U.S. Department of the Interior
PRIVACY IMPACT ASSESSMENT

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 Management Information System (LEMIS)
Bureau/Office: U.S. Fish and Wildlife Service (FWS)
Date: May 7, 2020
Point of Contact:
Name: Jennifer L. Schmidt
Title: Associate Privacy Officer
Email: FWS_Privacy@fws.gov
Phone: (703) 358-2291
Address: 5275 Leesburg Pike, MS: IRTM Falls Church, VA 22041-3803

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

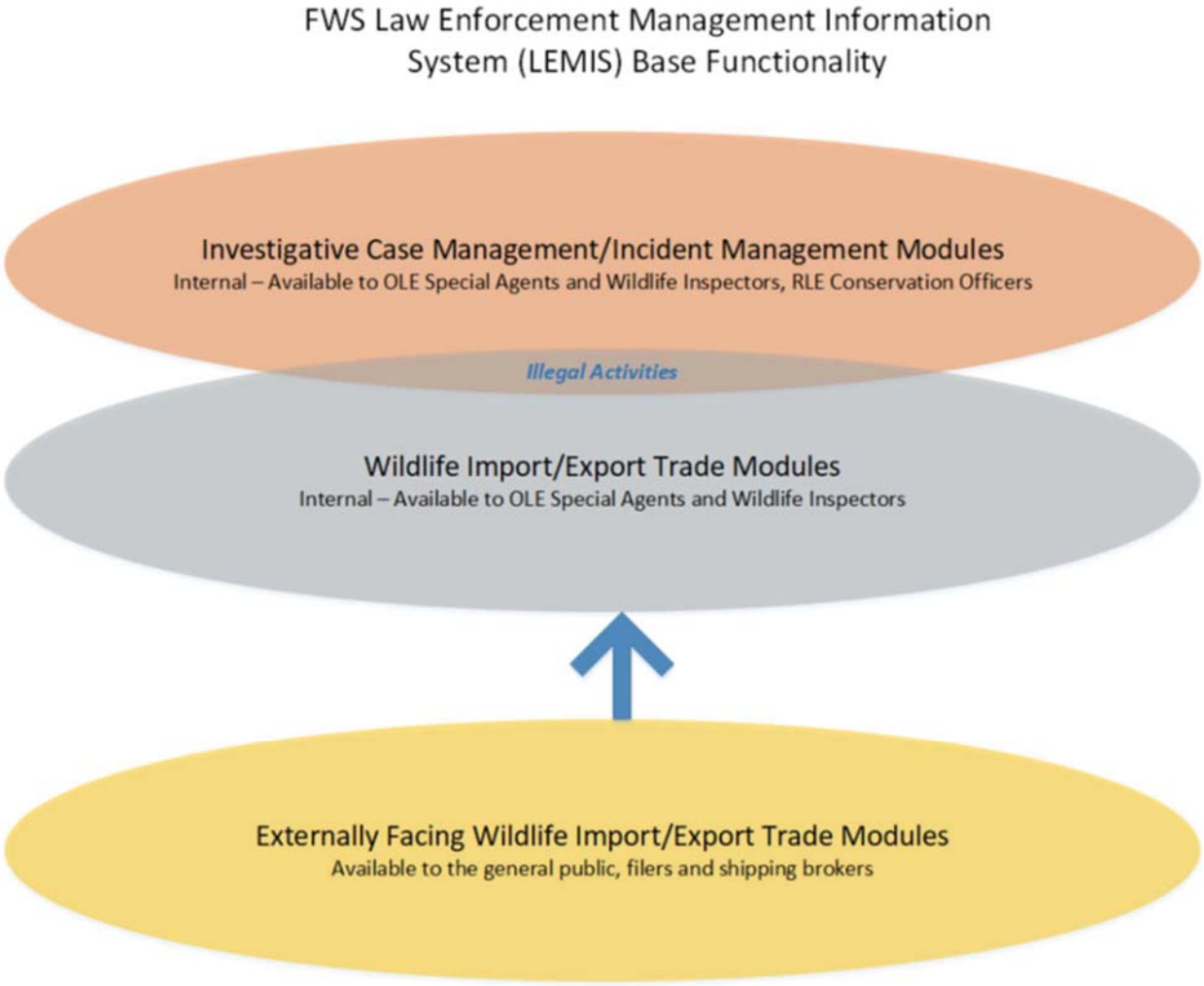
☐ No: *Information is NOT collected, maintained, or used that is identifiable to the individual in this system. Only sections 1 and 5 of this form are required to be completed.*

