Introduction

The Department of the Interior requires PIAs to be conducted and maintained on all IT systems whether already in existence, in development or undergoing modification in order to adequately evaluate privacy risks, ensure the protection of privacy information, and consider privacy implications throughout the information system development life cycle. This PIA form may not be modified and must be completed electronically; hand-written submissions will not be accepted. See the DOI PIA Guide for additional guidance on conducting a PIA or meeting the requirements of the E-Government Act of 2002. See Section 6.0 of the DOI PIA Guide for specific guidance on answering the questions in this form.

NOTE: See Section 7.0 of the DOI PIA Guide for guidance on using the DOI Adapted PIA template to assess third-party websites or applications.

Name of Project: Law Enforcement Training System (LETS)
Bureau/Office: U.S. Fish and Wildlife Service (FWS)
Date: April 26, 2021
Point of Contact:
Name: Jennifer Schmidt
Title: FWS Associate Privacy Officer
Email: fws_privacy@fws.gov
Phone: (703) 358-2291
Address: 5275 Leesburg Pike, MS: IRTM, Falls Church, VA 22041

Section 1. General System Information

A. Is a full PIA required?

☒ Yes, information is collected from or maintained on
- ☒ Members of the general public
- ☒ Federal personnel and/or Federal contractors
- ☐ Volunteers
- ☐ All

☐ No: *Information is NOT collected, maintained, or used that is identifiable to the individual in this system. Only sections 1 and 5 of this form are required to be completed.*

B. What is the purpose of the system?

The Law Enforcement Training System (LETS) is a Software-as-a-Service (SaaS) Cloud implementation product used by the Fish and Wildlife Service (FWS) Office of Law Enforcement (OLE) Training & Inspection Division to help manage its training operations for FWS Law Enforcement Officers (LEO), other Federal LEOs and local, State, Tribal, and international LEOs responsible for the enforcement of wildlife laws in the U.S. and abroad.

OLE coordinates and conducts training for FWS special agents, wildlife inspectors, and administrative staff, as well as for State, Native American, and foreign individuals responsible for wildlife and habitat protection. OLE offers this training virtually, at FWS' National Conservation Training Center (NCTC) in West Virginia, and at the interagency Federal Law Enforcement Training Center in Georgia. Over the past decade, there have been substantial increases in the numbers of programs and individuals trained, hours of training provided, and numbers of training sites.

LETS provides OLE a comprehensive, reliable, and secure internet-based system capable of planning, coordinating, and tracking the increased training-associated information and workflow, as well as the associated equipment, materials, and supplies required to successfully accomplish and sustain FWS vital training environments. LETS serves as a repository for records derived from field-based trainings, certifications and the like, with records access restricted to system administrators to use for reporting and tracking purposes.

C. What is the legal authority?

5 U.S.C. 4101, et seq., Government Organization and Employees Training. FWS law enforcement authorities derive from the Lacey Act (18 U.S.C. 42-44) and the Endangered Species Act (18 U.S.C. 1531-1543).

D. Why is this PIA being completed or modified?

☒ New Information System
☐ New Electronic Collection
☐ Existing Information System under Periodic Review
☐ Merging of Systems
☐ Significantly Modified Information System
☐ Conversion from Paper to Electronic Records
☐ Retiring or Decommissioning a System
☐ Other: *Describe*

E. Is this information system registered in CSAM?

☐ Yes: *Enter the UII Code and the System Security Plan (SSP) Name*
☒ No – LETS is in the process of CSAM registration.

F. List all minor applications or subsystems that are hosted on this system and covered under this privacy impact assessment.

Subsystem Name	**Purpose**	**Contains PII** *(Yes/No)*	**Describe** *If Yes, provide a description.*
None.			

G. Does this information system or electronic collection require a published Privacy Act System of Records Notice (SORN)?

☒ Yes: *List Privacy Act SORN Identifier(s)*

INTERIOR/DOI-16, Learning Management System, 83 FR 50682 (October 9, 2018).

Since LETS maintains records for the purpose of law enforcement training, information maintained in LETS may also be covered under the following Department of the Interior (DOI) SORNs, INTERIOR/DOI-10, Incident Management, Analysis and Reporting System (IMARS), 79 FR 31974 (June 3, 2014); INTERIOR/FWS-20, Investigative Case Files, 64 FR 29055 (May 28, 1999); modification published 73 FR 31877 (June 4, 2008). The FWS-20 SORN is currently under revision to provide general updates and incorporate new Federal requirements in accordance with OMB Circular A-108.

