



U.S. DEPARTMENT OF AGRICULTURE

PRIVACY IMPACT ASSESSMENT

VERSION 1.4

OFFICE OF THE CHIEF PRIVACY OFFICER

The completion of USDA Privacy Impact Assessments (PIAs) is mandated for any rulemaking, program, system, or practice that collects or uses PII under the authority of the E-government Act of 2002 (44 U.S.C. § 208(b)) and USDA DR 3515-002, Privacy Policy and Compliance for Personally Identifiable Information (PII).

The PIA is designed to identify risk associated with the use of PII by a system, program, project or practice, and to ensure that vital data stewardship issues are addressed for all phases of the System Development Life Cycle (SDLC) of IT systems. It also ensures that security and privacy protections are built into an IT system during its development cycle. By regularly assessing privacy concerns during the development process, USDA ensures that proponents of a program or technology have taken its potential privacy impact into account from the beginning. The PIA also serves to help identify what level of security risk is associated with a program or technology. In turn, this allows the Department to properly manage the security requirements under the Federal Information Security Management Act (FISMA).

USDA DR 3515-002, Privacy Policy and Compliance for Personally Identifiable Information (PII).

Please note that the E-government Act of 2002 requires that a PIA be made available to the public. In order to comply with this requirement, PIAs will be published online for the general public to view. When completing this document please use simple, straight-forward language, avoid overly technical terminology, and write out acronyms the first time you use them to ensure that the document can be read and understood by the general public.

Guidance on how to complete the following PIA Questionnaire is available [here](#).

Privacy Impact Assessment for the USDA IT System/Project:

Law Enforcement and Investigations Vault

(LEI Vault)

Law Enforcement and Investigations

NRE Forest Service

Date PIA submitted for review:

07 Mar 2024

Mission Area System/Program Contacts:

Mission Area Privacy Officer	Cynthia Ebersohn	cynthia.ebersohn@usda.gov	816-286-5272
Information System Security Officer	Darin Crisp	darin.crisp@usda.gov	208-995-4747
System/Program Manager	Curtis Davis	curtis.davis@usda.gov	912-554-4268

Abstract

The abstract provides the simplest explanation for the “what does the system do?” and will be published online to accompany the PIA link.

The USDA Forest Service Law Enforcement and Investigations’ (LEI) directorate is operating in production a Digital Media Evidence (DME) storage tool called LEI Vault. This system is the USDA-Forest Service implementation of storage to support Body Worn Camera (BWC) technology used by USDA Forest Service Law Enforcement Personnel. This PIA is being prepared because the DME is a data collection methodology that can capture a video image and audio recording of any type of privacy information, to include interviews with confidential informants, images of death, violence and mayhem, and video statements from victims of crime. Video and audio information is collected and is stored according to date. Video and audio information is not searchable by personal name or other identity information.

Overview

The overview is the most important section of the PIA. A thorough and clear overview gives the reader the appropriate context to understand the responses in the PIA.

LEI Vault is a centralized repository within the USDA Forest Service that exists as a separately accredited boundary supporting Law Enforcement and Investigations pursuant to Title 16, subsection I, U.S. Code § 559e-Forest Service Authorization. LEI Vault’s boundary incorporates the data produced from Body Worn Cameras (BWC) and the PII necessary to establish accounts and authorizations for the users. The camera technology is maintained by contract with Axon Federal within the Axon FedRAMP boundary.

Based on the Privacy Threshold Analysis (PTA), it was determined that LEI Vault can collect and store privacy information in image format when the item held in front of the camera during officer interaction with the public. A PIA is required.

LEI Vault provides the necessary and large capacity data storage to meet the requirements that underly the fielding of BWC equipment to individual law enforcement officers (LEO) and special agents (SA) by the USDA FS LEI directorate. BWCs are cameras with a microphone and internal data storage. They provide digital video and audio footage, known as Digital Media Evidence (DME), of officer interactions with the public. Cameras are typically designed to be located on an officer’s chest or head but may also be configured to deploy as part of a weapon.

Body-worn cameras are widely used by law enforcement agencies in the United States. They are authorized for use without prior notification under 18U.S.C. § 2511(2)(c&d). They are worn principally by officers in the performance of duties that require open and direct contact with the public. They support FS-LEI’s operational needs pursuant to U.S. Code § 559c- Powers of Officers and Employees of Forest Service.

LEI Vault leverages the FedRAMP-accredited cloud resources provided under contract by Axon Federal (Axon Evidence(dot)com) to store and manage law enforcement officers' digital media evidence (such as camera footage and audio recordings of interviews) and to provide a central management console for associated products and devices. All data originate with and is consumed by authorized USDA FS LEI law enforcement personnel and staff. The Forest Service retains ownership of all data associated with LEI Vault. All data is subject to the USDA FS LEI organization policies in place to govern this data, to include privacy and organization-level security.

Information is shared by LEI Vault. Information is shared two ways. The administrative account data for users is shared with USDA e-Auth, which is covered under an Interconnection Security Agreement (ISA). DME may be shared as part of a case file, on a piecemeal basis, but is not shared as part of a data sharing agreement. The shared DME is not searchable by PII.

Users of this system are either sworn law enforcement officers or are directly associated with the law enforcement and investigation directorate in support of the LEI mission. As a typical transaction, at the end of shift, policy requires an officer to authenticate into a workstation using a LincPass card and connect the BWC to a docking station paired with the workstation. The officer will open a browser link to the LEI Vault storage instance, authenticate into the storage repository and upload the days' video and audio.