B. What is the purpose of the system?

FWS law enforcement uses LEMIS to help carry out operations and enforcement actions. LEMIS is comprised of interconnected modules that help the Office of Law Enforcement (OLE) and Refuge Law Enforcement (RLE) achieve the mission of preserving fish and wildlife as national resources by deterring criminal activity and investigating individuals suspected of violating fish and wildlife laws.

Members of the public (individuals and commercial business representatives) use the Electronic License (eLicense) and Electronic Declarations (eDecs) modules within LEMIS to apply for import/export licenses and declare imports and/or exports of wildlife and wildlife products into and out of the U.S. OLE then uses this information to perform its statutory responsibility to inspect shipments and enforce fish and wildlife import/export laws and regulations. See the diagram below for a representation of how the main LEMIS modules interact.

Diagram 1.



C. What is the legal authority?

- Assault Act (18 U.S.C. 111)
- Bald and Golden Eagle Act (16 U.S.C. 668- 868c)
- Black Bass Act (16 U.S.C. 851- 856)

- Lacey Act (18 U.S.C. 42-44)
- National Wildlife Refuge System Administration Act (16 U.S.C 668dd- 668ee)
- Migratory Bird Hunting Stamp Act (16 U.S.C.718-718h)
- Migratory Bird Treaty Act (16 U.S.C. 703-711)
- Endangered Species Act (18 U.S.C. 1531-1543)
- Marine Mammal Act (16 U.S.C. 1361- 1407)
- Upper Mississippi Refuge Act (16 U.S.C. 721-731)
- Bear River Refuge Act (16 U.S.C. 690)
- Fish and Wildlife Recreation Act (16 U.S.C. 460k- 460k-4)
- Airborne Hunting Act (16 U.S.C. 742j)
- Tariff Classification Act (19 U.S.C. 1527)
- Uniform Federal Crime Reporting Act (28 U.S.C. 534)
- Intelligence Reform and Terrorism Prevention Act of 2004 (P.L. 108-458)
- Homeland Security Act of 2002 (P.L. 107-296)
- USA PATRIOT Act of 2001 (P.L. 107-56)
- USA PATRIOT Improvement Act of 2005 (P.L. 109-177)
- Homeland Security Presidential Directive 7 – Critical Infrastructure Identification, Prioritization, and Protection
- Homeland Security Presidential Directive 12 – Policy for a Common Identification Standard for Federal Employees and Contractors
- Criminal Intelligence Systems Operating Policies, 28 CFR Part 23

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 and Privacy Plan (SSPP) Name*

010-000000456 Law Enforcement Management Information System SSPP

☐ No

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.*
Electronic Declarations (eDecs)	Allows public (individuals and businesses) an alternative to filing hardcopy Form 3-177 declarations of imports/exports.	Yes	Username and password; Import/Export License Number; Customs Document Number; Complete name, U.S. or international address, phone number and email address; Customs Broker/Shipping Agent/Freight Forwarder (if applicable) complete business name, address, phone and fax numbers, email address and contact name.
Electronic License (eLicense)	Allows public (individuals and businesses) to request a new import/export license and amend or renew an existing license.	Yes	Username and password; Owner or Principal Officer full name, title and Date of Birth (DOB); Business name, mailing address & full Federal Tax Identification Number (TIN) or last four digits of Social Security Number (SSN); Principal Officer Email Address and phone numbers; Business URL/Web Address; Primary Contact Name, email address and phone number; and current FWS Import/Export (I/E) License number, if applicable. Also, any additional Partner(s) or Principal Officer(s)' full name and title; full TIN or SSN last four; DOB; full mailing address,

