Privacy Impact Assessment

for

Law Enforcement Investigations Reporting System (LEIRS)

Policy, E-Government and Fair Information Practices

Version: 1.0

Date: August 26, 2020

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

Contact Point

Curtis Davis

System Owner

USDA Forest Service LEI

912-554-4730

Reviewing Official

Cynthia Towers

Privacy Officer

USDA Forest Service

(816) 844-4000

DOCUMENT ADMINISTRATION

Document Revision and History

Revision	Date	Author and Title	Office	Comments
0.1	8/18/2020	B Richardson	FS ISSO Support	Draft Release
1.0	8/26/2020	B Richardson	FS ISSO Support	Initial Release

DOCUMENT REVIEW

Reviewer	Title	Date	Update Y/N	If systemic, please provide comments
C. Niffen	NRE FS Air Support	8/31/2020	Y	Comments provided to C Towers for approval
C. Towers	NRE FS Privacy Officer	9/2/2020	Y	Comments approved and additional comments provided

Abstract

The Law Enforcement and Investigations Reporting System (LEIRS) system is currently being developed to comply with the mandate to enhance and implement business processes for reporting of law enforcement activities and information to the Department of Justice (DOJ) using the National Incident Based Reporting System (NIBRS) no later than January 1, 2021. LEIRS will replace the legacy Law Enforcement and Investigations Management and Attainment Reporting System (LEIMARS). LEIMARS has provided Forest Service (FS) Law Enforcement and Investigations (LEI) with event analysis, case management, violation notice and incident reporting services for over 20 years. Even with a recent update, it is reaching end-of-life, and does not support NIBRS rules. LEIRS will be a Major Application under United States Department of Agriculture (USDA) Risk Management Framework (RMF) guidelines, National Institute of Standards and Technology (NIST) Special Publication (SP) 800-18 and Office of Management and Budget (OMB) Circular A-130 App III. It will be identified by USDA and Department of Homeland Security (DHS) as a High Value Asset. It is currently estimated LEIRS and LEIMARS will run in parallel for approximately one year prior to decommissioning LEIMARS.

When LEIRS enters production, it will provide a data collection, resource tracking, and reporting system that will afford workforce planning capabilities, and NIBRS Rules compliance for the Law Enforcement and Investigations directorate of the USDA Forest Service. LEIRS is built leveraging the commercial off the shelf functionality of the MicroPact entellitrak data tracking and management platform as configured for law enforcement management purposes, in conjunction with a Federal Risk and Authorization Management (FedRAMP) authorized cloud services Platform as a Service (PaaS) solution model.

The LEIRS application will be used to collect information related to all criminal incidents and civil investigations. Based upon the results from the LEIRS Privacy Threshold Analysis (PTA), the LEIRS database application is required to conduct a Privacy Impact Assessment (PIA).

User access to LEIRS is restricted by means of a Personal Identity Verification (PIV) LincPass card and a user login consisting of a username and password.

Overview

LEIRS is the incident reporting and case management system for the FS. It is a web-enabled commercial off the shelf (COTS) application using the MicroPact **entellitrak** case management system configured within a FedRAMP-certified Cloud Service Provider (CSP) environment with no public-facing access points. LEIRS uses advanced database security to protect data from unauthorized access. Its main purpose is to record criminal and claims activity on lands within the National Forest System (NFS) and to provide the ability to track incidents from discovery through case closure in a single system. LEIRS users access the application using the Forest

Service End User Computing Environment (FS EUCE). All data within the **entellitrak** application is encrypted using encryption methods described in the SSP on Intel multi-core processors. Encryption keys are assigned per volume (vs. an entire disk or disk array). Encryption keys are stored separately from stored data.

Application users are segregated based on role. Users are only permitted to access LEIRS data they are allowed to view and edit, based upon their role definition within the business rules of LEI that have been specified with the LEIRS application.

Personally identifiable information (PII) relevant to Contacts, Defendants and Vehicles is secured and available to authorized Law Enforcement personnel only.

The LEIRS application integrates information pertaining to the management of enforcement and investigations functions, including geographic information system functionality. The LEIRS system has approximately 600-700 FS users dispersed throughout the nine FS Regional Offices. Access to the system is granted by a LEI Steward for each FS region. Access to the system is limited to authorized and approved users who have access to the FS Local Area Network (LAN).