☐ No

H. Does this information system or electronic collection require an OMB Control Number?

☒ Yes: *Describe*

1018-0180 U.S. Fish and Wildlife Service Law Enforcement Training System, expires 5/31/2024

☐ No

Section 2. Summary of System Data

A. What PII will be collected? Indicate all that apply.

☒ Name
☒ Citizenship
☒ Passport Information (International Students only)
☒ Truncated Social Security Number (U.S. Students only)
☒ Home Telephone Number
☒ Official Phone Number
☒ Personal Mobile Phone Number
☒ Mailing/Home Address
☒ Official/Personal Email Address
☒ Gender

☒ Tribal or Other ID Number
☒ Date of Birth
☒ Law Enforcement (badge number)
☒ Employment Information
☒ Emergency Contact
☒ Place of Birth
☒ Other: *Specify the PII collected.*

From FWS LETS users: username and password.

From domestic students (including FWS): full name, gender, date of birth, truncated SSN, home address and telephone number, official or personal mobile number, official or personal email address, years of law enforcement officer experience, education level; agency name; title/rank, level in agency; agency address; supervisor's name, official phone number and email address; emergency contact name and telephone number. The last four digits of the SSN will assist with identifying and searching for student records with similar identifiers.

From international students: full name, gender, country of birth, date of birth, email address, home address, home and cell telephone numbers; country of residence; official passport number, country of issuance, and expiration date, and national identification number, if applicable; emergency contact name and telephone number; years of law enforcement officer experience, education level, and fluency in English and other languages.

LETS will maintain all student training records including dates of all (FWS) courses attended, pre- and post-test scores, and any incomplete training.

B. What is the source for the PII collected? Indicate all that apply.

☒ Individual
☒ Federal agency
☒ Tribal agency
☒ Local agency
☒ DOI records
☐ Third party source
☒ State agency
☐ Other: *Describe*

C. How will the information be collected? Indicate all that apply.

☐ Paper Format
☒ Email
☒ Face-to-Face Contact – it may be possible to register students on site.
☒ Web site

☒ Fax
☐ Telephone Interview
☒ Information Shared Between Systems *Describe*

FWS LEO training records currently contained in FWS' Law Enforcement Management Information System (LEMIS) will be manually imported into LETS.

To register domestic students OLE collects limited PII (full name, official email address and organization) via email from their employing agency and for international students from the U.S. Department of State (DOS). An authorized FWS user imports the students' information into LETS which automatically emails an enrollment confirmation to the students. This email contains a link to a secure web form where the student provides any further information required by FWS (contact information, DOB, gender, official passport number, country of issuance, expiration date, and national identification number) and confirms registration. An authorized FWS user reviews the registration form and enrolls the student. Students may also request enrollment by email or fax to OLE.

For FWS students' enrollment, authorized personnel, e.g. Supervisors, Training Officers, can view the personnel within their organization or sub-organization and may request enrollment for them. The actual enrollment of a FWS student may be automatic upon request, or subject to review and approval, as necessary.

☐ Other: *Describe*

D. What is the intended use of the PII collected?

The intended use of the PII is to accurately record, track and manage who has attended the training offered by FWS and have the capability to search who has attended training upon authorized, official inquiry. OLE needs to be able to confirm the identity of students and locate their records. The last four digits of the SSN assists OLE's Training and Inspection Division to categorize and retrieve students' records accurately.

LETS helps OLE's Training and Inspection Division manage administrative functions including but not limited to: student registration, scheduling and coordination of internal and external training events; testing and collecting course evaluations from students, as well as maintaining required law enforcement training records throughout the career of OLE personnel. In addition, LETS enhances the standardization of many of the internal processes associated with training and also provides OLE with an improved ability to respond to inquiries from Congress, the DOI, and other external agencies.

E. With whom will the PII be shared, both within DOI and outside DOI? Indicate all that apply.

☒ Within the Bureau/Office: *Describe the bureau/office and how the data will be used.*

PII from LETS is shared routinely with authorized FWS OLE employees responsible for law enforcement training and administration of the system. PII is shared with NCTC when training is held there.