			phone number and email address.
Declarations (Decs)	Maintains wildlife import/export data on businesses and individuals	Yes	Same as eDecs and eLicense.
Investigations	Used to store and track all formal OLE investigations.	Yes.	Any PII or personal information pertinent to the law enforcement investigation including name, address, DOB, SSN, physical characteristics, legal ID information, aliases, associated links to active and closed FWS investigations. May also include PII on witnesses, complainants, or investigating officers from across government and FWS employees.
Intelligence This module and its policies and procedures are in compliance with 28 CFR Part 23 - Criminal Intelligence Systems Operating Policies.	Maintains intelligence gathered by OLE.	Yes.	Any PII or personal information pertinent to ongoing investigations or prosecution activities relating to specific criminal activity that falls under the jurisdiction of the Service. This data may include name, address, date of birth, SSN, physical characteristics, legal ID information, aliases, associated links to active and closed FWS Investigations. May also include PII on witnesses, complainants, or investigating officers from across government and FWS employees.
Violation Notice (VN) The module allows users to enter incident information in a Central	Tracks violation notices issued by OLE.	Yes.	VN collects the following: case officer name and badge number; business and individual defendants'

Violations Bureau approved format. The entry form virtually matches the U.S District Court Violation Notice (Form 219).			name, address, phone number, physical description, driver's license information, SSN, vehicle tag information and description, associated links to active or closed FWS investigations or intelligence gathered by FWS.
National Eagle Repository	Used to process and manage requests from the public for eagle parts stored at the repository.	Yes.	Members of federally recognized Tribes provide name, physical address, mailing address (if different), DOB, Migratory Bird permit number, phone numbers, email address, alternate contact person and phone number, enrollment number, inmate number, if applicable. Also collects whether or not the individual or business owner/s has ever been convicted or entered a plea of guilty or nolo contendere for a felony violation of the Lacy Act, Migratory Bird Treaty Act or the Bald and Golden Eagle Protection Act; or forfeited collateral, or are currently under charges for any violations of the laws mentioned above.
National Targeting Initiative	Used by Investigative Analysts to facilitate information sharing with CBP relative to specific data sets.	Yes.	Any PII or personal information pertinent to authorized intelligence gathering activities, investigations or prosecution activities relating to specific criminal activity that

			falls under the jurisdiction of the Service. This data may include name, address, DOB, SSN, physical characteristics, legal ID information, aliases, associated links to active and closed Investigations. May also include PII on witnesses, associations, complainants, or investigating officers from across government and FWS employees.
Refuge Law Enforcement	Incident management and reporting for federal wildlife officers that work on National Wildlife Refuge System (NWRS) lands.	Yes.	Subject name, addresses, unique identifiers, SSN; case officer name and badge number.
Employee Information System	Personnel/HR system	Yes – employees only.	Name, badge number, address, last four of SSN, position and grade, employment information.
Activity Reporting	Tracks hours worked to determine OLE officers' availability pay.	Yes – employees only.	Name, badge number, email address.
Property Tracking	Tracks OLE real property.	Yes – employees only.	Name, badge number, email address.
Law Enforcement Tracking System	Tracks all basic training courses taken by OLE officers.	Yes – employees only.	Name, badge number, email address.
Wildlife Inspector Field Training Program	Tracks field training and evaluations for Wildlife Inspectors.	Yes – employees only.	Name, badge number, email address.
Special Agent Field Training	Tracks field training and evaluations for Special Agents.	Yes – employees only.	Name, badge number, email address.
Access Control	Interface that manages all LEMIS user accounts.	Yes – employees only.	Username and password; name, badge number, email address.
Coordinator Site	Interface used by LEMIS coordinators to	Yes – employees only.	Name, badge number, email address.

	perform basic administrative tasks.		

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/FWS-20, Investigative Case Files (June 4, 2008) 73 FR 31877, and INTERIOR/FWS-21, Permits System (June 4, 2008) 73 FR 31877. These SORNs are currently under revision to provide general updates and incorporate new Federal requirements in accordance with OMB Circular A-108. These systems are exempt from portions of the Privacy Act pursuant to 5 U.S.C. 552a(j)(2) and (k)(2).

INTERIOR/DOI-47: HSPD-12 Logical Security Files (Enterprise Access Control Service/EACS) 72 FR 11040 (March 12, 2007).