Section 1.0 Authorities and Other Requirements

The following questions are intended to identify all statutory and regulatory authority for operating the project, including the authority for collection, what SORN applies, if an ATO has been completed and if there is Paperwork Reduction Act coverage.

1.1. What legal authorities and/or agreements permit the collection of information by the project or system?

FS LEI Vault is a law enforcement system, used by law enforcement personnel in the performance of their duties. It records a stream of video and audio information that is not searchable by text-based searching.

The information gathered is collected in support of the law enforcement mission of the Forest Service Law Enforcement and Investigations organization, established under Title 16, subsection I, U.S. Code § 559e- Forest Service Authorization; and U.S. Code § 559c-Powers of Officers and Employees of Forest Service. The use of recording equipment by law enforcement officers is supported by 18 U.S.C. § 2511(2)(c).

Additionally, the federal wiretap act provides for one party consent to record an interaction. 18 USC § 2511, the federal Wiretap Act, makes it illegal to intercept, disclose, or use the contents of any wire, oral, or electronic communication through the use of a “device”. It requires that one person involved in the interchange be aware and give permission.

This is the principle of one-party consent. It's not illegal if one party to the conversation consents to the interception.

18 U.S.C. § 2511 states:

(c) It shall not be unlawful under this chapter for a person acting under color of law to intercept a wire, oral, or electronic communication, where such person is a party to the communication or one of the parties to the communication has given prior consent to such interception; and

(d) It shall not be unlawful under this chapter for a person not acting under color of law to intercept a wire, oral, or electronic communication where such person is a party to the communication or where one of the parties to the communication has given prior consent to such interception unless such communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State.

1.2 Has Authorization and Accreditation (A&A) been completed for the system?

Yes

1.3. What System of Records Notice(s) (SORN(s)) apply to the information?

NRE FS LEI information is covered under SORN FS33

1.4. Is the collection of information covered by the Paperwork Reduction Act?

No

Section 2.0 Characterization of the Information

The following questions are intended to define the scope of the information requested and collected as well as the reasons for its collection as part of the program, IT system, or technology being developed.

2.1. What information is collected, used, disseminated, or maintained in the system/program?

PII is defined as information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual. Mark all applicable PII and data elements in the table.

Please check any information listed below that your system collects, uses, disseminates, creates, or maintains. If additional sensitive PII is collected, used, disseminated, created, or maintained, please list those in the text box below:

Identifying Numbers					
☐	Social Security number		☐	Truncated or Partial Social Security number	
☒	Driver's License Number		☐	License Plate Number	
☐	Registration Number		☒	File/Case ID Number	
☐	Student ID Number		☐	Federal Student Aid Number	
☐	Passport number		☐	Alien Registration Number	
☐	DOD ID Number		☐	DOD Benefits Number	
☐	Employee Identification Number		☐	Professional License Number	
☐	Taxpayer Identification Number		☐	Business Taxpayer Identification Number (sole proprietor)	
☐	Credit/Debit Card Number		☐	Business Credit Card Number (sole proprietor)	
☐	Vehicle Identification Number		☐	Business Vehicle Identification Number (sole proprietor)	
☐	Personal Bank Account Number		☐	Business Bank Account Number (sole proprietor)	
☐	Personal Device Identifiers or Serial Numbers		☐	Business device identifiers or serial numbers (sole proprietor)	
☐	Personal Mobile Number		☐	Business Mobile Number (sole proprietor)	
☐	Health Plan Beneficiary Number				
Biographical Information					
☒	Name (including nicknames)		☐	Gender	
☒	Date of Birth (MM/DD/YY)		☐	Ethnicity	
☐	Country of Birth		☐	City or County of Birth	
☐	Citizenship		☐	Immigration Status	
☒	Home Address		☐	Zip Code	
☐	Spouse Information		☐	Sexual Orientation	
☐	Marital Status		☐	Military Service Information	
☐	Race		☐	Nationality	
☐	Personal e-mail address		☐	Business e-mail address	
☐	Employment Information		☐	Alias (username/screenname)	
☐	Education Information		☐	Resume or curriculum vitae	
☐			☐	Business Mailing Address (sole proprietor)	
☐			☐	Business Phone or Fax Number (sole proprietor)	
☐			☐	Group/Organization Membership	
☐			☐	Religion/Religious Preference	
☐			☐	Home Phone or Fax Number	
☐			☐	Children Information	
☐			☐	Mother's Maiden Name	
☐			☒	Global Positioning System (GPS)/Location Data	
☐			☐	Personal Financial Information (including loan information)	
☐			☐	Business Financial Information (including loan information)	
☐			☐	Professional/personal references	
Biometrics/Distinguishing Features/Characteristics					
☐	Fingerprints		☐	Palm prints	
☐	Retina/Iris Scans		☐	Dental Profile	
☐	Hair Color		☐	Eye Color	
☒	Video recording		☒	Photos	
☐	DNA Sample or Profile		☐	Signatures	
☐			☐	Vascular scans	
☐			☐	Scars, marks, tattoos	
☐			☐	Height	
☒			☒	Voice/ Audio Recording	
☐			☐	Weight	
Medical/Emergency Information					

☐	Medical/Health Information	☐	Mental Health Information	☐	Disability Information
☐	Workers' Compensation Information	☐	Patient ID Number	☐	Emergency Contact Information
Device Information					
☐	Device settings or preferences (e.g., security level, sharing options, ringtones)	☐	Cell tower records (e.g., logs, user location, time, etc.)	☐	Network communications data
Specific Information/File Types					
☐	Personnel Files	☒	Law Enforcement Information	☐	Credit History Information
☐	Health Information	☐	Academic/Professional Background Information	☒	Civil/Criminal History Information/Police Record
☒	Case files	☐	Security Clearance/Background Check	☐	Taxpayer Information/Tax Return Information

Digital Media Evidence (DME) is the primary information collected, used, disseminated, or maintained in the system. DME is audio and visual camera footage. LEI Vault is the Forest Service-provided physical hosting environment for this material. All DME is managed through LEI Vault. A secondary information type is the account management data required to establish and authorize access for the users of the system. This is minimal in nature (such as name and duty station), with the USDA e-Auth system providing most of the data management for LEI Vault account authentication.

