Camera Policy," the Bureau of Alcohol, Tobacco, Firearms, and Explosives, Drug Enforcement Administration, Federal Bureau of Investigation, and United States Marshals Service were instructed to expand the DOJ's use of Body Worn Cameras (BWCs) to federal law enforcement officers. While the OIG was not subject to the directive in this memorandum, the OIG has commenced planning to deploy BWC devices for OIG law enforcement operations consistent with this memorandum, including developing a comprehensive policy to address many of the concerns that law enforcement use of BWCs present.

2.2 Indicate the legal authorities, policies, or agreements that authorize collection of the information. (Check all that apply and include citations/references.)

	Authority	Citation/Reference
	Statute	Inspector General Act of 1978, as amended, 5 U.S.C. App. 3
	Executive Order	
	Federal Regulation	
	Agreement, memorandum of understanding, or other documented arrangement	
	Other (summarize and provide copy of relevant portion)	Deputy Attorney General Memorandum, *Body Worn Camera Policy*, June 7, 2021; *Body Worn Camera Program*, Inspector General Manual, Volume III, Chapter 236.

Section 3: Information in the Information Technology

3.1 Indicate below what types of information that may be personally identifiable in Column (1) will foreseeably be collected, handled, disseminated, stored and/or accessed by this information technology, regardless of the source of the information, whether the types of information are specifically requested to be collected, and whether particular fields are provided to organize or facilitate the information collection. Please check all that apply in Column (2), and indicate to whom the information relates in Column (3). Note: This list is provided for convenience; it is not exhaustive. Please add to "other" any other types of information.

The information collected by IGFIS includes digital evidence such as audio, video, or still images that has been captured in the normal course of law enforcement duties. Personal identifying information (PII) will be captured by BWCs when the recording device is activated during law enforcement operations. Data recorded is directly related to law enforcement activities and emergency response, and may include video images of people, driver licenses,

personal information verbally requested for the purposes of identifying individuals and/or arrests during a lawful contact, and criminal history information provided over the radio by the dispatch communications center. Information may also be obtained from publicly available sources, witnesses, concerned citizens, and any other sounds or images perceptible to the BWC from its location on the wearer. Virtually any type of PII may be collected by law enforcement officials while taking statements or during the course of an investigation.

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public - Non-USPERs	(4) Comments
Example: Personal email address	*X*	*B, C and D*	*Email addresses of members of the public (US and non-USPERs)*
Name	X	A, B, C, D	The names of targets of enforcement actions, third parties at the scene, and law enforcement officers present at the operation may be recorded by the BWC.
Date of birth or age	X	A, B, C and D	Could be discernable from the recording.
Place of birth	X	A, B, C and D	
Gender	X	A, B, C and D	Could be discernable from the recording.
Race, ethnicity or citizenship	X	A, B, C and D	Could be discernable from the recording.
Religion	X	A, B, C and D	
Social Security Number (full, last 4 digits or otherwise truncated)	X	A, B, C and D	
Tax Identification Number (TIN)			
Driver's license	X	A, B, C and D	
Alien registration number			
Passport number	X	A, B, C and D	
Mother's maiden name	X	A, B, C and D	
Vehicle identifiers	X	A, B, C and D	Could be discernable from the recording.
Personal mailing address	X	A, B, C and D	Could be discernable from the recording.
Personal e-mail address	X	A, B, C and D	
Personal phone number	X	A, B, C and D	
Medical records number			
Medical notes or other medical or health information			
Financial account information			
Applicant information			