☐ No

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

☒ Yes: *Describe*

- 1018-0012, Declaration for Importation or Exportation of Fish or Wildlife, 50 CFR 14.61-14.64 and 14.94(k)(4). Form is available at https://fws.gov/le/pdf/3177_1.pdf; renewal currently pending at OMB;
- 1018-0092, Federal Fish and Wildlife Applications and Reports - Law Enforcement; 50 CFR 13 and 14. Forms are available at https://www.fws.gov/forms/3-200-3a.pdf (US entities) and https://www.fws.gov/forms/3-200-3b.pdf (Foreign entities); renewal currently pending at OMB;
- 1018-0129, Captive Wildlife Safety Act, 50 CFR 14.250-14.255, expires 10/31/22. This information collection is a record-keeping requirement for certain wildlife sanctuaries; there is no official form.

☐ No

Section 2. Summary of System Data

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

☒ Name	☒ Religious Preference	☒ Social Security Number (SSN)
☒ Citizenship	☒ Security Clearance	☒ Personal Cell Telephone Number

☒ Gender	☒ Spouse Information	☒ Tribal or Other ID Number
☒ Birth Date	☒ Financial Information	☒ Personal Email Address
☒ Group Affiliation	☒ Medical Information	☒ Mother's Maiden Name
☒ Marital Status	☒ Disability Information	☒ Home Telephone Number
☒ Biometrics	☒ Credit Card Number	☒ Child or Dependent Information
☒ Other Names Used	☒ Law Enforcement	☒ Employment Information
☒ Truncated SSN	☒ Education Information	☒ Military Status/Service
☒ Legal Status	☒ Emergency Contact	☒ Mailing/Home Address
☒ Place of Birth	☒ Driver's License	☒ Race/Ethnicity

☒ Other: *Specify the PII collected.*

The primary PII LEMIS maintains is:

- Investigative subjects: name, address, DOB, SSN, physical characteristics, legal ID information, aliases, associated links to active and closed FWS investigations. May include photographs or video footage.
- Importers/Exporters: individual name, associated businesses, personal or business address, e-mail address and phone number, Customs Broker or Shipping Agent name, address and phone number.
- Employees: Badge number, name, residence address, Duty Station location, DOB, SSN, job title/grade/step, retirement program, personal phone number, work phone number, date of hire, eligible retirement date, mandatory retirement date, last medical exam date.

LEMIS also contains law enforcement incident reports, law enforcement personnel records, and law enforcement training records, which contain the following information: SSNs, driver's license numbers, vehicle identification numbers, license plate numbers, names, home addresses, work addresses, telephone numbers, email addresses and other contact information, emergency contact information, ethnicity and race, tribal identification numbers or other tribal enrollment data, work history, educational history, affiliations, and other related data, dates of birth, places of birth, passport numbers, gender, fingerprints, hair and eye color, and any other physical or distinguishing attributes of an individual. The system contains images and videos collected from audio/visual recording devices such as surveillance cameras, closed circuit television located at FWS facilities for security and/or law enforcement operations, a mobile video recorder installed on a patrol vehicle and a wearable video recorder (i.e., body-worn cameras) for authorized law enforcement operations.

Recordings of crimes or criminal activity, or recordings done as part of active investigations are maintained according to the investigation's disposition schedule in LEMIS, or in Service-approved hardware in the event that certain refuges and other remote FWS locations have connectivity issues. Additionally, RLE officers working in locations without internet and/or electricity may be temporarily unable to transfer footage from body-worn cameras to LEMIS or

other approved-storage device. In these situations, officers must download the footage as soon as they are able and retain only footage relevant to the authorized law enforcement activity. Otherwise, audio/visual footage is destroyed after 30 days in accordance with FWS' policy on Procedures for Evidence Collection, Handling and Storage (Exhibit 1, 445 FW 3) and the Department's overarching guidance DAA-0048-2015-0002-0001, Routine Surveillance Recordings.