2.2. What are the sources of the information in the system/program?

The primary source of information in the system originates with the body-worn camera (BWC) equipment. This produces data in the form of audio and video computer files. This data becomes information after review by the officer. A corollary source of information is produced when an individual speaks with an interviewing officer while being recorded. The secondary source is the limited information input of the officer's user data by the WO Admin when the account is created.

2.2.1. How is the information collected?

The information is collected during a law enforcement officer's interaction with the public. It consists of camera footage generated by a BWC. The information is collected when the camera is turned on and stored in an MPEG-4 media file. The footage is uploaded in whole daily to the LEI Vault repository, where it is maintained under the custody of the USDA Forest Service Law Enforcement and Investigations directorate. A minor secondary type of information is gathered when the user account is first created by the WO-Admin. This secondary type is considered "Business



Privacy Impact Assessment

Personae”, it is name, duty location and badge number. This information is directly related to job requirement, as described above in Section 1.

2.3. Does the project/program or system use information from commercial sources or publicly available data. If so, explain why this is used?

No

2.4. How will the information be checked for accuracy? How often will it be checked?

The digital media is comprised of video footage. This footage is an immutable camera record of the officer’s interactions with the public. It is not subject to checks for accuracy. However, it is subject to checks by specially trained personnel for clarity, usefulness, and other procedural practice as part of the supervisor’s review.

2.5. Does the system/program use third-party websites?

No

2.5.1. What is the purpose of the use of third-party websites?

N/A

2.5.1.1. What PII will be made available to the agency though the use of third-party websites?

N/A

2.6. PRIVACY IMPACT ANALYSIS: Related to Characterization of the Information.

Follow the format below:

Privacy Risk: The risks to privacy presented by this tool include:

- 1.** Loss of control of data
- 2.** Unnecessary recording
- 3.** Use of video evidence within a court hearing.
- 4.** Improper use of video recording for covert purposes
- 5.** Loss/Compromise/Corruption of data at rest

The five risks outlined above translate to five negative outcomes specifically posed by risk of loss of control of the DME video, in order from least to most impactful:

1. The agency’s reputation is likely to be damaged;

Privacy Impact Assessment

2. Financial penalties and damages can be incurred that could exceed more than US\$5 million dollars.
3. Any legal case associated to this video may suffer an impact from illegal release of this information;
4. The individuals in the video (typically the victims of the incident) could be recognized and come to harm, or their identifying information could be harvested and used for identity theft; and
5. **Most Impact:** The loss of account information could pose a threat to an officer, or to the stored data in the system.

Mitigation: The mitigation of the above risks are delineated below:

Risk: Collection/ use / loss of data.

Solution: Access to data is only available to those LEI employees who have completed training. All access will be accomplished using two factor authentication. All data is signed for by the person receiving the data. For full disclosure, the PIA and Policy & Guideline documents will be published on the public website. Data within Axon Federal storage is NOT available to the Axon personnel.

Mitigating Measures: LincPass (PIV) two factor authentication, assigned roles for authorization, HTTPS TLS 1.2 for data transfer, Cloud Service Provider encrypted and isolated data storage, BitLocker encrypted hard drive, follow FS-LEI Policy 51 BWC Use (See detail of instructions included below.)

Risk: Footage being recorded unnecessarily.

Solution: The system has been set up to retain data for the correct retention period (maximum 90 days, before deletion). Footage deemed Evidentiary must be retained for a minimum of 10 years.

Mitigating Measures: follow FS-LEI Policy 51 BWC Use (See detail of instructions included below.)

Risk: Recorded images (in private as opposed to public areas).

Solution: There will be a log of the booked-out cameras, which shows the user who booked out the camera. Footage will NOT be permitted to be recorded in private dwellings.

Mitigating Measures: follow FS-LEI Policy 51 BWC Use (See detail of instructions included below.)

Risk: The use of images in court proceedings.

Solution: The concern arises from use of BWC footage in magistrate court, where there may be more than one case queued up for hearings. Other non-involved people may see that footage and may even surreptitiously record that footage. All officers will receive training in all the necessary technical aspects of the equipment being used. This will cover the legal implications, equipment, and practical use.

Mitigating Measures: follow FS-LEI Policy 51 BWC Use (See detail of instructions included below.)

Risk: The use or misuse for covert surveillance.

Solution: The use or misuse of BWC in covert surveillance produces risks to both subjects and to officers. If the officer fails to follow the legal requirements, a risk to the subject arises. If footage is improperly released, and a subject recognizes the viewpoint, the officer can be at risk.

Mitigating Measures: BWCs will be deployed overtly and covertly using the same protocol for both.

Risk: Loss/Compromise/Corruption of data at rest.

Solution: The Forest Service Law Enforcement Portfolio relies upon the contractual responsibilities of the Axon Federal service provider to manage access to the digital media evidence.

Mitigating Measures: Axon Federal provides a number of protections for data at rest. These are subject to FedRAMP oversight.