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public - Non-USPERs	(4) Comments
Education records			
Military status or other information	X	A, B, C and D	
Employment status, history, or similar information	X	A, B, C and D	Could be discernable from the recording.
Employment performance ratings or other performance information, e.g., performance improvement plan	X	A, B, C and D	
Certificates			
Legal documents	X	A, B, C and D	
Device identifiers, e.g., mobile devices	X	A, B, C and D	
Web uniform resource locator(s)			
Foreign activities			
Criminal records information, e.g., criminal history, arrests, criminal charges	X	A, B, C and D	
Juvenile criminal records information			
Civil law enforcement information, e.g., allegations of civil law violations			
Whistleblower, e.g., tip, complaint or referral	X	A, B, C and D	
Grand jury information	X	A, B, C and D	
Information concerning witnesses to criminal matters, e.g., witness statements, witness contact information	X	A, B, C and D	
Procurement/contracting records			
Proprietary or business information			
Location information, including continuous or intermittent location tracking capabilities	X	A, B, C and D	Location data is captured via BWC as metadata.
Biometric data:			
- **Photographs or photographic identifiers**	X	A, B, C and D	
- **Video containing biometric data**	X	A, B, C and D	Could be discernable from the recording.
- **Fingerprints**			
- **Palm prints**	X	A, B, C and D	Could be discernable from the recording.

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public - Non-USPERs	(4) Comments
- **Iris image**	X	A, B, C and D	Could be discernable from the recording.
- **Dental profile**	X	A, B, C and D	Could be discernable from the recording.
- **Voice recording/signatures**	X	A, B, C and D	Could be discernable from the recording.
- **Scars, marks, tattoos**	X	A, B, C and D	Could be discernable from the recording.
- **Vascular scan, e.g., palm or finger vein biometric data**	X	A, B, C and D	Could be discernable from the recording.
- **DNA profiles**			
- **Other (specify)**			
System admin/audit data:			
- **User ID**	X	A	
- **User passwords/codes**	X	A	
- **IP address**			
- **Date/time of access**	X	A	Date and time stamps captured in audit logs.
- **Queries run**	X	A	
- **Content of files accessed/reviewed**	X	A	
- **Contents of files**	X	A	
Other (please list the type of info and describe as completely as possible):	X	A, B, C, D	Due to the unpredictable nature of law enforcement field operations, BWC may capture other data types not indicated here.

3.2 Indicate below the Department's source(s) of the information. (Check all that apply.)

Directly from the individual to whom the information pertains:					
In person	X	Hard copy: mail/fax		Online	X
Phone		Email			
Other (specify): All data contained within the system will either originate from a BWC, which is worn by a Special Agent, is entered in the system as redaction data regarding such recordings, or for basic system maintenance, i.e. account management, multifactor authentication, etc.					

Government sources:					
Within the Component	X	Other DOJ Components	X	Online	
State, local, tribal	X	Foreign (identify and provide the international agreement, memorandum of understanding, or other documented arrangement related to the transfer)			
Other (specify): OIG operations are almost always related to OIG investigations concerning DOJ employees. However, it is possible that OIG Special Agents may be called upon to support other law enforcement efforts as needed in special circumstances, e.g., disaster recovery, etc.					

Non-government sources:					
Members of the public	X	Public media, Internet	X	Private sector	X
Commercial data brokers					
Other (specify): OIG Special Agents may interact with members of the public or other sources during routine law enforcement operations. These interactions may be recorded by BWC.					

Section 4: Information Sharing

4.1 Indicate with whom the component intends to share the information and how the information will be shared or accessed, such as on a case-by-case basis by manual secure electronic transmission, external user authorized accounts (i.e., direct log-in access), interconnected systems, or electronic bulk transfer.

Recipient	**How information will be shared**			
	Case-by-case	**Bulk transfer**	**Direct log-in access**	**Explain specifics of the sharing, as well as how these disclosures will support and are compatible with the purposes of the collection.**
Within the Component			X	Registered users can access recordings stored in the Evidence.com portal according to the system's role-based access controls.
DOJ Components	X			Recordings may be considered evidence that could be subject to disclosure during the investigation, prosecution and/or litigation process.
Federal entities	X			Recordings may be considered evidence that could be shared as part of the investigation process.