Incident reports and records may include attachments such as photos, video, sketches, medical reports, and email and text messages, and information concerning criminal activity, response, and outcome of the incident. Reports and records may include information related to incidents occurring on National Wildlife Refuges. Refuge incident information may include injuries that are physical, emotional or sexual in nature, including but are not limited to the following: date of birth, age, suspected abuse (Physical, Emotional, Sexual), alleged offender name, potential witness name, etc. Records in this system also include information concerning Federal civilian employees and contractors, Federal, tribal, state and local law enforcement officers and may contain information regarding an officer's name, contact information, station and career history, firearms qualifications, medical history, background investigation and status, date of birth and SSN. LEMIS also contains information regarding officers' equipment, such as firearms, tasers, body armor, vehicles, computers and special equipment-related skills.

eDecs/Decs and eLicense collects whether or not an individual or business owner/s has ever been convicted or entered a plea of guilty or nolo contendere for a felony violation of the Lacy Act, Migratory Bird Treaty Act or the Bald and Golden Eagle Protection Act; or forfeited collateral, or are currently under charges for any violations of these laws. These factors disqualify the individual or business owner/s from receiving or exercising the privileges of a permit or license unless the Service Director approves a waiver. If the respondent answers yes, he or she must also provide the individual's name, date of charge, charge/s, location of incident, court, and action taken for each violation.

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
☒ Web site
☒ Fax
☒ Telephone Interview
☒ Information Shared Between Systems *Describe*

LEMIS receives data from the U.S. Customs and Border Patrol's (CBP) Automated Commercial Environment (ACE). CBP published a PIA on ACE, the main information technology component within the International Trade Data System (ITDS) at: https://www.dhs.gov/privacy-documents-us-customs-and-border-protection. The data flows from external declarations filer systems into ACE/ITDS where it is reviewed and if determined a valid entry, is sent to eDecs via secure transmission. FWS wildlife inspectors analyze the data in eDecs, then transmit back to ACE/ITDS an acknowledgement to proceed, hold for inspection, or reject. (Wildlife inspectors generally perform all inspections although it is possible that authorized customs inspectors may assist or identify wildlife and wildlife product shipments that need authorization from FWS.) FWS and CBP plan to implement an integration of eDecs and ACE by July 2020. The interconnection will allow for the direct exchange of Trade data to and from eDecs and is covered by an inter-agency Interconnection Security Agreement (ISA).

OLE may query FWS' permitting system for FWS permit and permit-holder data. LEMIS does receive endangered species data from FWS' permitting system but the transfer is one-way and contains no PII. The systems do not share any network connections or transmit data directly from system to system.

☒ Other: *Describe*

Data may be collected from authorized surveillance footage including photos or videos; telephone, text message or email records obtained from cellular carriers, internet service providers, and other companies. Information may also be obtained from public access web sites, newspapers, press releases, or other sources. Information may be derived from other Federal systems to share information across the law enforcement community.

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

In general, individual members of the public's and business representatives' PII in LEMIS is used to break up international and domestic smuggling rings that target imperiled animals; prevent the unlawful commercial exploitation of U.S. species; protect wildlife from environmental hazards and safeguard habitat for endangered species; issue and maintain records of notices of violations; enforce Federal migratory game bird hunting regulations and work with States to protect other game species and preserve legitimate hunting opportunities; provide liaison, coordination, and resource assistance in the collection, storage, exchange or

dissemination, and analysis of intelligence information in ongoing investigations or prosecution activities relating to specific criminal activity that falls under the jurisdiction of FWS; provide intelligence information and analysis of this information and suspected criminal activity to law enforcement and judicial personnel on individuals and organizations involved in, associated with, or related to identified criminal organizations and enterprises; inspect wildlife shipments to ensure compliance with laws and treaties and detect illegal trade; work with international counterparts to combat illegal trafficking in protected species; analyze evidence and solve wildlife crimes; protect lands and waters administered by the NWRS; protect NWRS visitors; and prevent unlawful commercial exploitation of all native, trust and endangered species.

Employee and contractor PII in LEMIS is used for human resources and administrative functions such as maintaining law enforcement equipment inventories and tracking personnel actions like training requirements, station and career history, firearms qualifications, special skills or certifications, assignments for government-issued property including tasers, body armor, vehicles, computers and devices.

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.*

LEMIS PII may be shared with FWS employees and contractors who have a "need-to-know" in the performance of their official duties. Routine sharing occurs between OLE and other FWS permit programs in Migratory Birds Management, Division of Management Authority, International Affairs and Ecological Services. OLE may query FWS' permitting system for FWS permit and permit-holder data.