- File integrity is validated using cyclic redundancy checks.
- SHA hashing is used for file integrity verification.
- Database storage includes a number of inherent protective measures. The provider leverages these to protect the data at rest.
- Direct access to evidence storage would require infrastructure access as well as administrative portal access, both requiring hard token MFA.
- IP restrictions are in place for access, with modification producing alerts and investigation.
- Event logging is maintained.

Section 3.0 Uses of the Information

The following questions are intended to clearly delineate the use of information and the accuracy of the data being used.



Privacy Impact Assessment

3.1. Describe why and how the information collected, used, disseminated and/or maintained will support the program's business purpose?

The data entered for account management purposes is only used to create and manage the user account within the system. The information gathered for account management includes only name, badge number, email, region and forest evidence group (an OU). This is considered "business personae information" and identifies the person via the work environment only.

The audio visual footage, in MPEG4 format, from the BWC is primarily used to support criminal case creation. It is video and audio data that shows one view of the officer's interaction with a subject. It can be used for: evidence in court; evidence in officer discipline cases; and officer training. This data is not searchable by name or personal identifier. This data is logged in, access tracked and any output is logged and reported.

3.2. Does the system/project/program use technology to conduct electronic searches, queries, or analysis in an electronic database to discover or locate a predictive pattern or anomaly? If so, state how USDA plans to use such results.

No

3.3. PRIVACY IMPACT ANALYSIS: Related to uses of the information.

Privacy Risk: The risks to privacy presented by this tool include:

- 1.** Loss of control of data
- 2.** Unnecessary recording
- 3.** Use of video evidence within a court hearing.
- 4.** Improper use of video recording for covert purposes
- 5.** Loss/Compromise/Corruption of data at rest

The five risks outlined above translate to five negative outcomes specifically posed by risk of loss of control of the DME video, in order from least to most impactful:

1. The agency's reputation is likely to be damaged;
2. Financial penalties and damages can be incurred that could exceed more than US\$5 million dollars.
3. Any legal case associated to this video may suffer an impact from illegal release of this information;
4. The individuals in the video (typically the victims of the incident) could be recognized and come to harm, or their identifying information could be harvested and used for identity theft; and
5. **Most Impact:** The loss of account information could pose a threat to an officer, or to the stored data in the system.



Privacy Impact Assessment

Mitigation:

Risk: Collection/ use / loss of data.

Solution: Access to data is only available to those LEI employees who have completed training. All access will be accomplished using two factor authentication. All data is signed for by the person receiving the data. For full disclosure, the PIA and Policy & Guideline documents will be published on the public website. Data within Axon Federal storage is NOT available to the Axon personnel.

Mitigating Measures: LincPass (PIV) two factor authentication, assigned roles for authorization, HTTPS TLS 1.2 for data transfer, Cloud Service Provider encrypted and isolated data storage, BitLocker encrypted hard drive, follow FS-LEI Policy 51 BWC Use (See detail of instructions included below.)

Risk: Footage being recorded unnecessarily.

Solution: The system has been set up to retain data for the correct retention period (maximum 90 days, before deletion). Footage deemed Evidentiary must be retained for a minimum of 10 years.

Mitigating Measures: follow FS-LEI Policy 51 BWC Use (See detail of instructions included below.)

Risk: Recorded images (in private as opposed to public areas).

Solution: There will be a log of the booked-out cameras, which shows the user who booked out the camera. Footage will NOT be permitted to be recorded in private dwellings.

Mitigating Measures: follow FS-LEI Policy 51 BWC Use (See detail of instructions included below.)

Risk: The use of images in court proceedings.

Solution: The concern arises from use of BWC footage in magistrate court, where there may be more than one case queued up for hearings. Other non-involved people may see that footage and may even surreptitiously record that footage. All officers will receive training in all the necessary technical aspects of the equipment being used. This will cover the legal implications, equipment, and practical use.

Mitigating Measures: follow FS-LEI Policy 51 BWC Use (See detail of instructions included below.)

Risk: The use or misuse for covert surveillance.

Solution: The use or misuse of BWC in covert surveillance produces risks to both subjects and to officers. If the officer fails to follow the legal requirements, a risk to the subject arises. If footage is improperly released, and a subject recognizes the viewpoint, the officer can be at risk.

Mitigating Measures: BWCs will be deployed overtly and covertly using the same protocol for both.

Risk: Loss/Compromise/Corruption of data at rest.

Solution: The Forest Service Law Enforcement Portfolio relies upon the contractual responsibilities of the Axon Federal service provider to manage access to the digital media evidence.

Mitigating Measures: Axon Federal provides a number of protections for data at rest. These are subject to FedRAMP oversight.

- File integrity is validated using cyclic redundancy checks.
- SHA hashing is used for file integrity verification.
- Database storage includes a number of inherent protective measures. The provider leverages these to protect the data at rest.
- Direct access to evidence storage would require infrastructure access as well as administrative portal access, both requiring hard token MFA.
- IP restrictions are in place for access, with modification producing alerts and investigation.
- Event logging is maintained.

Section 4.0 Notice

The following questions are directed at providing notice to the individual of the scope of information collected, the right to consent to uses of the information, and the right to decline to provide information.

4.1. How does the project/program/system provide notice to individuals prior to collection?

Law Enforcement is not required to provide individual notification.

Body Worn Cameras are authorized for use without prior notification under 18 U.S.C. § 2511(2)(c&d). The USDA Forest Service System of Records Notice, “Department of Agriculture, Forest Service, FS-33—Law Enforcement and Investigative Records” allows Law Enforcement and Investigations to record claims and criminal activities in the National Forests which include verified violations of criminal statutes and/or Agency policy, as well as situations that may result in civil claims for or against the government.

