U.S. DEPARTMENT OF AGRICULTURE

PRIVACY IMPACT ASSESSMENT

Law Enforcement Investigations & Reporting System (LEIRS)

VERSION 3.0

OFFICE OF THE CHIEF PRIVACY OFFICER

Privacy Impact Assessment

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

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

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

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

Guidance on how to complete the following PIA Questionnaire is available here.

Privacy Impact Assessment for the USDA IT System/Project:

Law Enforcement Investigations & Reporting System (LEIRS)

USDA – Forest Service

Law Enforcement & Investigations (LEI)

Date PIA submitted for review:

<<ADD DATE HERE>>

Mission Area System/Program Contacts:

	Name	E-mail	Phone Number
Mission Area Privacy Officer	*Cynthia Ebersohn*	***cynthia.ebersohn@usda.gov***	*386-301-4060*
Information System Security Manager	*Benjamin Moreau*	***benjamin.moreau@usda.gov***	***202-380-6165***
System/Program Managers	*Curtis Davis*	*curtis.davis@usda.gov*	*912-554-4268*

Abstract

The Law Enforcement and Investigations Reporting System (LEIRS) is the incident reporting and case management system for the Forest Service. LEIRS provides data collection, resource tracking, and reporting that support Law Enforcement & Investigations (LEI) workforce planning capabilities and ensure compliance with Department of Justice reporting systems to include National Incident-Based Reporting System (NIBRS) rules for the Law Enforcement and Investigations directorate of the USDA Forest Service.

Overview

LEIRS is a web-enabled commercial off the shelf (COTS) application using the Tyler Federal MicroPact entellitrak case management system configured within a FedRAMP-certified Cloud Service Provider (CSP) environment with no public-facing access points. The FedRAMP ID is FR2108649352. LEIRS uses advanced database security to protect data from unauthorized access. The LEIRS application is used to collect information related to all criminal incidents and civil investigations 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. 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.

LEIRS is considered 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 is further identified by USDA and Department of Homeland Security (DHS) as a High Value Asset. LEIRS is listed by DHS as a High Value Asset and carries an HVA ID of 211006000858.

Section 1.0 Authorities and Other Requirements

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

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

If required, as part of a law enforcement investigation, LEIRS may collect an individual's SSN to establish positive identification. LEIRS collects Social Security Number (SSN), not Tax Identification Number (TIN). 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 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 FS Law & Investigation is supporting/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 law enforcement files which could alert subjects of investigations that their activities are being scrutinized thus allowing 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.

Title 16, Untied States Code, section 559

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

Yes. Expires on May 23, 2025.

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

LEIRS operates under Systems of Records Notices (SORN), Law Enforcement Investigation Records, USDA/FS-33 dated September 17, 2004.

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

NO

Section 2.0 Characterization of the Information

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

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

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

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

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

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

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

Information in LEIRS comes from a variety of reports and other documents connected to the administration of National Forest Service (NFS) resources. These include:

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

2.2.1. 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.

2.3. Does the project/program or system use information from commercial sources or publicly available data. If so, explain why this 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 and criminal investigations including PII information related to suspects, witnesses, and victims. LEIRS is also used to document incidents that may be non-criminal in nature, but related civil matters that may affect or produce claims for or against the government.

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

The Law Enforcement Officers (LEOs) and/or Special Agents (SAs) verify the accuracy of the LEIRS data (hard documents, LEIRS database, etc.) at the time of entry into the system.

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

No

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

Third party websites are not used.

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

Third party websites are not used.

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

Privacy Risk: Privacy Act (PA) risks associated with the characterization of information may include:

Misclassification of Data: Incorrectly categorizing PII which can lead to inadequate protection measures, exposing sensitive data to unauthorized access or misuse.

Inadequate Security Controls: If PII is not properly identified and characterized, it may not receive the necessary security measures, increasing the risk of data breaches.

Over-collection of Data: Misunderstanding classification of information may result in collecting more data than necessary, violating principles of data minimization and increasing exposure to risk.

Mitigation: **By implementing some or all the following mitigation actions, mission areas can effectively characterize personal identifiable information (PII), manage privacy risks, and comply with the PA requirements**:

Data Classification Policy: Adhere to departments data classification policy that categorizes PII based on sensitivity and the potential impact of unauthorized access or disclosure.

Regular Data Inventory: Conduct regular inventories of personal information to identify and categorize the types of data collected, stored, and processed by the organization.