☒ Other Bureaus/Offices: *Describe the bureau/office and how the data will be used.*

PII from is routinely shared with other Department Bureaus or Offices who sponsor students for OLE training. PII of DOI employees that attend OLE training may also be shared with the Department's learning management system, DOI Talent.

☒ Other Federal Agencies: *Describe the federal agency and how the data will be used.*

PII is routinely shared with other Federal Agencies who sponsor students at OLE training and with the Federal Law Enforcement Training Center (FLETC). For example, if a U.S. student fails to attend training, OLE will notify the point of contact from the employing agency. For the international students, OLE would notify the U.S. Department of State (DOS) point of contact for that student. PII is shared with FLETC when training is held there, and/or when FLETC co-teaches curriculum in the Wildlife Crime Scene Investigation.

☒ Tribal, State or Local Agencies: *Describe the Tribal, state or local agencies and how the data will be used.*

PII from is routinely shared with Tribal, State or Local Agencies who sponsor students OLE training.

☒ Contractor: *Describe the contractor and how the data will be used.*

PII is shared routinely with authorized FWS OLE contractors responsible for law enforcement training and administration or maintenance of the system.

☒ Other Third Party Sources: *Describe the third party source and how the data will be used.*

Private contractors may be hired to assist instruction and they will have access to the students' PII necessary to teach the course. They will not have access to LETS or the students' personal or training records therein.

F. Do individuals have the opportunity to decline to provide information or to consent to the specific uses of their PII?

☒ Yes: *Describe the method by which individuals can decline to provide information or how individuals consent to specific uses.*

Non FWS students voluntarily provide their PII when registering for training and may decline to provide all the requested information to complete their registration; however, they will not be able to register or attend training.

FWS LEOs are automatically enrolled in LETS and may not have an opportunity to decline; however, they receive notice as to how their PII may be used, maintained and shared during the hiring and onboarding process.

Authorized FWS LETS users may not have an opportunity to decline but they receive notice as to how their PII may be used, maintained and shared during the hiring and onboarding process.

☐ No: *State the reason why individuals cannot object or why individuals cannot give or withhold their consent.*

G. What information is provided to an individual when asked to provide PII data? Indicate all that apply.

☒ Privacy Act Statement: *Describe each applicable format.*

Privacy Act statements are provided during the hiring and onboarding process to all Federal employees including LEOs. LETS provides a Privacy Act statement to all users on the course registration web form (see Section 2.C above).

☒ Privacy Notice: *Describe each applicable format.*

Notice is provided through publication of this PIA and related SORNs published in the *Federal Register*. Please see the SORNs on the DOI SORN website at https://www.doi.gov/privacy/sorn. More information about the Department's privacy program including compliance documents and how to submit a request for agency records protected by the Privacy Act of 1974 is available at DOI's Privacy website at https://www.doi.gov/privacy.

☒ Other: *Describe each applicable format.*

LETS users are provided with a DOI security warning banner upon network logon that they are accessing a DOI system and Privacy Act System of Records, that they are subject to being monitored, and there is no expectation of privacy during use of the system.

☐ None

H. How will the data be retrieved? List the identifiers that will be used to retrieve information (e.g., name, case number, etc.).

Records may be searched for and retrieved by the student's full name, country of origin, or specific identification number identified in question 2.A above.

I. Will reports be produced on individuals?

☒ Yes: *What will be the use of these reports? Who will have access to them?*

LETS can generate an individual's training record. These transcripts generally include the names and dates of all (FWS) courses attended, pre- and post-test scores, and any incomplete training. For example, FWS OLE may disclose a student's LETS training record if a LEO is subject of an official "use of force" review, and the record is requested in accordance with DOI Privacy Act regulations. See 43 CFR Part 2, Subpart K.

☐ No

Section 3. Attributes of System Data

A. How will data collected from sources other than DOI records be verified for accuracy?

Once students' PII collected from DOS or employing agency is manually imported into LETS by an authorized FWS user, LETS emails a secure link to the students to complete a registration form. Students are responsible for verifying the accuracy of their information during registration. Once registered, students may update or correct their information in LETS by contacting the FWS OLE or LETS system administrator.

B. How will data be checked for completeness?

Students are responsible for providing complete information during the registration process. LETS utilizes required fields so that all necessary information must be filled out by users (FWS administrators and students) before they can move forward to the step in the registration process. They will not be able to submit their information until all required fields are completed and validated by the student for completeness and accuracy.