4.2. What options are available for individuals to consent, decline, or opt out of the project?



Privacy Impact Assessment

Individuals do not have the option to consent, decline or opt-out of FS LEI Body Worn Camera recording.

4.3. PRIVACY IMPACT ANALYSIS: Related to Notice

Follow the format below:

Privacy Risk: N/A

Mitigation: N/A

Section 5.0 Data Retention

The following questions are intended to outline how long information will be retained after the initial collection.

5.1. What information is retained and for how long?

NARA guidelines identify that case files and video records are held for ten years and are considered “Temporary” (FSH 6209.11—NARA Code N1-95-10-9 Item 8). Program records and operational reports are considered “Permanent” (FSH 6209.11—NARA Code N1-95-10-9 Item 9). Video recordings not scheduled to be used by the Agency or for court proceedings (non-evidentiary) will be maintained for 90-calendar days. All evidentiary recordings will be held indefinitely if required for Litigation Holds (FS-LEI Policy 51.14.2). These are mandated by both NARA and by Litigation Hold requirements.

5.2. Has the retention schedule been approved by the USDA records office and the National Archives and Records Administration (NARA)? If so, please indicate the name of the records retention schedule.

Yes. These periods are incorporated into the law enforcement business processes of the LEI directorate, as approved by NARA when the organization was created.

The Forest Service Records Officer stated that the approval process includes subject matter experts working with the previous records officer to prepare the package for submission to NARA for final approval.

(FSH 6209.11—NARA Code N1-95-10-9 Item 8). Program records and operational reports are considered “Permanent” (FSH 6209.11—NARA Code N1-95-10-9 Item 9).

5.3. PRIVACY IMPACT ANALYSIS: Related to retention of information.

Follow the format below:

Privacy Risk: The risks to privacy presented by this tool include:

1. Loss of control of data
2. Unnecessary recording
3. Use of video evidence within a court hearing.
4. Improper use of video recording for covert purposes
5. Loss/Compromise/Corruption of data at rest

The five risks outlined above translate to five negative outcomes specifically posed by risk of loss of control of the DME video, in order from least to most impactful:

1. The agency's reputation is likely to be damaged;
2. Financial penalties and damages can be incurred that could exceed more than US\$5 million dollars.
3. Any legal case associated to this video may suffer an impact from illegal release of this information;
4. The individuals in the video (typically the victims of the incident) could be recognized and come to harm, or their identifying information could be harvested and used for identity theft; and
5. **Most Impact:** The loss of account information could pose a threat to an officer, or to the stored data in the system.

Mitigation:

Risk: Collection/ use / loss of data.

Solution: Access to data is only available to those LEI employees who have completed training. All access will be accomplished using two factor authentication. All data is signed for by the person receiving the data. For full disclosure, the PIA and Policy & Guideline documents will be published on the public website. Data within Axon Federal storage is NOT available to the Axon personnel.

Mitigating Measures: LincPass (PIV) two factor authentication, assigned roles for authorization, HTTPS TLS 1.2 for data transfer, Cloud Service Provider encrypted and isolated data storage, BitLocker encrypted hard drive, follow FS-LEI Policy 51 BWC Use (See detail of instructions included below.)

Risk: Footage being recorded unnecessarily.

Solution: The system has been set up to retain data for the correct retention period (maximum 90 days, before deletion). Footage deemed Evidentiary must be retained for a minimum of 10 years.

Mitigating Measures: follow FS-LEI Policy 51 BWC Use (See detail of instructions included below.)

Risk: Recorded images (in private as opposed to public areas).



Privacy Impact Assessment

Solution: There will be a log of the booked-out cameras, which shows the user who booked out the camera. Footage will NOT be permitted to be recorded in private dwellings.

Mitigating Measures: follow FS-LEI Policy 51 BWC Use (See detail of instructions included below.)

Risk: The use of images in court proceedings.

Solution: The concern arises from use of BWC footage in magistrate court, where there may be more than one case queued up for hearings. Other non-involved people may see that footage and may even surreptitiously record that footage. All officers will receive training in all the necessary technical aspects of the equipment being used. This will cover the legal implications, equipment, and practical use.

Mitigating Measures: follow FS-LEI Policy 51 BWC Use (See detail of instructions included below.)

Risk: The use or misuse for covert surveillance.

Solution: The use or misuse of BWC in covert surveillance produces risks to both subjects and to officers. If the officer fails to follow the legal requirements, a risk to the subject arises. If footage is improperly released, and a subject recognizes the viewpoint, the officer can be at risk.

Mitigating Measures: BWCs will be deployed overtly and covertly using the same protocol for both.

Risk: Loss/Compromise/Corruption of data at rest.

Solution: The Forest Service Law Enforcement Portfolio relies upon the contractual responsibilities of the Axon Federal service provider to manage access to the digital media evidence.

Mitigating Measures: Axon Federal provides a number of protections for data at rest. These are subject to FedRAMP oversight.

File integrity is validated using cyclic redundancy checks.

- SHA hashing is used for file integrity verification.
- Database storage includes a number of inherent protective measures. The provider leverages these to protect the data at rest.
- Direct access to evidence storage would require infrastructure access as well as administrative portal access, both requiring hard token MFA.



Privacy Impact Assessment

- IP restrictions are in place for access, with modification producing alerts and investigation.
- Event logging is maintained.

Forest Service Measures require that all FS-LEI personnel follow FS-LEI Policy 51 BWC Use (See detail of instructions included below.)