Recipient	How information will be shared			
	Case-by-case	**Bulk transfer**	**Direct log-in access**	**Explain specifics of the sharing, as well as how these disclosures will support and are compatible with the purposes of the collection.**
State, local, tribal gov't entities	X			Recordings may be considered evidence that could be shared as part of the investigation process.
Public				
Counsel, parties, witnesses, and possibly courts or other judicial tribunals for litigation purposes	X			Recordings may be considered evidence that could be subject to disclosure during the investigation, prosecution and/or litigation process.
Private sector				
Foreign governments				
Foreign entities				
Other (specify):			X	A limited number of highly vetted Axon employees will have access to all system data, including the content of BWC recordings.

The sharing of data from IGFIS is discussed in greater detail in Section 8.

4.2 If the information will be released to the public for "Open Data" purposes, e.g., on data.gov (a clearinghouse for data from the Executive Branch of the Federal Government), and/or for research or statistical analysis purposes, explain whether—and, if so, how—the information will be de-identified, aggregated, or otherwise privacy protected.

No information will be released to the public for Open Data and/or research or statistical analysis purposes.

Section 5: Notice, Consent, Access, and Amendment

5.1 What, if any, kind of notice will be provided to individuals informing them about the collection, use, sharing or other processing of their PII, e.g., a Federal Register System of Records Notice (SORN), providing generalized notice to the public, a Privacy Act § 552a(e)(3) notice for individuals, or both? Will any other notices be provided? If no notice is provided, please explain.

The Department's SORN OIG-001, *Office of the Inspector General Investigative Records*, 72 Fed. Reg. 36725 (July 5, 2007) covers records obtained during an investigation and provides notice regarding the collection of investigative records.

Due to the purpose and nature of the BWC system, to support law enforcement operations and investigations, individuals generally will not be given notice prior to being recorded. However, when a planned criminal law enforcement interview is recorded, agents provide notice to the person(s) that the interview is being recorded and a preamble confirming the date, time, people in attendance, and reason for the interview is given before questioning begins.[6]

5.2 What, if any, opportunities will there be for individuals to voluntarily participate in the collection, use or dissemination of information in the system, for example, to consent to collection or specific uses of their information? If no opportunities, please explain why.

Individuals generally do not have an opportunity to voluntarily participate in BWC recordings if they are present during a law enforcement operation where a BWC is deployed. However, OIG agents equipped with BWCs are instructed to be mindful of locations where recording may be considered insensitive, inappropriate, or prohibited by privacy policies. Agents are reminded during training that the BWC captures a 146-degree field of view and has several microphones. Agents are also reminded that they should be aware of what they are seeing and hearing because that is being recorded by the BWC.

5.3 What, if any, procedures exist to allow individuals to gain access to information in the system pertaining to them, request amendment or correction of said information, and receive notification of these procedures (e.g., Freedom of Information Act or Privacy Act procedures)? If no procedures exist, please explain why.

In all circumstances, BWC recordings shall be treated as law enforcement sensitive information, the premature disclosure of which could reasonably be expected to interfere with enforcement proceedings. BWC recordings will also be treated as potential evidence in a federal investigation subject to applicable federal laws, rules, chain of custody requirements, and policies concerning disclosure. All requests for OIG BWC recordings unrelated to a pending OIG criminal investigation or case will be forwarded to the Office of General Counsel, which is responsible for processing and responding to such requests.

In any situation where BWCs record content that otherwise should not be shared because of law enforcement sensitivities or privacy concerns, which could include activities involving classified information, undercover personnel, confidential sources, sensitive investigative techniques or equipment, minors, injured or incapacitated individuals, or sensitive locations such as restrooms, locker rooms, or medical facilities, the BWC Program Manager, in consultation with the General Counsel or his or her designee, may use redaction software to blur images or portions of images, or minimize audio content, when making copies of BWC recordings for any authorized purpose.

All FOIA and Privacy Act procedures are handled by the DOJ OIG's Office of General Counsel. System data will be made available to DOJ OIG's OGC as needed. DOJ OIG's OGC

[6] DOJ-OIG-001 notes that the Attorney General has exempted this system of records from Subsection (e)(3) of the Privacy Act. The Privacy Act, however, limits this exemption to certain criminal law enforcement purposes.

is responsible for determining what information (if any) may be withheld from disclosure pursuant to FOIA.