LEIRS will continue using the LEIMARS Mobile module, a legacy stand-alone Java application used by LEI officers on their ruggedized FS laptops to issue incident reports (IRs) and federal violation notices (VNs) from the field while disconnected from the FS network. The IR and VN data are stored on the ruggedized laptop before being uploaded to the centralized database that is protected using encryption. Once each week, officers connect to the FS network and upload the data to the centralized database. After uploading, the data is removed from the ruggedized laptop.

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?

LEIRS is primarily a criminal and civil investigation tool used to collect information concerning criminal incidents that includes the Personally Identifiable Information (PII) related to suspects, witnesses, and victims, in addition to information pertaining to the investigation of criminal activity. The LEIRS system collects the following information (that may be considered PII): first name, last name, middle initial, date of birth, home or mailing address, work address, driver's license, fishing license, hunting license, military issued ID, school issued ID, social security ID, state issued ID, height, weight, race, sex, hair color, eye color, adult/juvenile, and occupation, handwriting or an image of the signature, identifying characteristics and

miscellaneous agency identified identification numbers. LEIRS is also used to document incidents that may be non-criminal in nature, primarily pertaining to civil cases which may result in a claim for or against the government.

1.2 Source

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

Information in LEIRS comes from a variety of reports and other documents connected to the administration of NFS lands. These sources include:

- Incident Reports
- Warning Notices
- Violation Notices
- Motor Vehicle Accident Reports
- Case Investigations
- Other agency reports.

1.3 Justification

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

The Law Enforcement and Investigations Reporting System (LEIRS) system is currently being developed to comply with the mandate to enhance and implement business processes for reporting of law enforcement activities and information to the Department of Justice (DOJ) using the National Incident Based Reporting System (NIBRS) no later than January 1, 2021.

Information is being collected to document all criminal and civil investigations that take place or are related to crimes committed on NFS lands. LEIRS may also contain information related to criminal and civil investigations where an FS Law Enforcement Officer (LEO) was assisting another law enforcement agency or department.

1.4 Collection

How is the information collected?

Information is collected by Law Enforcement personnel through interviews or interrogations of individuals, surveillance, physical and forensic evidence, other law enforcement or interagency information sharing, and requesting information from an institutional third party on a case-by-case basis.

1.5 Validation

How will the information be checked for accuracy?

The LEOs and/or Special Agents (SAs) verify the accuracy of the LEIRS data (hard documents, LEIRS database, etc.) by reviewing it after entering it into the system.

1.6 Authority

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

LEIRS collects Social Security Number (SSN), not Tax Identification Number (TIN). If required, as part of a law enforcement investigation, an individual's SSN may be collected to establish positive identification.

Agencies are authorized under 42 U.S.C., in the administration of any tax, general public assistance, driver's license, or motor vehicle registration law within the agencies' jurisdiction, to use the SSN for the purpose of establishing the identification of individuals affected by such law, and may require any individual to furnish his/her SSN. Individuals from whom an SSN is being collected are notified of the following:

- Whether furnishing the information is mandatory of voluntary
- By what law or other authority the agency is requesting the SSN; and
- What uses will be made of it

Information is being collected to document all criminal and civil investigations that take place or are related to crimes committed on NFS lands. LEIRS may also contain information related to criminal and civil investigations where an FS Law Enforcement Officer (LEO) was assisting another law enforcement agency or department. This system has been exempted pursuant to 5 U.S.C. 552a(k)(2) from the requirements of 5 U.S.C. 552a(c)(3), (d), (e)(1), (3)(4)(G), (H), (I), and (f). See 7 CFR 1.123. This exemption will only be used to maintain the efficiency and integrity of lawful investigations, and to prevent unauthorized access to certain law enforcement files which would alert subjects of investigations that their activities are being scrutinized and thus allow them time to take measures to prevent detection of illegal action or escape prosecution. Any individual who feels, however, that he or she has been denied any right, privilege or benefit for which he or she would otherwise be eligible as a result of the maintenance of such material may request access to the material. Such requests should be addressed to the appropriate system manager.