C. What procedures are taken to ensure the data is current? Identify the process or name the document (e.g., data models).

International students are vetted as current official LEOs in good standing by DOS. Domestic students are considered vetted by their employing agency; otherwise students must provide LEO

identification such as badge number to FWS. Current students are responsible for maintaining accurate and current information in LETS.

As for the pre and post test scores, these will be thoroughly reviewed for accuracy and relevancy by trained OLE personnel and their supervisors before adding to the official record pursuant to FWS law enforcement procedures and policies as documented in FWS Service Manual Chapter 400, *Evaluations, Investigations and Law Enforcement*. Data may be verified with other Federal, State or local information databases or law enforcement agencies.

D. What are the retention periods for data in the system? Identify the associated records retention schedule for the records in this system.

In general, LETS training records are considered temporary and may be destroyed after 3 years in accordance with Department Records Schedule 2.1, Short-term Human Resources Records (DAA-0048-2013-0001-0004). It is possible that training records related to specialized program areas may be covered under other approved records retention schedules based on the program or mission area and agency needs. As specified in SORNs INTERIOR/DOI-10, INTERIOR/DOI-16, and INTERIOR/FWS-20, retention periods may vary based on the training program or subject matter, and longer retention is authorized for specific training programs when it is necessary to support business use, or to meet Federal records requirements.

E. What are the procedures for disposition of the data at the end of the retention period? Where are the procedures documented?

Approved disposition methods include shredding or pulping for paper records, and degaussing or erasing for electronic records, in accordance with NARA guidelines and Departmental policy.

F. Briefly describe privacy risks and how information handling practices at each stage of the "information lifecycle" (i.e., collection, use, retention, processing, disclosure and destruction) affect individual privacy.

There are moderate risks to individual privacy inherent in the use of LETS. The primary risks to privacy are unauthorized access, disclosure or misuse of the data and collecting more information than necessary. There are also privacy risks posed from lack of system notice, the possibility of retaining information longer than necessary, inaccurate data caused by indirect collection of PII, as well as capturing information via web form and maintaining information in the "cloud." These risks are addressed and mitigated through a variety of administrative, technical and physical controls.

Unauthorized system access and misuse of the data are mitigated by authenticating all users and controlling access. LETS implements role-based access control using the principles of least

privilege. OLE grants administrative access to only a select number of OLE employees who may view students' PII and control student access and enrollment. Also, any data errors not identified during import into LETS may be corrected by direct student access once granted. Students may request access to and/or amendment of any incorrect, untimely or irrelevant information related to them or their academic performance by writing to the system manager as described in DOI Privacy Act regulations at 43 CFR Part 2, Subpart K.

Unauthorized or inappropriate disclosure is mitigated by requiring all non-routine sharing of data, including PII, and requests for information from LETS go through OLE's Freedom of Information Act (FOIA) team. This team releases or withholds information in accordance with FOIA, the Privacy Act and Departmental regulations and in consultation with the FWS FOIA Officer and Associate Privacy Officer as necessary. Indeed, some records maintained in LETS are exempt from disclosure even to the record-subject such as testing for employment qualifications ((5 USC § 552a(k)(6)). For more of LETS' exemptions see Federal Register publication 40 FR 50432. The Special-Agent-in Charge of OLE's Training and Inspection division is the LETS system owner and reviews all requests and authorizes all disclosures before release.

Controls such as audit logs which monitors system usage and the required user agreements help to prevent misuse of the data. LETS collects only the minimum information necessary to establish eligibility of the applicant and to assess the application, and limits the number of active, standard accounts to current students only. Only the training results/record will be maintained for the LEOs career. Additionally, dispositioning of user account records will be accomplished within the automated records retention functions built in the system.

The privacy risks of collecting and maintaining data in the cloud are mitigated through use of industry-standard encryption techniques. The cloud service provider utilized by LETS is FedRAMP certified; accordingly, all encryption in use is FIPS 140-2 compliant. All web interfaces utilize Hypertext Transfer Protocol Secure (HTTPS) over TLS 1.2 with publicly validated TLS certificates.