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

PII may be shared with Department employees and contractors who have a "need-to-know" in the performance of their official duties. In the ordinary course of business, PII related to investigations is shared with the Department's Office of Law Enforcement and Security. PII may be shared with other Bureau law enforcement offices pursuant to a formal law enforcement request.

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

OLE shares importers and exporters PII routinely with the U.S. Customs and Border Patrol (CBP) via ACE to facilitate customs inspections. OLE collaborates with CBP and other law enforcement and intelligence agencies at CBP's Commercial Targeting and Analysis Center (CTAC). The CTAC is an operational extension of "One-U.S. Government at the Border" and an inter-agency effort to prevent, deter, interdict and investigate violations of import and export laws. OLE intelligence analysts staff the CTAC to facilitate information sharing and leverage

collective resources of participating government agencies. For example, OLE may submit requests for information on a target data set (all shipments from company X through the port of Y) to CBP through LEMIS' National Targeting Imitative module. The OLE Intelligence Analyst assigned to the CTAC submits the request into CBP's system, retrieves the results, then manually loads them into NTI for the requesting officer.

OLE shares PII of investigative subjects routinely with Assistant U.S. Attorneys for the purpose of prosecuting wildlife crimes.

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

Investigative subjects' PII is shared routinely with State Divisions of wildlife and law enforcement agencies.

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

Contractors working directly for OLE have authorized access to all LEMIS modules and databases.

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

PII is shared with attorneys or court staff for judicial reasons. Information may also be shared with other third parties as authorized and described in the routine uses published in the INTERIOR/FWS-20, Investigative Case Files and INTERIOR/FWS-21 Permits System system of records notices available at https://www.doi.gov/privacy/fws-notices.

All authorized disclosures of PII outside of the Department are documented in the case file by the investigating case officer in accordance with the Privacy Act of 1974 (5 U.S.C. 552a(c)(1)).

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.*

Import/export license applicants and those declaring wildlife customs receive notice of how their information may be used and that failure to provide the information may prevent them from being able to import or export wildlife or wildlife products into or out of the U.S.

FWS employees and contractors assigned to OLE/RLE may not decline to provide PII in order to be granted authorized access to the system; however, they do receive notice of how their PII may be used 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 available on hard copy forms, 3-177, *Filers of the Declaration for the Importation of Exportation of Fish or Wildlife*; on the eDecs login and account creation web pages; on the hard copy 3-200 series forms, *Federal Fish and Wildlife Permit Applications and Reports,* and on the eLicense login and account creation web pages.

☒ Privacy Notice: *Describe each applicable format.*

Notice is provided through publication of this PIA and related SORNS published in the *Federal Register*. License applicants and declarations filers as well as FWS users (employees and contractors) receive notice of system monitoring at login. Also, the FWS internet privacy policy is hyperlinked in every FWS webpage footer. More information about the Department's privacy program including how to submit a request for records protected by the Privacy Act is available at https://www.doi.gov/privacy.

☒ Other: *Describe each applicable format.*

Subjects of investigations and prosecutions may receive notice of their rights under the Fifth Amendment including the "Miranda Warning."

☒ None.

In most instances, individualized notice to persons under investigation would interfere with OLE/RLE's ability to obtain, serve, and issue subpoenas, warrants and other court documents that may be filed under seal, and could result in disclosure of investigative techniques, procedures, and evidence. In addition, providing notice in certain situations could impede law enforcement by compromising the existence of an investigation or reveal the identity of witnesses or confidential informants. The FWS-20 Investigative Case Files system is exempt from portions of the Privacy Act (40 FR 50432). For use of audio and visual recordings, individuals who enter on Federal properties and public areas, including NWRS lands, do not have a reasonable expectation of privacy. Some FWS-controlled areas may have signage that informs individuals of surveillance activities, but in many cases notice may not be provided or consent obtained for audio or images captured during law enforcement activities.

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

Data is retrieved routinely name of case subject or location. Data may also be retrieved by PII in any LEMIS identifier data field, and/or by any related investigative case or incident numbers.

