Privacy Impact Assessment

for

Law Enforcement Investigation Management Attainment Reporting System (LEIMARS)

Policy, E-Government and Fair Information Practices

Version: 1.1

Date: January 24, 2020

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

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 Law Enforcement Investigations Management Attainment Reporting System (LEIMARS) is a web-enabled application comprised of multiple servers connected in a fault tolerant configuration using LINUX operating systems, Java, and Database servers. Access to the system is through Agency networks via the FS Intranet, https://apps.fs.usda.gov/leimars

It is a national Law Enforcement reporting database and is currently maintained at the National Information Technology Center (NITC) in Kansas City, MO. While NITC serves as the primary processing site, the alternate processing site for NITC FS Application Cloud Environment (ACE) is located in St. Louis, MO. The ACE Data Center serves as the alternate location for the FS ACE and all supporting applications, including LEIMARS. LEIMARS components at NITC and alternate processing site are managed by FS personnel (e.g. System Administrators and Database Administrators). FS ACE provides services including but not limited to: web, application, database storage, backup and recovery, and monitoring. Alternate site is serving as the backup site for FS ACE at NITC, residing applications are assessed separately. In addition, access is restricted to digital and non-digital media at NITC and alternate site using security measures that meet FS security guidelines. Only users who have been granted specific access to NITC and alternate site are allowed to physically access the digital and non-digital media such as magnetic tape backups. Access is restricted by means of a Personal Identity Verification (PIV) LincPass card and a user defined personal identification number (pin).

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

Overview

LEIMARS is the incident reporting and case management system for the FS. It is an intranet based application fully contained within the USFS network and firewalls with no public-facing access points. LEIMARS utilizes an advanced database security implementation to protect the 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.

LEIMARS is implemented as a Virtual Private Database (VPD) utilizing row-level security (RLS) providing a consistent, secure method for managing data access ensuring:

Consistency in applying policies regardless of the point of entry (LEIMARS Application, SQL Plus, ODBC, etc.)

Application users are segregated based on what parts of LEIMARS data they are allowed to view and edit, based upon their role definition within the business rules of LEI, that have been subsequently been programmed into the application.

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

Security policies are implemented on a row-by-row basis within a given table. All DML (select, insert, update, delete) are governed by those polices, including select statements that access views.

Consistent application and management of the security model. Developers need not code/recode security rules that govern DML within the application as they are applied by RLS in the database.

The application integrates information pertaining to the management of enforcement and investigations functions, including geographic information system functionality. The LEIMARS system has approximately 600-700 FS users dispersed throughout the nine FS Regional Offices. Access to the system is granted by an 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).

The LEIMARS Mobile module is a stand-alone desktop application which supports LEI officers in the issuance of incident reports and violation notices from the field while not being connected to any network.

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?

LEIMARS is primarily a criminal and civil investigation database and is 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 LEIMARS 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. LEIMARS is also used to document incidents that may be non-criminal in the 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 LEIMARS 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?

Information is being collected to document all criminal and civil investigations that take place or are related to crimes committed on NFS lands. LEIMARS 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 being collected by Law Enforcement personnel through contact with the public and first-hand findings from investigations.

1.5 Validation

How will the information be checked for accuracy?

The LEOs and/or Special Agents (SAs) verify the accuracy of the LEIMARS data (hard ic documents, LEIMARS 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?

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 access to certain law enforcement files that potentially could 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 Data Steward.

LEIMARS was granted Authority to Operate (ATO) on January 31, 2018.

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 LEIMARS are managed through the LEIMARS database security model. LEIMARS utilizes an advanced database security implementation called Row-Level Security (RLS) to protect the data from unauthorized access. RLS is a method of fine-grained access control which provides a consistent, secure method for managing data access, ensuring:

Consistency in applying policies regardless of the point of entry (LEIMARS Application, SQL Plus, ODBC, etc.)

Application users are segregated based on what parts of LEIMARS data they are allowed to view and edit. Application users are also segregated based upon their role definition within the business rules of LEI. These business rules have been subsequently programmed into the application.

PII relevant to Contacts, Defendants and Vehicles is secured and available to authorized LEI personnel only.

Security policies are implemented on a row-by-row basis within a given table. All Data Manipulation Language (DML) (select, insert, update, delete, call, merge, etc.) are governed by those polices, including select statements that access views.

Consistent application and management of the security model. Developers need not code/recode security rules that govern DML within the application as they are applied by RLS in the database.

Permissions on schema objects are granted to LEIMARS database roles. These database roles are in turn granted to the LEIMARS proxy account as non-default roles, requiring a LincPass PIV card to activate the role for the current session. The lowest-level role is active as a default. This role can only select non-sensitive data, which excludes all PII such as personal contact or vehicle information.

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

Authorized users are required to fill out the LEIMARS Access/Change Request form (FS-5300-0067) and to send it to 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.

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 LEIMARS:

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?

The LEIMARS customized 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

LEIMARS does not use any commercial or publicly available data. LEIMARS 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. LEIMARS 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.

The 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, Database Manager. In addition, all PII data including SSNs are encrypted in LEIMARS, which is maintained in an FS-managed section of the NITC, where the Application Hosting Environment (FS ACE) General Support System (GSS) is housed.

External network connections for the infrastructure housing LEIMARS are protected by individual firewalls and are managed and maintained by the USDA Universal Telecommunications Network (UTN). Internal connections are transmitted via the FS Wide Area Network (WAN) and through the firewall architecture.