Section 6: Maintenance of Privacy and Security Controls

6.1 The Department uses administrative, technical, and physical controls to protect information. Indicate the controls below. (Check all that apply).

X	**The information is secured in accordance with Federal Information Security Modernization Act (FISMA) requirements, including development of written security and privacy risk assessments pursuant to National Institute of Standards and Technology (NIST) guidelines, the development and implementation of privacy controls and an assessment of the efficacy of applicable privacy controls. Provide date of most recent Authorization to Operate (ATO):** **If an ATO has not been completed, but is underway, provide status or expected completion date:** ATT (authority to test) most recently approved 12/30/21. ATO (Authority to Operate) is expected to be approved 4/01/22. **Unless such information is sensitive and release of the information could pose risks to the component, summarize any outstanding plans of actions and milestones (POAMs) for any privacy controls resulting from the ATO process or risk assessment and provide a link to the applicable POAM documentation:**
	This system is not subject to the ATO processes and/or it is unclear whether NIST privacy controls have been implemented and assessed. Please explain:
X	**Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify:** Security control assessments, both OIG and Axon, are conducted on a routine[7] basis as required by NIST, FedRAMP, and DOJ requirements.
X	**Auditing procedures are in place to ensure compliance with security and privacy standards. Explain how often system logs are reviewed or auditing procedures conducted:** Pursuant to the requirements outlined by NIST and within the System Security Plan for the system, system audit log reviews are conducted weekly by Axon and the OIG. Axon provides the customer access to a subset of logs pertaining to evidence data interactions, user logins, and administrative activity of customer administrators of the customer's instance of the system. The System Owner, in consultation with the Information System Security Officer, is responsible for reviewing the customer accessible logs for indications of inappropriate or unusual activity. This review is required to be completed and recorded weekly.
X	**Contractors that have access to the system are subject to information security, privacy and other provisions in their contract binding them under the Privacy Act, other applicable laws, and as required by DOJ policy**.

[7] All security controls are required to be assessed at least once every three years. A subset of controls are assessed each year, throughout the year, but that subset changes per FedRAMP's or DOJ's guidance.

X	**Each component is required to implement foundational privacy-related training for all component personnel, including employees, interns, and contractors, when personnel on-board and to implement refresher privacy training annually. Indicate whether there is additional training specific to this system, and if so, please describe:** Training for BWC deployment consists of three modules: (a) prior to deployment of BWCs, each OIG agent must complete an OIG-approved initial training module to ensure the proper use and operation of the BWC, as well as compliance with privacy and civil liberties laws; (b) OIG agents must complete a semi-annual BWC familiarization module in conjunction with control tactics training or firearms training, to maintain proficiency in the use of BWCs and ensure continued functionality of the devices; and (c) OIG agents must receive a refresher module during OIG in-service training to ensure the proper use of the BWC, as well as compliance with privacy and civil liberties laws. Additionally, OIG agents are advised that recordings that contain case-pertinent information are to be kept in accordance with the rules of evidence outlined in OIG's evidence policy.

6.2 Explain key privacy and security administrative, technical, or physical controls that are designed to minimize privacy risks. For example, how are access controls being utilized to reduce the risk of unauthorized access and disclosure, what types of controls will protect PII in transmission, and how will regular auditing of role-based access be used to detect possible unauthorized access?

The Axon Security Team is responsible for implementing the appropriate physical and technical safeguards to prevent unauthorized access to the system, including evidence.com and related mobile applications. Noted security features include, without limitation, transport layer security encryption, AES 256-bit encryption, role-based user security, watermark screenshots, firewall compatibility, and a password-protected meeting option. This ensures that the recordings and associated data is encrypted in transit and while at rest. It is Axon's responsibility to collect and monitor the system's audit logs to ensure the system has not been hacked or otherwise compromised.[8]

Authorized user accounts have access to their own recordings via the web portal or desktop application. Administrative access is required to view other content and/or activity created by other users. Administrators have access to all recordings and the authority to change user permissions. All other users do not have direct access to recordings other than their own. This system is an implementation of the FedRAMP authorized, Axon - US Axon FedCloud solution. As such, the cloud service provider's compliance with monitoring privileged user activity is monitored by FedRAMP and the Third Party Assessment Organization (3PAO). The OIG, specifically the System Owner in consultation with the Information System Security Officer, reviews the CSP provided audit logs for indications of inappropriate or unusual activity for both privileged and general OIG users of the system.