There is also some privacy risk associated with lack of notice for the system. This risk is mitigated for Federal personnel by notices provided during the hiring and onboarding process. A Privacy Act statement is provided on the registration form that describes the authority, purpose, and the ways individuals' information may be used, shared and disseminated. External users have the opportunity to decline to provide their information during the registration process. For all users, several notices of routine uses, authorized disclosures and the permissible ways that FWS may collect, use, distribute or maintain information about individuals in LETS are provided in this PIA, the applicable SORNs, and DOI's privacy program and policies available at https://www.doi.gov/privacy. These notices provide information to individuals on how their PII will be used and shared and how they may seek notification, access, or amendment of their records.

LETS is undergoing a formal Assessment and Accreditation toward being granted an authority to operate in accordance with the Federal Information Security Modernization Act

(FISMA) and National Institute of Standards and Technology (NIST) standards. LETS will be rated as Moderate based on the type of data and it requires the Moderate baseline of security and privacy controls to protect the confidentiality, integrity and availability of the PII contained in the system. LETS will develop a System Security and Privacy Plan (SSPP) based on NIST guidance and is a part of the FWS Continuous Monitoring program that includes ongoing security control assessments to ensure adequate security controls are implemented and assessed in compliance with DOI policy and standards.

Finally, the use of LETS will be conducted in accordance with the appropriate DOI use policy. IT systems, in accordance with applicable DOI guidance, will maintain an audit trail of activity sufficient to reconstruct security relevant events. The audit trail will include the identity of each account accessing the system; time and date of access; and activities that could modify, bypass or negate the system's security controls. Audit logs are encrypted and are reviewed on a regular, periodic basis and any suspected attempts of unauthorized access or scanning are reported to the DOI Computer Incident Response Center (CIRC). FWS follows the principal of least privilege so that only the least amount of access is given to a user to complete their required activity. All access is controlled by authentication methods to validate the authorized user. DOI employees and contractors are required to complete annual security and privacy awareness training, and those employees authorized to manage, use, or operate a system are required to take additional Role Based Security and Privacy Training. All employees are required to sign annually the DOI Rules of Behavior acknowledging their security and privacy responsibilities.

Section 4. PIA Risk Review

A. Is the use of the data both relevant and necessary to the purpose for which the system is being designed?

☒ Yes: *Explanation*

FWS has oversight responsibilities under statutory and regulatory authorities to regulate the importation, exportation, and transportation of wildlife. FWS is charged with enforcing Federal wildlife laws and protecting natural resources and is designated to carry out international conservation and enforcement efforts through agreements and treaties such as the Convention on International Trade in Endangered Species of Wild Fauna and Flora (CITES).

OLE is responsible for ensuring that FWS law enforcement personnel are properly and effectively trained to execute their law enforcement duties. OLE also conducts professional training and provides professional development opportunities for FWS employees and contractors to ensure they are well trained and nationally/internationally recognized as outstanding professionals and law enforcement conservation subject matter experts.

OLE coordinates and conducts training for Service special agents, wildlife inspectors, and administrative staff, as well as for State, Native American, and foreign individuals responsible

for wildlife and habitat protection. Over the past decade, there have been substantial increases in the numbers of programs and individuals trained, hours of training provided, and numbers of training sites.

☐ No

B. Does this system or electronic collection derive new data or create previously unavailable data about an individual through data aggregation?

☐ Yes: *Explain what risks are introduced by this data aggregation and how these risks will be mitigated.*

☒ No

C. Will the new data be placed in the individual's record?

☐ Yes: *Explanation*

☒ No – not applicable, LETS does not derive new data or create previously unavailable data about an individual through data aggregation.

D. Can the system make determinations about individuals that would not be possible without the new data?

☐ Yes: *Explanation*

☒ No – not applicable, LETS does not derive new data or create previously unavailable data about an individual through data aggregation.

E. How will the new data be verified for relevance and accuracy?

Not applicable.

F. Are the data or the processes being consolidated?

☐ Yes, data is being consolidated. *Describe the controls that are in place to protect the data from unauthorized access or use.*

☐ Yes, processes are being consolidated. *Describe the controls that are in place to protect the data from unauthorized access or use.*

☒ No, data or processes are not being consolidated.

G. Who will have access to data in the system or electronic collection? Indicate all that apply.

☒ Users
☒ Contractors
☒ Developers (not including access to PII)
☒ System Administrator
☐ Other: *Describe*

H. How is user access to data determined? Will users have access to all data or will access be restricted?

Within the system, access to data is controlled using Role Based Access Control. System administrators may access the PII needed, including DOB, to enroll international students or manage the system.