Contextual Information Use: Ensure that the context in which personal information is collected and used is considered when characterizing data, recognizing how this affects privacy risks.

Section 3.0 Uses of the Information

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

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

Data is primarily collected and used for documentation of investigations in support of criminal and/or civil judicial proceedings. Individuals subject to investigations are not informed in writing of the principal purpose of the information being collected.

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

LEIRS uses built-in reports and Microsoft Office to conduct statistical crime analysis. The results of such analysis (excluding PII) is shared within the FS, Congress, and other agencies on a need-to-know basis.

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

Privacy Risk: Privacy act risks associated with the uses of information include:

Unauthorized Use of Data: PII may be used for purposes other than those for which it was collected, violating privacy principles and user expectations.

Data Misuse: Employees or third parties may misuse PII, either intentionally or unintentionally, leading to breaches of confidentiality and trust.

Inadequate Consent: If individuals are not adequately informed about how their data will be used, or if consent is not appropriately obtained, it can result in legal non-compliance and ethical concerns.

Mitigation: **By implementing some or all the following mitigation actions, mission areas may better safeguard PII and ensure responsible use in compliance with PA requirement:**

Purpose Limitation: Clearly define and communicate the specific purposes for which PII is collected and used, ensuring that it is not used for unrelated purposes without consent.

Data Minimization: Collect and use only the minimum amount of PII necessary to achieve the intended purpose, reducing the risk of misuse.

User Consent: Obtain explicit consent from individuals before using their personal information, particularly for purposes that go beyond the original intent of collection.

Section 4.0 Notice

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

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

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 Court Violation Notice provided to the individual includes a written Privacy Act Disclosure Statement.

Notice-related information is also 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.

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

Individuals can exercise their right to remain silent or decline to provide information. Once collected, individuals do not have the right to consent to a particular use of the information.

4.3. PRIVACY IMPACT ANALYSIS: Related to Notice

Privacy Risk: **Privacy Act risks associated with notices include:**

Inadequate Disclosure: Notices may fail to adequately inform individuals about how their personal information will be collected, used, and shared, leading to misunderstandings about privacy practices.

Ambiguity: If notices are unclear or overly complex, individuals may not fully understand their rights or the mission area's data practices, leading to a lack of informed consent.

Non-compliance with Regulations: Failing to provide required notices as stipulated by the Privacy Act can result in legal penalties and regulatory scrutiny.

Mitigation: Implementing some or all the following mitigation actions, mission areas can better protect individual privacy rights and comply with privacy act requirements:

Clear Communication: Ensure that privacy notices are written in clear, accessible language. Avoid legal jargon to make it understandable for all users.

Regular Updates: Review and update privacy notices regularly to reflect changes in data practices, regulations, or business operations.

User Consent: Implement mechanisms for obtaining explicit user consent for data collection and processing and provide options for users to withdraw consent easily.

Section 5.0 Data Retention

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

5.1. What information is retained and for how long?

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

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

DAA-GRS- 2017-0006- 0030 Destroy when 25 years old, but longer retention is authorized if required for business use.

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

Privacy Risk: **Privacy act risks associated with the retention of information include:**

Excessive Data Retention: Retaining PII longer than necessary can violate data minimization principles, increasing the risk of unauthorized access and exposure.

Data Breaches: The longer PII is retained, the greater the risk of data breaches occurring, whether through hacking, accidental disclosures, or insider threats.

Non-compliance with Regulations: Failing to adhere to legal requirements regarding data retention periods can lead to regulatory penalties and legal liabilities.

Mitigation: **Implementing the following mitigation actions, mission areas can ensure responsible retention of PII while complying with the PA.**

Data Retention Policy: Use NARA data retention policies that outline how long different types of PII will be retained and the rationale for those timeframes.

Regular Reviews: Conduct regular reviews of stored data to ensure compliance with retention policies and to identify information that is no longer necessary for business purposes.

Secure Disposal Procedures: Establish secure methods for the disposal of personal information that is no longer needed, such as shredding paper documents or using data-wiping software for electronic files.

Section 6.0 Information Sharing

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

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

Information is not shared with any internal USDA organizations.

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

Privacy Risk: N/A

Mitigation: N/A

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

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.

Information is shared with Department of Justice (DOJ) (including United States Attorney Offices), local court systems or other Federal agencies in conducting litigation or in proceedings before any court, adjudicative or administrative body; 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.

Information from the record of an individual is shared in response to an inquiry from that congressional office made at the request of the individual to whom the record pertains.