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 LEIMARS is retained indefinitely. The data must be available if a case is reopened. Therefore, LEIMARS'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, a retention period has not been defined for LEIMARS

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 that only authorized personnel can access these documents.

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 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 and other agencies on a need-to-know basis.

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.

LEIMARS system is operated under Systems of Records Notices (SORN), Law Enforcement Investigation Records, USDA/FS-33 dated September 17, 2004. Information such as statistical crime analysis—including the number of incidents and cases, but excluding PII—is shared outside the FS.

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 the number of incidents, number of arrests, number of marijuana plants, and total numbers for closed and open cases for the fiscal year.

LEIMARS 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.

LEIMARS shares statistical crime analysis information, excluding PII information, with other agencies. As a result, LEIMARS 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 that 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 FS-33

6.2 Individual Notification

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

In regard to the data collected, individuals are not informed in writing of the principal purpose of the information being collected.

In regard to users entering the information into LEIMARS, the only notification that occurs is during the initial sign-on notification that all users see when they log onto the system. The notification states that the user is using a government machine and is subject to review. Aside from the initial sign-on notification, no users are affected by the collection of this information.

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 Registry to support 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?

In regard to the data collected, individuals do not have the right to decline providing information due to the fact that they are not informed of the data collection process for LEIMARS.

LEIMARS users are not members of the public nor can anyone within the FS have access to the system without it being granted by LEI. LEIMARS does not

have a warning banner before logging into the system except the hardware encryption and the Windows login banner.

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 due to the fact that they are not informed of the data collection process for LEIMARS.

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.

In regard to the data collected, individuals are not informed in writing of the principal purpose of the information being collected. The principal purpose of the data being collected is for retention and use for documentation of investigations, which may or may not have been used in criminal and/or civil judicial proceedings.

In regard to users entering the information into LEIMARS, the Forest Service End User Computing Environment (FS EUCE) notification warning banner provides notice. Users are aware that they are accessing a government system on a government network. They are given a choice to accept or decline; by accepting they are acknowledging that they are OK with entering the system and having the system use their information. If a user declines, he or she is not allowed 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?

LEIMARS contains information about individuals that is recorded on a 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.

Individuals are not allowed to access their information through the LEIMARS database. 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 of 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 that they believe is most likely to maintain the records of which 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 are able to write 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 LEIMARS 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. This information is provided on the back of the notice. The recipient can send all written correspondence to the Correspondence Address listed. 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 case that records need to be changed, LEOs, Special Agents, and LEIMARS Data Stewards will update that inaccurate or erroneous information within LEIMARS.

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.

As the LEIMARS 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 LEIMARS 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 such case, LEIMARS 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 LEIMARS Access/Change Request form and to send it to 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 LEIMARS.

Any modifications to the accounts are authorized by Supervisor or SAC and performed by the LEIMARS Data Steward. When LEIMARS users are terminated, that individual or LEIMARS Data Steward is required to fill out the LEIMARS Access/Change Request form with check box “Delete User-Employee no longer has need for Oracle ID or LEIMARS Access” and to send it to Supervisor or SAC for approval. The Supervisor or designee approves the request and a Data Steward then remove that user out the LEIMARS roles table. The individual’s account is deleted from the system, but the history is maintained. When LEIMARS users are transferred, that individual also fills out the LEIMARS Access/Change Request form for approval to terminate access. LEIMARS does not monitor for periods of extended inactivity and does not perform annual account recertification.

Access to the data is controlled through the LEIMARS application interface. Individual users do not have individual Oracle database accounts, nor do they have access to the LEIMARS database accounts. Activity is logged and audited on an individual basis. These procedures are documented in the LEIMARS SSP Section 1.6 and 1.7 available within CSAM.

8.2 Contractor Access

Will Department contractors have access to the system?

The LEIMARS Development Team, who have developed and supported the system, have access to LEIMARS

8.3 Privacy Training

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

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

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 is January 31, 2021.

8.5 Audit and Technical Safeguards

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

LEIMARS System Owner (SO) or LEIMARS Information Systems Security Officer (ISSO) utilize Splunk, the defined audit tool to check and ensure the integrity of LEIMARS data.

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?

LEIMARS uses separation of duties and multi-layered levels of security to mitigate privacy risk for sharing information to other agencies. The 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. Separated roles prevent any one 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?

LEIMARS 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.

The security controls in place both physically and internal to LEIMARS, which resides on FS ACE, mitigate or eliminate privacy concerns. FS ACE works in tandem with other GSSs to support the security of the FS's core data.

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 and/or applications are not used for LEIMARS.

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 and/or applications are not used for LEIMARS.

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 and/or applications are not used for LEIMARS.

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 and/or applications are not used for LEIMARS.

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 and/or applications are not used for LEIMARS cable.

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 and/or applications are not used for LEIMARS.

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 and/or applications are not used for LEIMARS.

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 and/or applications are not used for LEIMARS.

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?

LEIMARS does not use web management 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?

LEIMARS 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 and/or applications are not used for LEIMARS.

Responsible Official

CURTIS DAVIS Digitally signed by CURTIS DAVIS Date: 2020.04.28 14:17:05 -04'00'

Curtis Davis
System Owner (SO)
Natural Resources and Environment, Forest Service
United States Department of Agriculture

Approval Signature

CYNTHIA TOWERS Digitally signed by CYNTHIA TOWERS Date: 2020.04.30 14:15:12 -05'00'

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

LAURA HILL Digitally signed by LAURA HILL Date: 2020.05.04 08:41:39 -06'00'

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