6.3 Indicate how long the information will be retained to accomplish the intended purpose, and how it will be disposed of at the end of the retention period. (Reference the applicable retention schedule approved by the National Archives and Records Administration, if

[8] A limited number of highly vetted Axon employees will have access to all system data, including the content of BWC recordings.

available.)

BWC recordings will be securely stored according to the following OIG-mandated procedures. Recordings will be maintained in an OIG-controlled Microsoft Azure Government cloud storage service where they are initially uploaded. Recordings will be organized and retrieved by case number. BWC recordings associated with information pertinent to the case being investigated, such a spontaneous statement of a subject, witness, or law enforcement officer, will be kept with the case file in accordance with OIG's case records retention policy (Inspector General Manual (IGM)III-100 and IGM V-240) and consistent with federal law.

BWC recordings[9] that are or become associated with use of force incidents involving OIG employees, complaints or allegations made against OIG employees, or any other investigations of OIG employees, will be retained as directed by the AIGI or his or her designee in consultation with the General Counsel.

BWC recordings associated with normal training exercises (i.e., no injuries) will be deleted after the appropriate instructor (firearms instructor, control tactics instructor, use of force instructor, etc.) reviews the recordings for teachable scenarios and confirms it is acceptable to delete the recording. If a teachable scenario is found, the instructor will ask the OIG agent(s) involved if they would like their faces redacted and/or voices changed from the recording before its use in future trainings. In these circumstances, the BWC Program Manager will redact faces and change voices, as requested and pursuant to a process outlined in OIG BWC Policy distinct from that referenced in Section 5.3 above. The unredacted BWC recording will be deleted after all changes are made to the training video.

BWC recordings that are not associated with complaints or allegations made against OIG employees and do not contain information pertinent to the case being investigated will be deleted five (5) years following case closure, unless a request is provided in writing to the BWC Program Manager through the Assistance Inspector General for Investigations (AIGI) or their designee.

Any request to delete a portion or portions of the recordings (e.g., accidental recording) must be submitted via a memorandum from the OIG agent, through his or her supervisor and the Special Agent in Charge, and approved in writing by the Assistant Inspector General for Investigations or his or her designee, the Deputy Inspector General, or the Inspector General, in consultation with the General Counsel. The memorandum must state the reason(s) for the request to delete the recording. If the request is approved, the request memorandum and the written approval will be provided to the BWC Program Manager. The BWC Program Manager may delete the recording only after receiving the requested memorandum and written approval. All requests and final decisions will be maintained by the BWC Program Manager.

Section 7: Privacy Act

7.1 Indicate whether information related to U.S. citizens or aliens lawfully admitted for

[9] Again, OIG only uses BWCs as part of OIG's execution of criminal law enforcement authorities and training in support of those authorities.

permanent residence will be retrieved by a personal identifier (i.e., indicate whether information maintained by this information technology will qualify as "records" maintained in a "system of records," as defined in the Privacy Act of 1974, as amended).

_____ No. __X___ Yes.

7.2 Please cite and provide a link (if possible) to existing SORNs that cover the records, and/or explain if a new SORN is being published:

OIG-001, *Office of the Inspector General Investigative Records*, 72 Fed. Reg. 36725 (July 5, 2007) and amended by 82 Fed. Reg. 24151, 160 (May 25, 2017). Exemptions Claimed Pursuant to 5 U.S.C. 552a(j)(2), (k)(1), and (k)(2). See 28 C.F.R. § 16.75.

