Privacy Impact Assessment

for

Law Enforcement and Investigations Vault (LEI Vault)

Policy, E-Government and Fair Information Practices

Version: 1.3

Date: 16 January 2020

Prepared for: USDA OCIO-Policy, E-Government and Fair Information Practices (PE&F)

United States Department of Agriculture

Contact Point

Curtis Davis

System Owner

USDA NRE Forest Service

703-605-4730

Reviewing Official

Cynthia Towers

Privacy Officer

USDA NRE Forest Service

(816) 844-4000

Abstract

The USDA Forest Service Law Enforcement and Investigations' (LEI) directorate is developing 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 potentially 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

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 within the LEIMARS boundary.

Based on the Privacy Threshold Analysis (PTA), it was determined that LEI Vault can potentially collect and store privacy information in image format when 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 18 U.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 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 Characterization of the Information

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

1.1 Identification

What information is collected, used, disseminated, or maintained in the system?

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.

1.2 Source

What is the source(s) of the information in the system?

The primary source of information for the system is the body-worn camera (BWC) equipment. The secondary source is the limited information input by the WO Admin when the account is created.

1.3 Justification

Why is the information being collected, used, disseminated, or maintained?

The material 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.

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.

LEI Vault is not a searchable data collection system. It stores video-data files in MPEG-4 format that are not manipulatable by data search tools.

1.4 Collection

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 Body Worn Camera (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.

1.5 Validation

How will the information be checked for accuracy?

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.

1.6 Authority

What specific legal authorities, arrangements, and/or agreements defined the collection of information?

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). Further exemptions and exclusions are provided under the Federal Freedom of Information Act (FOIA).

The Federal Freedom of Information Act (FOIA) broadly exempts from disclosure "records or information compiled for law enforcement purposes". It also provides three exclusions (two law enforcement related, and one counterintelligence related).

Per the FOIA.gov web site

FOIA Exemption 7:

Information compiled for law enforcement purposes that:

7(A). Could reasonably be expected to interfere with enforcement proceedings;

7(B). Would deprive a person of a right to a fair trial or an impartial adjudication;

7(C). Could reasonably be expected to constitute an unwarranted invasion of personal privacy;

7(D). Could reasonably be expected to disclose the identity of a confidential source;

7(E). Would disclose techniques and procedures for law enforcement investigations or prosecutions, or would disclose guidelines for law enforcement investigations or prosecutions if such disclosure could reasonably be expected to risk circumvention of the law; or

7(F). Could reasonably be expected to endanger the life or physical safety of any individual.

FOIA Exclusions

Congress has provided special protection in the FOIA for three narrow categories of law enforcement and national security records. The provisions protecting those records are known as “exclusions.”

The first exclusion protects the existence of an ongoing criminal law enforcement investigation when the subject of the investigation is unaware that it is pending, and disclosure could reasonably be expected to interfere with enforcement proceedings.

The second exclusion is limited to criminal law enforcement agencies and protects the existence of informant records when the informant’s status has not been officially confirmed. Records falling within an exclusion are not subject to the requirements of the FOIA.

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.

1.7 Risk Mitigation

Given the amount and type of data collected, discuss the privacy risks identified and how they were mitigated.

The privacy risks, solutions, and mitigations are outlined as follows:

Risk: Collection/ use / loss of data.

Solution: Access to data is only available to those that 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.

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.

Risk: Footage being recorded unnecessarily.

Solution: The system has been properly set up to retain data for the correct retention period (maximum 90 days, before deletion). This is with the exception of retained footage requested by the courts where the data is stored for a minimum of 10 years.

Mitigating Measures: follow FS-LEI Policy 51 BWC Use.

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.

Risk: The use of images in court proceedings.

Solution: 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.

Risk: The potential for covert surveillance.

Solution: BWCs will be deployed in overt and covert manners using the same protocol for both.

Mitigating Measures: follow FS-LEI Policy 51 BWC Use.

Detail of instructions 51.14 - Control and Preservation of Storage Media:

BWCs shall be downloaded and uploaded to the video management system at the end of every shift unless mitigated by supervisor;

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;

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; and

All video recordings generated by BWCs are the property of the Forest Service and must remain under the control of the Forest Service, LEI.

There are four negative outcomes specifically posed by risk of loss of control of the DME video, in order from least to most impactful:

The agency's reputation is likely to be damaged;

Any legal case associated to this video may suffer an impact from illegal release of this information;

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

The loss of account information could pose a threat to an officer, or to the stored data in the system.

Section 2.0 Uses of the Information

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

2.1 Usage

Describe all the uses of information.

The data entered for account management purposes is only used to create and manage the user account within the system.

The MPEG4 material 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.

2.2 Analysis and Production

What types of tools are used to analyze data and what type of data may be produced?

Data from the BWC is in MPEG4 format. The tools used to analyze the data are covered with the boundary of the Axon Evidence (dot) com system.