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 associated with data maintained by LEIRS are managed through the LEIRS defense in depth security model. Information stored within LEIRS is secured in compliance with NIST 800-53, Revision 4 security controls. The LEIRS technical architecture prevents unauthorized access to the personally identifiable data stored within the system. The risk of attacks or unauthorized access attempts on the application and its database are mitigated through protection mechanisms that include firewalls, antivirus software, role-based user access, and FIPS 140-2 compliant encryption. LEIRS is password protected, and data is maintained in physical locations accessible only to authorized personnel. The LEIRS System Security Plan (SSP) specifically addresses the management, operational, and technical security controls used in the system. These controls are periodically reviewed, re-evaluated, and updated in the SSP. Additional management controls include performing a national agency check on all personnel, including contractors, prior to granting them access to the system. Other specific risk mitigation

- NIST 800-53 compliant information security policies are applied consistently across the entire architecture, regardless of the entry point (LEIRS Application, Oracle SQL Plus, etc.).
- PII relevant to Contacts, Defendants and Vehicles is secured and available to authorized LEI personnel only.
- LEIRS users are segregated based on their role, and what data they are authorized to view and edit. Users are also segregated based upon their role definition within the business rules of LEI.
- All computer equipment, including laptops, have a password protected login screen. Access to computer equipment requires a user to enter the correct, secure password prior to obtaining access to the device or any LEIRS data.
- Any time a LEIRS user steps away from their computer, they are required to initiate the screen lock feature. This minimizes the chance unauthorized individuals will gain access to any data within LEIRS.
- All laptop computers using the LEIMARS mobile module and connecting to the LEIRS system must have full disk encryption.
- No sensitive data is permitted to be copied to portable media.

- All backup media containing PII or information covered under the Privacy Act are encrypted using FIPS 140-2 compliant algorithms.

It is important to note that individual access to the data is controlled through the LEIRS application interface. Individual users do not have individual Oracle database accounts, nor do they have access to any LEIRS database accounts. These privacy risks are managed by restricting access to LEIRS. Access to LEIRS is limited only to authorized and approved users who have access to the FS LAN. Access to the LEIRS system is granted by LEI Stewards for each Region respectively. There are no guest/anonymous or temporary accounts for LEIRS. In addition, all PII data including Social Security Number (SSN) is encrypted.

Authorized users are required to fill out the LEIRS Access/Change Request form (FS-5300-0067) and to send it to the Supervisor or Special Agent in Charge (SAC) for approval. The Supervisor or designee approves the request and determines the level of access, and a Data Steward creates the account and manages the user roles. The Data Steward uses the Enterprise Active Directory short name to ensure the validity of user. The user is presented with an additional Statement of Information Security Responsibilities for Users with Privileged Access to Information Systems to which he or she must agree to and sign to prior to being given system access.

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 principal purpose of the data being collected is for retention and use for documentation of investigations, which may be or may have been used in criminal and/or civil judicial proceedings. Individuals are not informed in writing of the principal purpose of the information being collected. Routine uses are defined as disclosures where information is routinely shared whether internally or externally. Below are routine uses applicable to LEIRS:

Sharing information with the Department of Justice (DOJ) (including United States Attorney Offices), local court systems or other Federal agencies. This information is shared in conducting litigation or in proceedings before any court, adjudicative or administrative body, In addition, this information is shared when it is necessary to the litigation and one of the following is a party to the litigation or has an interest in such litigation.

Sharing information with a congressional office from the record of an individual. This information sharing is in response to an inquiry from that congressional office made at the request of the individual to whom the record pertains.

Sharing information with the National Archives and Records Administration (NARA) or other Federal government agencies pursuant to records management inspections being conducted under the authority of 44 U.S.C. §§ 2904 and 2906.

Sharing information with an agency, organization, or individual for the purpose of performing audit or oversight operations as authorized by law, but only such information as is necessary and relevant to such audit or oversight function.

Sharing information with appropriate agencies, entities, and persons when: the FS suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; the FS has determined that as a result of the suspected or confirmed compromise, there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the Department or another agency or entity) or harm to the individual that rely upon the compromised information; and the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Department's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

Sharing information with contractors and their agents, grantees, experts, consultants, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for FS, when necessary to accomplish an agency function related to this system of records. Individuals provided information under this routine use are subject to the same Privacy Act requirements and limitations on disclosure as are applicable to FS officers and employees.