A business-related risk is that the contract with the host environment could expire or otherwise become invalid, or the organization could go out of business, and make the system and data inaccessible. Note that this is a discussion of and recognition of current limitations. While there may be mitigation by incorporating an exit strategy that includes a method for recovering the complete set of FS LEI Vault data holdings, there is not at this time such a capability. This is identified in the Business Impact Analysis. This is in discussion with the service provider to resolve, and may produce a federal-wide solution, since no other agency has this in place either, according to the provider.

Section 6.0 Information Sharing

The following questions are intended to define the content, scope, and authority for information sharing.

6.1. With which internal organizations and/or systems is information shared/received/transmitted? What information is shared/received/transmitted, and for what purpose? How is the information transmitted?

DME may be shared with department or agency attorneys outside the LEI Directorate. The attorneys may request the data in support of a legal proceeding.

LEI Vault DME is made available to stakeholders through tools provided by Axon Federal. The responsible officer first creates folders within the LEI Vault instance, then assigns a limited permission set to other individuals who require access. This permission set allows either download or streaming services. A copy of the specific DME is moved to the folder. The video may be edited, blurred or obscured for purposes of confidentiality.

In all circumstances, a pristine original is maintained by Axon Federal. Copies are made, marked, and these are provided to the requestor.

6.2. PRIVACY IMPACT ANALYSIS: Related to internal sharing and disclosure.

Follow the format below:

Privacy Risk: The risks to privacy presented by this tool include:

1. Loss of control of data
2. Unnecessary recording
3. Use of video evidence within a court hearing.
4. Improper use of video recording for covert purposes
5. Loss/Compromise/Corruption of data at rest

The five risks outlined above translate to five negative outcomes specifically posed by risk of loss of control of the DME video, in order from least to most impactful:

1. The agency's reputation is likely to be damaged;
2. Financial penalties and damages can be incurred that could exceed more than US\$5 million dollars.
3. Any legal case associated to this video may suffer an impact from illegal release of this information;
4. The individuals in the video (typically the victims of the incident) could be recognized and come to harm, or their identifying information could be harvested and used for identity theft; and
5. **Most Impact:** The loss of account information could pose a threat to an officer, or to the stored data in the system.

Mitigation:

Risk: Collection/ use / loss of data.

Solution: Access to data is only available to those LEI employees who have completed training. All access will be accomplished using two factor authentication. All data is signed for by the person receiving the data. For full disclosure, the PIA and Policy & Guideline documents will be published on the public website. Data within Axon Federal storage is NOT available to the Axon personnel.

Mitigating Measures: LincPass (PIV) two factor authentication, assigned roles for authorization, HTTPS TLS 1.2 for data transfer, Cloud Service Provider encrypted and isolated data storage, BitLocker encrypted hard drive, follow FS-LEI Policy 51 BWC Use (See detail of instructions included below.)

Risk: Footage being recorded unnecessarily.

Solution: The system has been set up to retain data for the correct retention period (maximum 90 days, before deletion). Footage deemed Evidentiary must be retained for a minimum of 10 years.

Mitigating Measures: follow FS-LEI Policy 51 BWC Use (See detail of instructions included below.)

Risk: Recorded images (in private as opposed to public areas).

Privacy Impact Assessment

Solution: There will be a log of the booked-out cameras, which shows the user who booked out the camera. Footage will NOT be permitted to be recorded in private dwellings.

Mitigating Measures: follow FS-LEI Policy 51 BWC Use (See detail of instructions included below.)

Risk: The use of images in court proceedings.

Solution: The concern arises from use of BWC footage in magistrate court, where there may be more than one case queued up for hearings. Other non-involved people may see that footage and may even surreptitiously record that footage. All officers will receive training in all the necessary technical aspects of the equipment being used. This will cover the legal implications, equipment, and practical use.

Mitigating Measures: follow FS-LEI Policy 51 BWC Use (See detail of instructions included below.)

Risk: The use or misuse for covert surveillance.

Solution: The use or misuse of BWC in covert surveillance produces risks to both subjects and to officers. If the officer fails to follow the legal requirements, a risk to the subject arises. If footage is improperly released, and a subject recognizes the viewpoint, the officer can be at risk.

Mitigating Measures: BWCs will be deployed overtly and covertly using the same protocol for both.

Risk: Loss/Compromise/Corruption of data at rest.

Solution: The Forest Service Law Enforcement Portfolio relies upon the contractual responsibilities of the Axon Federal service provider to manage access to the digital media evidence.

Mitigating Measures: Axon Federal provides a number of protections for data at rest. These are subject to FedRAMP oversight.

- File integrity is validated using cyclic redundancy checks.
- SHA hashing is used for file integrity verification.
- Database storage includes a number of inherent protective measures. The provider leverages these to protect the data at rest.
- Direct access to evidence storage would require infrastructure access as well as administrative portal access, both requiring hard token MFA.
- IP restrictions are in place for access, with modification producing alerts and investigation.



Privacy Impact Assessment

- Event logging is maintained.

6.3. With which external organizations (outside USDA) is information shared/received/transmitted? What information is shared/received/transmitted, and for what purpose? How is the information transmitted?

This information may be shared with Department of Justice and US Attorneys for the purpose of trial/prosecution. Information is also shared w/defense attorneys, district attorneys and other law enforcement agencies for the same purposes and pursuant to discovery. As well, per the mandates in EO 14074, federal LEI agencies are required to make video involving in-custody death or serious bodily injury available to the general public following procedures yet to be determined by the White House. The FS LEI has been invited and is participating in the workgroup developing those White House required procedures.