The account management data is not analyzed, in the strict definition of the word. It is used as an identifier.

2.3 Commercial/Public Use

If the system uses commercial or publicly available data, please explain why and how it is used

N/A. The BWC system does not use commercial or publicly available data

2.4 Risk Mitigation

Describe any types of controls that may be in place to ensure that information is handled in accordance with the above described uses.

N/A

Section 3.0 Retention

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

3.1 Time Period

How long is information retained?

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. (FS-LEI Policy 51.14.2)

3.2 Approval

Has the retention period been approved by the component records officer and the National Archives and Records Administration (NARA)?

Yes.

3.3 Risk Mitigation

Please discuss the risks associated with the length of time data is retained and how those risks are mitigated.

The longer any data is stored, the higher the likelihood of data loss or corruption. These risks are identified and are mitigated with the same measures described in Section 1.7 of this document.

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. This may be mitigated by incorporating an exit strategy that includes a method for recovering the complete set of FS LEI Vault data holdings.

Section 4.0 Internal Sharing and Disclosure

The following questions are intended to define the scope of sharing within the United States Department of Agriculture.

4.1 Identification and Purpose

With which organization(s) outside of the Forest Service, but still within the Department of Agriculture is the information shared? What information is shared and for what purpose?

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.

4.2 Delivery and Disclosure

How is the information transmitted or disclosed?

The information is combined into a case file and physically transported by the officer to the attorney's office, using formally established evidentiary transmittal/disclosure procedures as may be necessary to maintain chains of evidence.

4.3 Risk Mitigation

Considering the extent of internal information sharing, discuss the privacy risks associated with the sharing and how they were mitigated.

Information is only shared with authorized internal personnel who have been approved and granted access to the system. The authorized personnel are required to undergo yearly privacy training.

Section 5.0 External Sharing and Disclosure

The following questions are intended to define the content, scope, and authority for information sharing external to USDA which includes Federal, state and local government, and the private sector.

5.1 Identification and Purpose

With which external organization(s), outside of both the Forest Service and the Department of Agriculture, is the information shared? What information is shared, and for what purpose?

This information may be shared with the Department of Justice for evidentiary proceedings or for training.

5.2 Compatibility

Is the sharing of personally identifiable information outside the Department compatible with the original collection? If so, is it covered by an appropriate routine use in a SORN? If so, please describe. If not, please describe under what legal mechanism the program or system is allowed to share the personally identifiable information outside of USDA.

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. (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.

5.3 Delivery and Security Measures

How is the information shared outside the Department and what security measures safeguard its transmission?

The information is made available either to a member of the recipient organization who has met the requirements for access and has been granted user privileges to the system, or the information is combined into a case file and physically transported by the officer to the attorney's office, using established evidentiary processing procedures.

5.4 Risk Mitigation

Given the external sharing, explain the privacy risks identified and describe how they were mitigated.

Information is only shared with authorized internal personnel who have been approved and granted access to the system or the case file(s), following established procedures.

Section 6.0 System of Records Notice (SORN)

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

6.1 Requirement and Identification

Does this system require a SORN and if so, please provide SORN name and URL?

(Note: If a SORN is not required, answer "No" to this question, and "N/A" for questions 6.2 through 6.5.)

No.

LEI Vault collects and stores digital media evidence (DME) during the process of law enforcement. Per the policy described in FA LEI Policy 51-Body Worn Cameras, the officer operates the camera during interactions with the public, except in certain clearly defined circumstances. LEI Vault does not collect PII directly from the individual. The camera records anything within the field of view of the lens or auditory range of the microphone(s). The use of this video recording equipment is not a matter of choice by the subject because of the laws covering use of recording devices, and the FOIA act exemption and exclusions (as described in Item 1.6). Further, notice is not given to the subjects being recorded, as provided for officers in the course of duty in 18 U.S.C. § 2511(2)(c, d).

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.

6.2 Individual Notification

Was notice provided to the individual prior to collection of information?

N/A.

6.3 Right to Decline

Do individuals have the opportunity and/or right to decline to provide information?

N/A.

6.4 Right of Consent

Do individuals have the right to consent to particular uses of the information? If so, how does the individual exercise the right?

N/A.

6.5 Risk Mitigation

Describe how notice is provided to individuals, and how the risks associated with individuals being unaware of the collection are mitigated.

N/A.

Section 7.0 Access, Redress and Correction

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

7.1 Access

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 Correction

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 Notification

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 Redress Alternatives

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

N/A

7.5 Risk Mitigation

Please discuss the privacy risks associated with the redress available to individuals and how those risks are mitigated.

N/A

Section 8.0 Technical Access and Security

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

8.1 Procedures

What procedures are in place to determine which users may access the system and are they documented?

The procedures to access the system are documented in the LEI Account Management guide.

8.2 Contractor Access

Will Department contractors have access to the system?

No.

8.3 Privacy Training

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

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.