Sharing information with an appropriate Federal, State, tribal, local, international, or foreign law enforcement agency or other appropriate authority charged with investigating or prosecuting a violation or enforcing or implementing a law, rule, regulation, or order, where a record, either on its face or in conjunction with other information, indicates a violation or potential violation of law, which includes criminal, civil, or regulatory violations and such disclosure is proper and consistent with the official duties of the person making the disclosure.

Sharing information with the news media and the public, in consultation with counsel, when there exists a legitimate public interest in the disclosure of the information or when disclosure is necessary to preserve confidence in the

integrity of FS or is necessary to demonstrate the accountability of FS's officers, employees, or individuals covered by the system, except to the extent it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy.

2.2 Analysis and Production

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

LEIRS built-in reports, Oracle, and Microsoft Office are used to analyze data. Information such as statistical crime analysis (excluding PII), is produced and shared within the FS, Congress, and other agencies on a need-to-know basis.

2.3 Commercial/Public Use

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

LEIRS does not use any commercial or publicly available data. LEIRS is primarily a criminal and civil investigation database. The information system is used to collect information related to criminal incidents to include the PII information related to suspects, witnesses, and victims, in addition to information related to the investigation of criminal activity, LEIRS is also used to document incidents that may be non-criminal in nature, but routinely related civil matters that may produce a claim for or against the government.

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.

LEIRS information is secured and protected through PIV LincPass card and a user defined personal identification number for access. Access is granted based on the position the individual holds, such as, but not limited to uniformed LEO, SA, Senior SA, Assistant Special Agent in Charge (ASAC), SAC, Data Stewards, and Database Manager.

In addition, all PII data including SSNs, are encrypted in LEIRS, which is maintained and operated in a FEDRAMP authorized, NIST 800-53 (Rev 4) compliant, cloud-based Platform as a Service (PaaS) architecture by a Cloud Service Provider (CSP). The CSP provides many security controls, including physical and administrative controls such as managing access to physical servers to ensure proper security standards are implemented. Detailed information is captured in the LEIRS SSP.

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?

Information residing within LEIRS is retained indefinitely. The data must be available if a case is reopened. Therefore, LEIRS's data is an exception to the FS's published records disposition schedules, as approved by the NARA.

3.2 Approval

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

As stated in Section 3.1, LEIRS information is retained indefinitely.

3.3 Risk Mitigation

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

The data is retained indefinitely due to ongoing investigations and so that, in the event of a previously closed case being re-opened, the data can be easily accessed by the requesting agent. Retaining such large amounts of data does create a higher amount of risk due to the continually increasing amount of PII stored within the database indefinitely. The FS implements the database security model described in Section 1.7 to help mitigate this risk.

Any hard copies of documents related to case investigations are stored in a room with an extra security lock. This local security serves as an additional measure to ensure only authorized personnel can access these documents. Each regional office location has its own storage area.

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?

Information is not shared with any internal USDA organizations at this time.

4.2 Delivery and Disclosure

How is the information transmitted or disclosed?

N/A

4.3 Risk Mitigation

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

N/A

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?

The information is shared on a need-to-know basis with Law Enforcement partners and the Federal, State, and Local court systems. Information, such as statistical crime analysis—including but not limited to the number of incidents and number of cases, is shared within Congress, the Department of Justice (DOJ), and other agencies on a need-to-know basis.

Sharing information with the Department of Justice (DOJ) (including United States Attorney Offices), local court systems or other Federal agencies. This information is shared in conducting litigation or in proceedings before any court, adjudicative or administrative body, In addition, this information is shared when it is necessary to the litigation and one of the following is a party to the litigation or has an interest in such litigation.

Sharing information with a congressional office from the record of an individual. This information sharing is in response to an inquiry from that congressional office made at the request of the individual to whom the record pertains.

Sharing information with the National Archives and Records Administration (NARA) or other Federal government agencies pursuant to records management inspections being conducted under the authority of 44 U.S.C. §§ 2904 and 2906.

Sharing information with an agency, organization, or individual for the purpose of performing audit or oversight operations as authorized by law, but only such information as is necessary and relevant to such audit or oversight function.