The information may also be used for internal FS LEI training or alerting purposes. In this case, only FS LEI officers would be involved. Redaction may or may not occur depending on the reasons for the training or content. For instance, a use of force case identified to correct a procedure might have redacted information and blurred features. However, a daily brief for a Be On Look Out (BOLO) officer safety alert might show full features, vehicle license or home address, and similar identifying characteristics.

A further information-sharing scenario may involve sharing with local LE cooperating agencies. In this case, a daily brief for a Be On Look Out (BOLO) officer safety alert might show full features, vehicle license or home address, and similar identifying characteristics.

The sharing of personally identifiable information outside the Department (legal entities) is compatible with the original collection of information as evidence. The information is collected for the purposes of prosecution of criminal activities. It further facilitates investigations of accusations of officer misconduct, officer training in certain instances, and as briefing material for officer safety alerts. (See Item 1.6). The information gathered is digital imaging and audio. While considered PII, the images are stored by date, not by a unique retrievable identifier of individuals. Because of this, No SORN is required.

The information stored as DME is shared electronically by granting the recipient a certain level of access—View/Download or simply View Only. The access is granted by the evidence owner.

6.4. PRIVACY IMPACT ANALYSIS: Related to external sharing and disclosure.

Follow the format below:

Privacy Risk:



Privacy Impact Assessment

Mitigation: Information is only shared with authorized personnel who have been approved and granted access to the system or the case file(s), following the procedures established within FS LEI Policy 51 Body Worn Camera Use (attached as Appendix A). Authorized personnel may include other law enforcement personnel, Department of Justice Prosecutors and staff, and U.S. Attorneys. These agencies require the members to maintain their agency privacy certification requirements.

Section 7.0 Redress

The following questions are directed at an individual's ability to ensure the accuracy of the information collected about him or her.

7.1. What are the procedures that allow individuals to gain access to their information?

An individual may file a FOIA request, or in the situation of an active criminal case, petition the court.

7.2. What are the procedures for correcting inaccurate or erroneous information?

N/A. Video and audio is real-time unedited recording that does not contain erroneous or inaccurate information.

7.3. How are individuals notified of the procedures for correcting their information?

N/A. Individuals do not have the ability to correct video or audio data.

7.4. If no formal redress is provided, what alternatives are available to the individual?

N/A

7.5. PRIVACY IMPACT ANALYSIS: Related to Redress.

Follow the format below:

Privacy Risk: N/A

Mitigation: N/A

Section 8 Auditing and Accountability

The following questions are intended to describe technical safeguards and security measures.



Privacy Impact Assessment

8.1. How is the information in the system/project/program secured?

LincPass (PIV) two factor authentication (personnel assurance);

Assigned roles for authorization (personnel assurance);

HTTPS TLS 1.2 for data transfer (credential loss/data corruption);

Encrypted, isolated data storage provided by CSP (credential loss/data corruption or accidental exposure);

BitLocker encrypted hard drive when necessary for direct file download (personnel practices);

FS-LEI Law enforcement policy 51.14 BWC Policy (personnel practices);

Auditing measures and technical safeguards are in place commensurate with the National Institute of Standards and Technology (NIST) Recommended Security Controls for Federal Information Systems and Organizations Moderate-Impact Baseline Special Publication (SP) 800-53, Rev. 4. This includes at a minimum:

- User identification and authentication;
- The use of network and application access controls;
- Encryption of data at rest, in transit, and in use; and
- Auditing of significant changes to systems or data.

The LEI Vault system further takes advantage of Axon Federal auditing to log individual access to the respective storage folder. The supervisors and evidence technicians have additional access, which is also logged. Any duplication or copy must first be permitted in writing by a Supervisory Special Agent (SSA) or Supervisory Law Enforcement Officer (SLEO).

FS-LEI Vault inherits encryption from Axon Federal. Due to the public nature of this document, the method of encryption can be found in the Axon Federal FedRAMP System Security Plan, control SC-13. All encryption is FIPS 140-02 compliant.

8.2. What procedures are in place to determine which users may access the program or system/project, and are they documented?

The procedures to access the system are documented in the LEI Account Management guide. There are two categories of Forest Service Personnel authorized for access to



Privacy Impact Assessment

LEI Vault. Only sworn LEI Personnel and LEI Program Specialist administrators have access to LEI Vault. LEI Vault uses role based security to define information access boundaries within the application.

8.3. How does the program review and approve information sharing requirements?

Information shared with the public must be performed in a manner consistent with applicable law, including the Privacy Act of 1974, to protect the privacy rights of individuals and to protect the integrity and security of ongoing law enforcement operations. The Forest Service does not share information except through evidentiary, Touhy, or FOIA procedures, in response to a written and valid request with the approval of the responsible Supervisory Special Agent or Supervisory Law Enforcement Officer. The Forest Service does not make copies of information requested by other agencies or parties except through administrative request, evidentiary procedures, or consent of the responsible Supervisory Special Agent or Supervisory Law Enforcement Officer.

8.4. Describe what privacy training is provided to users either generally or specifically relevant to the program or system/project?

Users of this system are either sworn law enforcement personnel or are highly trained information technology professionals employed by the Forest Service in support of the law enforcement and investigations mission.

All personnel who access the system must complete an annual security awareness training course that includes a significant amount of privacy protection information as part of the annual security awareness training required for all users of Forest Service and USDA systems.

The LEI officers and special agents also have a substantial block of mandatory privacy awareness and protection training that is updated with periodic law enforcement-related retraining.

The IT professionals are held to a higher standard of privacy awareness than non-IT professionals and are subject to annual role-based security training.