The LEI officers and special agents 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.

8.4 System Authority to Operate

Has Assessment & Authorization been completed for the system(s) supporting the program? If so, answer “Yes” and provide ATO expiration date(s).

Yes. ATO expiration date for LEI Vault is February 10, 2023.

8.5 Audit and Technical Safeguards

What auditing measures and technical safeguards are in place to prevent misuse of data?

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 Evidence (dot) com 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 Evidence(dot)com. Due to the public nature of this document, the method of encryption can be found in the Axon Evidence(dot)com FedRAMP System Security Plan, control SC-13. All encryption is FIPS 140-02 compliant.

8.6 Risk Mitigation

Given the sensitivity and scope of the information collected, as well as any information sharing conducted on the system, what privacy risks were identified and how do the security controls mitigate them?

There are four negative outcomes that can occur from loss of control of the DME video. From least to most impactful, first, the agency's reputation is likely to be damaged, Second, any legal case associated to this video may suffer an impact from illegal release of this information. Third, the individuals in the video could be recognized and come to harm, or their identifying information could be harvested and used for identity theft. Finally, the loss of account

information could pose a threat to an officer, or to the stored data in the system. These will be mitigated by use of:

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); and

Further information as described in Section 1.7 of this document.

Section 9.0 Technology

The following questions are directed at critically analyzing the selection process for any technologies utilized by the system, including system hardware and other technology.

9.1 Description

What type of project is the program or system?

LEI Vault is a Major Application.

9.2 Privacy Concerns

Does the project employ technology which may raise privacy concerns? If so, please discuss their implementation.

The primary technology is a digital video camera that is worn by the officer. As such it collects an image of everything in the path of the lens. This can be scenes of violence, private information on documents or even personally embarrassing situations such as nudity or partial disrobement. This is mitigated by a comprehensive use policy described in the FA-LEI Policy Item 51—Body Worn Camera System Policy.

Section 10.0 Third Party Websites/Applications

The following questions are directed at critically analyzing the privacy impact of using third party websites and/or applications.

10.1 Review

Has the System Owner (SO) and/or Information Systems Security Program Manager (ISSPM) reviewed Office of Management and Budget (OMB) memorandums M-10-22 “Guidance for Online Use of Web Measurement and Customization Technology” and M-10-23 “Guidance for Agency Use of Third-Party Websites and Applications”?

Yes.

10.2 Purpose

What is the specific purpose of the agency’s use of 3rd party websites and/or applications?

N/A

10.3 PII Availability

What Personally Identifiable Information (PII) will become available through the agency’s use of 3rd party websites and/or applications.

N/A

10.4 PII Usage

How will the PII that becomes available through the agency’s use of 3rd party websites and/or applications be used?

N/A

10.5 PII Maintenance and Security

How will the PII that becomes available through the agency’s use of 3rd party websites and/or applications be maintained and secured?

N/A

10.6 PII Purging

Is the PII that becomes available through the agency's use of 3rd party websites and/or applications purged periodically? If so, is it done automatically? If so, is it done on a recurring basis?

N/A

10.7 PII Access

Who will have access to PII that becomes available through the agency's use of 3rd party websites and/or applications?

N/A

10.8 PII Sharing

With whom will the PII that becomes available through the agency's use of 3rd party websites and/or applications be shared—either internally or externally?

N/A

10.9 SORN Requirement

Will the activities involving the PII that becomes available through the agency's use of 3rd party websites and/or applications require either the creation or modification of a system of records notice (SORN)?

N/A

10.10 Web Measurement and Customization

Does the system use web measurement and customization technology? If so, is the system and procedures reviewed annually to demonstrate compliance to OMB M-10-23?

N/A

10.11 Web Measurement and Customization Opt-In/Opt-Out

Does the system allow users to either decline to opt-in or decide to opt-out of all uses of web measurement and customization technology? If so, does the agency provide the public with alternatives for acquiring comparable information and services?

N/A

10.12 Risk Mitigation

Given the amount and type of PII that becomes available through the agency's use of 3rd party websites and/or applications, discuss the privacy risks identified and how they were mitigated.

N/A

Responsible Official

CURTIS DAVIS Digitally signed by CURTIS DAVIS
Date: 2020.05.12 13:37:31 -04'00'

Curtis Davis
System Owner (SO)
Law Enforcement and Investigations, Forest Service
United States Department of Agriculture

Approval Signature

CYNTHIA TOWERS Digitally signed by CYNTHIA TOWERS
Date: 2020.05.12 14:25:22 -05'00'

Cynthia Towers
Privacy Officer (PO)
Natural Resources and Environment, Forest Service
United States Department of Agriculture

ROBERT CHADDERDON Digitally signed by ROBERT CHADDERDON
Date: 2020.05.18 08:18:19 -06'00'

Laura Hill
Information System Security Program Manager (ISSPM)
Natural Resources and Environment, Forest Service
United States Department of Agriculture