Sharing information with appropriate agencies, entities, and persons when: the FS suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; the FS has determined that as a result of the suspected or confirmed compromise, there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the Department or another agency or entity) or harm to the individual that

rely upon the compromised information; and the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Department's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

Sharing information with contractors and their agents, grantees, experts, consultants, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for FS, when necessary to accomplish an agency function related to this system of records. Individuals provided information under this routine use are subject to the same Privacy Act requirements and limitations on disclosure as are applicable to FS officers and employees.

Sharing information with an appropriate Federal, State, tribal, local, international, or foreign law enforcement agency or other appropriate authority charged with investigating or prosecuting a violation or enforcing or implementing a law, rule, regulation, or order, where a record, either on its face or in conjunction with other information, indicates a violation or potential violation of law, which includes criminal, civil, or regulatory violations and such disclosure is proper and consistent with the official duties of the person making the disclosure.

Sharing information with the news media and the public, in consultation with counsel, when there exists a legitimate public interest in the disclosure of the information or when disclosure is necessary to preserve confidence in the integrity of FS or is necessary to demonstrate the accountability of FS's officers, employees, or individuals covered by the system, except to the extent it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy.

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.

LEIRS is a new system, and currently doesn't have a separate SORN. The system will be operated under Systems of Records Notices (SORN), Law Enforcement Investigation Records, USDA/FS-33 dated September 17, 2004. This SORN has been reviewed by the Department. Information is shared on a need-to-know basis with Law Enforcement partners and the Federal, State, and Local court systems. Information, such as statistical crime analysis, including but not limited to the number of incidents and cases, but excluding PII, is shared within Congress and other agencies on a need-to-know basis.

5.3 Delivery and Security Measures

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

The statistical crime analysis is sent out to other Federal agencies electronically via FS e-mail or by FedEx mail. Statistical crime analysis comprises information such as the number of incidents, number of arrests, number of marijuana plants, and total numbers for closed and open cases for the fiscal year.

LEIRS relies on FS ACE and the FS Chief Information Officer (CIO) to have secure telecommunications and transfer protocols in place.

5.4 Risk Mitigation

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

LEIRS shares statistical crime analysis information, excluding PII information, with other agencies. As a result, LEIRS has privacy risks for consideration. This information is only released on a 'need-to-know' basis under a statutory or other lawful authority to maintain such information. The information is used in accordance with the statutory authority and purpose.

The FS will review the quality (including objectivity, utility, and integrity) of information before it is disseminated to ensure it complies with the standards set forth in the Department's general information quality guidelines.

The methods used to obtain, send, disclose and store information complies with applicable laws, such as those governing privacy, confidentiality, recordkeeping, and accessibility to persons with disabilities.

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.)

The system requires a SORN:

https://www.fs.usda.gov/about-agency/foia/privacyact

6.2 Individual Notification

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

Individuals are notified of the principal purpose of the information being collected. LEIRS contains information about individuals that are recorded on a United States District Violation Notice. Individuals who receive a Violation Notice are provided with a copy at the time of the incident. The notification provides a copy of all recorded information to individuals. The Court Violation Notice provided to the individual includes a written Privacy Act Disclosure Statement.

Notice-related information will also be available within the System of Records Notice (SORN), which is mandated by the Privacy Act of 1974. The SORN will be published in the Federal Register complying with the requirement that any agency collecting information have a published SORN in place no less than 40 days prior to collection of that information.

6.3 Right to Decline

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

Individuals can exercise their right to remain silent, or decline to provide information.

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?

Not Applicable - In regard to the data collected, individuals do not have the right to consent to a particular use of the information. This is because individuals are not informed of the data collection process for LEIRS.

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.

Individuals are notified of the principal purpose of the information being collected. LEIRS contains information about individuals that are recorded on a United States District Violation Notice. Individuals who receive a Violation Notice are provided with a copy at the time of the incident. The notification provides a copy of all recorded information to individuals. The Court Violation Notice provided to the individual includes a written Privacy Act Disclosure Statement.