Privacy Impact Assessment

Approval Signatures:

Curtis Davis
FS LEI Vault System Owner
Law Enforcement and Investigations
NRE Forest Service
United States Department of Agriculture

Cynthia (Towers) Ebersohn
ACIO Privacy Officer
NRE Forest Service
United States Department of Agriculture

Benjamin Moreau
ACISO
NRE Forest Service
United States Department of Agriculture

Office of the Chief Privacy Officer
United States Department of Agriculture



Appendix A.

FS LEI Policy 51 Body Worn Camera Use

[51.13 - Body Worn Cameras](#)

The use of Body Worn Cameras (BWCs) provides documentary evidence for criminal investigations, internal or administrative investigations, and civil litigation. Officers shall utilize this device in accordance with the provisions in this policy to maximize the effectiveness of the audio/video documentation to achieve operational objectives and to ensure evidence integrity. All uniformed LEOs will wear a BWC in plain view while performing law enforcement duties. BWCs shall be worn in an area on the uniform shirt or approved outer carrier that has the greatest potential to capture optimal footage.

[51.13a - Operating Procedures](#)

1. BWCs shall be provided by the Agency. Using personally owned devices is prohibited.
2. This policy is not intended to describe every possible circumstance. The policy sets forth standards that imply a reasonableness and sound judgement in their application. In addition to the required conditions, Officers may activate the system any time they feel its use would be appropriate and/or valuable to document an incident. Situations that Officers shall not record are listed in section 51.31 (4) of this chapter.
3. Unless it is unsafe or impractical to do so, or mechanical issues that impede the use of the device are present, Officers shall make every attempt to activate their BWCs prior to making contact in the following incidents:
 - a. Enforcement encounters where there is a reasonable suspicion the person(s) is/are involved in criminal activity. This includes, but is not limited to, calls for service, as well as, self-initiated activities.
 - b. Any other contact that becomes adversarial after the initial contact in a situation that would not otherwise require the activation of the BWC.
4. Officers shall not use the BWC for the following situations:
 - a. Recording events of a political or religious nature absent a clear connection to an investigation.
 - b. Recording incidents that would unnecessarily infringe upon a citizen's privacy or are not critical to investigations.

Privacy Impact Assessment

- c. Unless part of an active incident or investigation, recording of other Agency/office employees is normally prohibited and shall only be conducted in accordance with departmental regulations.
 - d. Using BWCs for employees' personal use or using recordings or other data captured by government devices for personal use, including the sharing of audio or video recordings, screen captures, or other data, and posting the recordings or data on social media.
 - e. Manipulating evidence after it has been recorded. All electronic, audio, and photographic evidence must be maintained in accordance with Forest Service policy and all relevant Federal laws and procedures.
 - f. The use of BWCs in medical facilities should not include recording of sensitive or confidential patient information, unless a part of an investigation.
 - h. Privileged and confidential conversations; In order to protect attorney-client privilege, or confidential patient-doctor or pastor-citizen conversations. BWCs are prohibited in situations in which a privileged communication occurs or has been invoked and is known to the officer/agent.
 - i. To protect Officers from accusations of inappropriate recording, Officers shall ensure BWCs are off prior to entering shared restroom or locker facilities.
5. Prior to going into service, officers utilizing a BWC should ensure the device is charged and working properly. The primary storage media should have sufficient storage space and a spare should be available, if so equipped.
6. Officers shall be aware of their particular state notification requirements (privacy laws) in advance of operating a BWC. Those state requirements may affect cases that are referred through those jurisdictions.
7. Law enforcement personnel shall not erase BWC storage media, except in accordance with this policy and other relevant or related policies.
8. Lost or stolen BWCs shall be reported to the supervisor as soon as practical after discovery.
9. Officers shall comply with direction in accordance with FSH 5309.11, ch. 20, secs. 22.41 (Photographic and Video Evidence), 22.43 (Photographing Scene) and 22.44 (Video Photography).
10. An employee may review BWC files as it results to:
- a. Their involvement in an incident for the purposes of completing a criminal investigation and preparing reports.

- b. Prior to courtroom testimony or for courtroom presentation.
- c. In the case of a use of force incident, Officers shall normally be afforded the opportunity to view applicable BWC recordings before giving a statement or writing a report.
- d. Reviewing recordings for training purposes with the consent of the Officer, the Officer(s) involved or during a Field Training and Evaluation Program phase is acceptable. Law enforcement personnel are encouraged to review their own recordings. Recordings used or shown for the purpose of ridicule or embarrassing any employee are prohibited.

51.14 - Control and Preservation of Storage Media

- 1. BWCs shall be downloaded and uploaded to the video management system at the end of every shift unless mitigated by supervisor.
- 2. Video recordings not scheduled to be used by the Agency or for court proceedings (non-evidentiary) will be maintained for 90-calendar days. All evidentiary recordings will be maintained a minimum of 10 years.
- 3. Do not duplicate or issue copies of recordings except through evidentiary procedures, FOIA procedures or in response to a written request with the approval of the responsible Supervisory Special Agent or Supervisory Law Enforcement Officer.
- 4. All video recordings generated by BWCs are the property of the Forest Service and must remain under the control of the Forest Service, LEL.

51.15 - Use of Recorded Images for Training

- 1. Recorded BWC images that contain material deemed beneficial for training purposes by the responsible Supervisory Special Agent or Supervisory Law Enforcement Officer may be utilized for training with the concurrence of the Special Agent in Charge. Any Officer may recommend video recordings to be used and submit them for review and approval through the proper chain of command.
- 2. During the Field Training Program, Field Training Officers and Trainees are authorized to review BWC videos in relation to the day's training events and completion of Daily Observation Reports.