FWS students may be able to access their own transcripts; all other students or authorized representative will have to request them.

I. Are contractors involved with the design and/or development of the system, or will they be involved with the maintenance of the system?

☒ Yes. *Were Privacy Act contract clauses included in their contracts and other regulatory measures addressed?*

Yes, LETS is FWS' version of Envisage Technologies' Acadis Readiness Suite who will be involved in the maintenance of the system and their contract includes the required Federal Acquisition Regulation (FAR) Privacy Act clauses.

☐ No

J. Is the system using technologies in ways that the DOI has not previously employed (e.g., monitoring software, SmartCards or Caller ID)?

☐ Yes. *Explanation*

☒ No

K. Will this system provide the capability to identify, locate and monitor individuals?

☒ Yes. *Explanation*

The system audit log provides the capability to identify users in the event of inappropriate usage and is only accessible by systems administrators with elevated privileges. The audit log captures administrator activity, authentication checks, authorization checks, data deletions, data

access, data changes, permission changes and access history.

☐ No

L. What kinds of information are collected as a function of the monitoring of individuals?

As a function of monitoring system usage, the log captures date and time of user access, object access, object modification, access changes, and settings changes.

M. What controls will be used to prevent unauthorized monitoring?

LETS utilizes the concept of least access thus limiting access to the minimum functions necessary for the user to perform his or her official duties. Only system administrators who have elevated privileges may access the audit log in accordance with NIST's Control AU-09(4) Protection of Audit Information - Access by Subset of Privileged Users to help prevent unauthorized monitoring. This control requires that the number of users authorized to perform audit-related activity is limited to a small subset of privileged-users.

N. How will the PII be secured?

(1) Physical Controls. Indicate all that apply.

☒ Security Guards
☒ Key Guards
☒ Locked File Cabinets
☒Secured Facility
☒ Closed Circuit Television
☐ Cipher Locks
☒ Identification Badges
☐ Safes
☐ Combination Locks
☒Locked Offices
☐ Other. *Describe*

(2) Technical Controls. Indicate all that apply.

☒ Password
☒ Firewall
☒ Encryption
☒ User Identification
☐ Biometrics
☒ Intrusion Detection System (IDS)

☒ Virtual Private Network (VPN)
☒ Public Key Infrastructure (PKI) Certificates
☒ Personal Identity Verification (PIV) Card
☐ Other. *Describe*

(3) Administrative Controls. Indicate all that apply.

☒ Periodic Security Audits
☒ Backups Secured Off-site
☒ Rules of Behavior
☒ Role-Based Training
☒ Regular Monitoring of Users' Security Practices
☒ Methods to Ensure Only Authorized Personnel Have Access to PII
☒ Encryption of Backups Containing Sensitive Data
☒ Mandatory Security, Privacy and Records Management Training
☐ Other. *Describe*

O. Who will be responsible for protecting the privacy rights of the public and employees? This includes officials responsible for addressing Privacy Act complaints and requests for redress or amendment of records.

The LETS Information System Owner is the official responsible for oversight and management of the LETS security controls and the protection of agency information processed and stored in LETS. The Information System Owner and Information System Security Officer (ISSO) are responsible for ensuring adequate safeguards are implemented to protect individual privacy in compliance with Federal laws and policies for the data managed, used, and stored in the LETS system. These officials and authorized LETS personnel are responsible for protecting individual privacy for the information collected, maintained, and used in the system, and for meeting the requirements of the Privacy Act, including providing adequate notice, making decisions on Privacy Act requests for notification, access, and amendment, as well as processing complaints, in consultation with the FWS Associate Privacy Officer.

P. Who is responsible for assuring proper use of the data and for reporting the loss, compromise, unauthorized disclosure, or unauthorized access of privacy protected information?

The LETS Information System Owner is responsible for oversight and management of the LETS security and privacy controls, and for ensuring to the greatest possible extent that DOI and FWS data in LETS is properly managed and that access to data has been granted in a secure and auditable manner. The Information System Owner is also responsible for ensuring that any loss, compromise, unauthorized access or disclosure of customer agency and agency PII is reported to DOI-CIRC within one hour of discovery in accordance with Federal policy and

established procedures. In accordance with the Federal Records Act, the Departmental Records Officer and bureau Records Officers are responsible for reporting any unauthorized records loss or destruction to NARA per 36 CFR 1230.