Information is being collected to document all criminal and civil investigations that take place or are related to crimes committed on NFS lands. LEIRS may also contain information related to criminal and civil investigations where an FS Law Enforcement Officer (LEO) was assisting another law enforcement agency or department. This system has been exempted pursuant to 5 U.S.C. 552a(k)(2) from the requirements of 5 U.S.C. 552a(c)(3), (d), (e)(1), (3)(4)(G), (H), (I), and (f). See 7 CFR 1.123. This exemption will only be used to maintain the efficiency and integrity of lawful investigations, and to prevent unauthorized access to certain law enforcement files which would alert subjects of investigations that their activities are being scrutinized and thus allow them time to take measures to prevent detection of illegal action or escape prosecution. Any individual who feels, however, that he or she has been denied any right, privilege or benefit for which he or she would otherwise be eligible as a result of the maintenance of such material may request access to the material. Such requests should be addressed to the appropriate system manager.

The LEIRS system implements the Forest Service End User Computing Environment (FS EUCE) notification warning banner providing notice to end users they are accessing a government system on a government network. In addition to providing a definitive warning to potential intruders, the banner advises authorized and legitimate users of LEIRS of their obligations and acceptable use requirements of the system and its resources, data, and network access capabilities prior to login. Users are given a choice to accept or decline to continue. By accepting, users acknowledge they understand their obligations and responsibilities when they login to LEIRS. If a user declines, he or she is not allowed to log into the system.

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?

Individuals are not allowed to access their information through the LEIRS application. Although access to the system may be denied, any person, including U.S. citizens, foreign nationals, organizations, universities, businesses, and state and local governments, can file a Freedom of Information Act (FOIA) request to acquire copies of records housed within the system. Federal employees may not use government time or equipment when requesting information under the FOIA.

Individuals are able to write to the FS FOIA Office. Personnel in that division will then forward the request to the section of the agency they believe is most likely to maintain the records the individual is seeking. The individual must specify that he or she wishes the records of the system to be checked. At a minimum, the individual should include: name; date and place of birth; current mailing address and zip code; signature; a brief description of the circumstances that caused the creation of the record (including the city and/or country and the approximate dates) which gives the individual cause to believe that this system has records pertaining to him or her.

Individuals can submit FOIA requests to: USDA FS, FOIA Service Center 1400 Independence Avenue, SW, Mail Stop: 1143, Washington, DC 20250-1143.

Correspondence may also be sent via fax or e-mail: Fax: (202) 260-3245 and E-mail correspondence to: wo_foia@usda.gov

The guidance for the content of requests for correction of information is not intended to constitute a set of legally binding requirements. Requestors bear the 'burden of proof' with respect to the necessity for correction as well as with respect to the type of correction they seek. However, the FS may be unable to process, in a timely fashion or at all, requests that omit one or more of the requested elements.

Examples of data that cannot be disclosed include:

- Any information describing LEIRS architecture or database structure.
- Descriptions of LEI surveillance techniques or equipment that could be used to compromise an investigation.

- Records of individuals other than those of the requestor.

7.2 Correction

What are the procedures for correcting inaccurate or erroneous information?

If a recipient of a Violation Notice (VN) wants to update or change the information recorded on the notice, he or she must contact the Central Violations Bureau (CVB) directly. Details on how to contact the CVB are provided on the back of the notice. The recipient can send all written correspondence to the Correspondence Address listed on the VN. A Payment Address and other applicable phone numbers have also been provided. The CVB will provide a blank Violation Form so the most up-to-date information can be documented.

In the event records need to be changed, LEOs, Special Agents, and LEIRS Data Stewards will update inaccurate or erroneous information within the LEIRS system.

7.3 Notification

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

The VN contains instructions for changing address. Users can contact the CVB using the address and/or phone number listed on the VN. Individuals may submit requests for corrections via the methods described in Section 7.1

7.4 Redress Alternatives

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

Redress is provided in that individuals are able to contact the CVB to have their information updated. Alternatives outside of this formal redress process do not exist.

7.5 Risk Mitigation

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

Because the LEIRS system is not accessible to the public, all redress actions are performed exclusively by authorized LEI personnel. Individuals in these roles are the only personnel allowed to correct inaccurate or erroneous information within LEIRS itself. However, any individuals who would like to inquire about the status of their violations such as date of violation, date to

appear in court, dollar amount of a fine, etc. are able to access this information via the Central Violations Bureau (CVB).