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

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

Information may be shared 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. Disclosure made to such agencies, entities, and persons as are reasonably necessary to assist in connection with the Department's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy harm that may result from relying on such information.

Information is shared 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.

Information is shared with appropriate Federal, State, tribal, local, international, or foreign law enforcement agencies or any other appropriate authorities 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 those requesting/making the disclosure.

Information is shared 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.

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

Privacy Risk: LEIRS shares statistical crime analysis information, excluding PII information, with other agencies. As a result, LEIRS has privacy risks for consideration. They include:

Unauthorized Access: Sharing PII with third parties increases the risk of unauthorized access, especially if those parties do not have adequate security measures in place.

Data Breaches: External sharing can lead to data breaches, either through hacking or inadvertent exposure, resulting in unauthorized individuals gaining access to sensitive information.

Loss of Control: Once PII is shared externally, mission areas may lose control over how that information is used, which can lead to misuse or unauthorized applications of the data.

Mitigation: Implementing the following mitigation actions, mission areas can manage the risk associated with external sharing and disclosure of personal information while complying with PA requirements.

Due Diligence: Conduct thorough due diligence on third parties before sharing personal data, ensuring their privacy standards and practices are comparable to the PA and USDA requirements.

Written Agreements: Establish written agreements or contracts with third parties that outline their responsibilities for safeguarding shared data and compliance with privacy laws.

Section 7.0 Redress

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

7.1. What are the procedures that allow individuals to gain access to their information?
Individuals are not allowed to directly access their information through the LEIRS application. However, 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 can direct requests 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. Privacy Impact Assessment Page 20 Law Enforcement Investigations Reporting System (LEIRS)
- Records of individuals other than those of the requestor.

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

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

7.5. PRIVACY IMPACT ANALYSIS: Related to Redress.

Privacy Risk: Privacy Act risks associated with redress include:

Inadequate Processes: If the processes for individuals to seek redress for privacy violations are unclear or cumbersome, it can deter individuals from exercising their rights and lead to unresolved complaints.

Lack of Transparency: Not providing clear information about how redress mechanisms work can create confusion and mistrust among individuals regarding their rights and the agency's accountability.

Failure to Address Complaints: Mission areas or agencies may not adequately address or resolve complaints related to privacy violations, leading to dissatisfaction and potential legal repercussions.

Mitigation: Implementing the following mitigation actions, mission areas can enhance redress mechanisms, ensuring individuals have effective means to address privacy concerns.

Establish Clear Procedures: Develop and communicate clear procedures for individuals to submit complaints or requests for redress related to privacy violations.

User Awareness Campaigns: Educate users about their rights under the privacy act and the available redress mechanisms through workshops, newsletters, or online resources.

Dedicated Privacy Officer/Privacy Point of Contact: Appoint a dedicated privacy officer or other personnel responsible for handling redress requests and ensuring timely responses to complaints.

Section 8 Auditing and Accountability

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

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

LEIRS information is secured and protected through PIV LincPass card and a user defined personal identification number for access enforced by USDA eAuth. 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 5) 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. More detailed information is captured in the LEIRS SSP.

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

Individual access is controlled through the LEIRS application interface. Individual users do not have access to any LEIRS database accounts. 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 one of the designated LEI Account Managers. There are no guest/anonymous or temporary accounts for LEIRS.

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 an Account Manager creates the account and manages the user roles. The Account Manager 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.

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

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.

This information is only shared when a legal responsibility exists to make the information available. Examples include federally-mandated information disclosure to support U.S. Department of Justice data gathering efforts, and court-mandated discovery.

The FS reviews 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.

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

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.

Approval Signatures:

_____

Curtis Davis
Assistant Director-LEI
System Owner
Forest Service
Law Enforcement & Investigations, WO-FLETC
United States Department of Agriculture

_____

Cynthia (Towers) Ebersohn,
NRE FS Privacy Officer
Forest Service
United States Department of Agriculture Natural Resources and Environment Forest Service Chief Information Office
United States Department of Agriculture

_____

Benjamin Moreau
Assistant Chief Information Security Officer (ACISO) Assistant Director, Cybersecurity
Forest Service
United States Department of Agriculture
Natural Resources and Environment Forest Service Chief Information Office
United States Department of Agriculture

TRACY HENDRIX Digitally signed by TRACY HENDRIX
Date: 2025.06.25 22:24:22 -04'00'

_____

Officer of the Chief Privacy Officer
United States Department of Agriculture