Section 8: Privacy Risks and Mitigation

When considering the proposed use of the information, its purpose, and the benefit to the Department of the collection and use of this information, what privacy risks are associated with the collection, use, access, dissemination, and maintenance of the information and how are those risks being mitigated?

Axon's Body Worn Camera system satisfies FedRAMP's standards for protecting sensitive information at the Moderate impact level. In order to ensure the OIG's use of BWCs fits within the Moderate impact level, a number of limitations have been placed on OIG's use of BWCs. For example, OIG's Body Worn Camera Policy prohibits the use of BWCs to record personnel conducting activities involving classified information, it requires the blurring of images or portions of images when making copies of BWC footage for disclosure when law enforcement sensitives or privacy concerns are present including undercover personnel, confidential sources, sensitive investigative techniques, minors, or sensitive locations. The policy further mandates a pre-operational briefing to include a discussion of steps to avoid recording undercover personnel or confidential informants or sources. Further, OIG's Standard Operating Procedures require that if an undercover agent will be participating in an operation where BWCs are used, the Body Worn Camera Manager shall be notified to ensure the protection of the undercover agent's identity in circumstances where the recording may be released outside of the OIG.

In situations where sensitive law enforcement information or high confidentiality impact level information is recorded with the BWCs such as undercover personnel or confidential informants, the BWC program manager will generate a hash value for the recording, save a copy to a separate OIG-controlled storage location protected at a high impact level and designated for sensitive law enforcement information, verify the hash value match of the original recording and the copy, and then purge the original recording from evidence.com after receiving OGC approval.

Risk: Inaccurate or altered recordings.

Mitigation: Agents are provided training on how to use and upload recordings to the Axon digital evidence management system (DEMS). Cameras are barcoded and tracked by serial number. Agents are assigned a specific camera with an agency applied barcode. The barcodes are tracked in an asset management system. The serial number for the camera is assigned to the agent in the DEMS and all recordings uploaded to DEMS are stamped with the agents' identifiers. Recordings can only be

uploaded through Axon docking stations, LTE upload, and Axon View XL software which may be installed on the agent's computer. The docking station automatically pulls the recordings from the camera and uploads them directly to DEMS. The LTE upload must be initiated by the agent conducting a certain sequence of button presses and cannot be used to alter the video in any manner. The Axon View XL software allows agents to upload recordings to the DEMS by connecting the BWC to the computer through a USB cord. Again, agents have no ability to alter the recording during this process. Access to Axon View XL is username and password protected.

It is worth noting that recordings are only able to be edited by a system administrator or a user with a redaction license. All edited recordings are marked "edited" and the original recordings are kept separate and identifiable from the edited recordings.

Risk: Improper safeguards during the transfer of data.

Mitigation: Recordings on the camera are only able to be downloaded to the system through a docking station, connection to a computer with Axon View XL software (username and password required), or through cellular connection directly from the camera as stated above. Recordings are automatically encrypted and routed to the DEMS by the camera when downloaded. If a camera is lost prior to uploading video, the video will not be able to be recovered remotely. If a camera is destroyed, forensic recovery methods can be attempted if the solid-state embedded media card is viable.

Risk: Unauthorized access to data.

Mitigation: Axon DEMS requires username, password, and multifactor identification code to gain access. Once access is granted, all actions taken within the system are tracked and viewable in an audit report accessible by the system administrators. Administrators can remove or suspend users when they leave the agency or when exigent circumstances exist.

Risk: Unauthorized sharing or dissemination of recordings.

Mitigation: Recordings can be shared within the Axon DEMS by providing an internal link to other Axon users or an external link to non-Axon users. The external link requires the user to set up a temporary Axon account to view the information. Agents and administrators sharing the recordings can set parameters regarding how long the recording will be shared and who can view the recordings. External users are not permitted to download the recordings. Only administrators can redact recordings. Once a recording is redacted, the original recording remains in the system and the redacted recording is stamped as redacted. All access, viewing, sharing, redaction, and associated actions are captured by the Axon DEMS and available in a detailed audit report. Recordings are watermarked with the name of the person viewing the recording as well as the associated meta-data.