Privacy risks associated with redress entail individuals providing false information about themselves during the time the information is documented at the incident and during redress procedures. In these situations, LEIRS personnel are responsible for thoroughly reviewing and investigating information that has been provided by individuals to ensure accuracy.

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?

Authorized users are required to fill out the LEIRS Access/Change Request form and to send it to the Supervisor or Special Agent in Charge (SAC) for approval. The Supervisor or designee approves the request and determines the level of access, and a Data Steward creates the account and manages the user roles. The Data Steward uses the Enterprise Active Directory short name to ensure the validity of user. The user is presented with an additional Statement of Information Security Responsibilities for Users with Privileged Access to Information Systems to which he or she must agree and sign to prior to being given system access. There are no guest/anonymous and temporary accounts in LEIRS.

When LEIRS users are terminated, the terminated individual or the LEIRS Data Steward must complete the LEIRS Access/Change Request form with the check box “Delete User- Employee no longer has need for Oracle ID or LEIRS Access” selected, and send it to their Supervisor or SAC for approval.

Individual users do not have individual Oracle database accounts, nor do they have access to any LEIRS database accounts. Activity is logged and audited on an individual basis. This process is used to ensure only authorized users access the LEIRS system. These procedures are documented in Section 13.3 of the LEIRS SSP, available within CSAM.

8.2 Contractor Access

Will Department contractors have access to the system?

The vendor that developed the COTS product used for LEIRS will have access to the system.

8.3 Privacy Training

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

All LEIRS users are trained on initial system login procedure, required data entry procedures, and procedures required to run LEIRS system reports. In

addition, all LEIRS users are required to annually complete the Ag Learn Information Security Awareness Training, which includes privacy 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).

No. This is a new system. An ATO is being pursued, with the goal of not later than December 31, 2020.

8.5 Audit and Technical Safeguards

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

The LEIRS System Owner (SO) or LEIRS Information Systems Security Officer (ISSO) use Splunk, the defined audit tool to verify and ensure LEIRS data integrity.

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?

LEIRS uses separation of duties, need-to-know, and multi-layered levels of security to mitigate privacy risk for sharing information with other agencies. Data is shared on a need-to-know basis. By keeping the information disseminated across multiple systems in the FS (through secure internal processing and connections), no one system can be illegally accessed to steal user data. Role separation prevents any single user from having full access for fraudulent use of the data and information.

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?

LEIRS is a web-enabled database application.

9.2 Privacy Concerns

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

NIST 800-53 (Rev 4) compliant security controls have been implemented to mitigate or eliminate privacy concerns. LEIRS is maintained and operated in a FEDRAMP authorized, NIST 800-53 (Rev 4) compliant, cloud-based Platform as a Service (PaaS) architecture by a Cloud Service Provider (CSP). The CSP provides many security controls, including physical and administrative controls such as managing access to physical servers to ensure proper security standards are implemented. Additional NIST 800-53 (Rev 4) compliant security controls have been implemented in the LEIRS application. These are in addition to the existing FS security controls already implemented. Detailed information is presented in the LEIRS SSP.

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, the ISSO has reviewed OMB M-10-22 and OMB M-10-23

10.2 Purpose

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

Third party websites are not used.

10.3 PII Availability

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

Third party websites are not used.

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?

Third party websites are not used.

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?

Third party websites are not used.

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?

Third party websites are not used.

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?

Third party websites are not used.

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?

Third party websites are not used.

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)?

Third party websites are not used.

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?

LEIRS does not use web measurement and customization technology.

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?

LEIRS does not use web management and customization technology.

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.

Third party websites are not used.

Responsible Official

CURTIS DAVIS Digitally signed by CURTIS DAVIS Date: 2020.10.13 12:36:00 -04'00'

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

Approval Signature

CYNTHIA TOWERS Digitally signed by CYNTHIA TOWERS Date: 2020.10.19 10:32:34 -05'00'

Cynthia Towers
Forest Service CIO Privacy Officer
USDA Forest Service Chief Information Office

LAURA HILL Digitally signed by LAURA HILL Date: 2020.10.20 10:51:44 -06'00'

Laura Hill
Forest Service Agency Chief Information Security Officer (ACISO)
USDA Forest Service Chief Information Office