I. Will reports be produced on individuals?

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

Authorized users can manually run reports for investigative purposes. The following reports are available to authorized users: Be On the Lookout (BOLO), Request for Identification Report, Criminal History Report, and Missing Person reports or Amber/Silver alerts. Incident, supplemental, crash, arrest, ticket, and suspicious activity reports can be produced. Detailed information may be viewed by authorized users including incident, person, property, vehicle, address, etc. Administrative reports may also be generated in response to audits, oversight, and compliance. Reports of historical violations or convictions on individuals are available to run in LEMIS.

OLE/RLE use LEMIS data to create investigative reports on individuals or businesses as needed for FWS and Department leadership, and for referrals to State or local law enforcement, DOJ and Assistant U.S. Attorneys.

☐ No

Section 3. Attributes of System Data

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

License applicants and declaration filers must acknowledge that they have read and are familiar with Federal fish and wildlife regulations; that they are submitting complete and accurate information; and that any false statement in their application/s may lead to criminal penalties pursuant to 18 U.S.C. 1001.

eDecs and eLicense user accounts are first verified for accuracy by wildlife inspectors and permit issuers/examiners, respectively, before individuals may use the system to file declarations or apply for/renew their license/s.

Import/export declarations are verified for accuracy by a multi-tiered review process. First, the declaration is reviewed to ensure the filer has an existing import/export license and that all the filer identifying information matches. Then, the declaration itself is queued up for review by

port-based wildlife inspectors. Using their training and specialized knowledge, inspectors choose to either clear, refuse, hold for physical inspection, or re-export back to the country of origin. Inspected shipments whose declarations are inaccurate may be subject to further inspection and/or criminal prosecution.

License applications or renewals are first reviewed to ensure all identifying information is accurate and then for any historical violations, investigations or incidents. Applications without issue are accepted while those with "hits" are sent for further review and decision to the Assistant Special Agent in Charge (ASAC).

For investigations, direct supervisors must approve cases within 30 days of opening and again every 90 days until the case is closed. Upon closure or referral for prosecution, the ASAC and Special Agent in Charge (SAC) also approve.

B. How will data be checked for completeness?

LEMIS utilizes required fields wherever possible. Any missing required data element will prevent the application or declaration from being submitted in eDecs and eLicense.

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

Licenses must be renewed annually. Declarations must be filed prior to every shipment into or out of the U.S. Authorized eDecs and eLicense users are responsible for maintaining accurate, complete and relevant information in their profiles, applications and declarations. These modules passwords must be changed every 60 days which provides importer/exporters to update their account information which they may do anytime. Accounts are automatically deleted after 13 months of inactivity.

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

LEMIS records including audio/visual recordings are retained and disposed of in accordance with FWS Records Schedule, Enforcement Records (ENFR-110) which has been approved by the National Archives and Records Administration (NARA) (N1-022-05-01/63). LEMIS records are considered temporary and may be deleted 20 years after the related case is closed.

Non-investigative data includes data relating to the user/officer and their unit of assignment, badge number, training, qualifications, etc. This data will be cut-off after the user/officer retires, resigns, leaves FWS, or is assigned to a position that no longer requires access to LEMIS. This data is archived three years after cut-off and destroyed 65 years after archiving.

Video records and other types of evidence are managed in accordance with FWS' policy on Procedures for Evidence Collection, Handling and Storage (Exhibit 1, 445 FW 3) and the Department's overarching guidance DAA-0048-2015-0002-0001, Routine Surveillance Recordings. The Department's guidance provides that recordings of a non-evidentiary value will be destroyed after 30 days. There may be circumstances where RLE working in remote locations without internet and/or electricity may be temporarily unable to upload the footage from their body-worn cameras to LEMIS or other FWS-approved storage device within the 30 day time limit. In these circumstances, officers must download the footage as soon as they are able and retain only footage relevant to the authorized law enforcement activity in accordance with FWS' forthcoming official guidance concerning body-worm cameras.

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 384 Departmental Manual 1. Archival and disposition of records will be accomplished within the automated records retention functions built in the system and procedures will follow applicable guidance by NARA, applicable legislation such as the Federal Records Act, Departmental guidance and the FWS Records Schedule. These procedures are documented in FWS' policy, Case Management Documentation (449 FW 1). Further procedures for disposition of evidence are documented in FWS' Procedures for Evidence Collection, Handling and Storage (Exhibit 1, 445 FW 3).

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 privacy risks due to the amount of sensitive PII and personal information maintained in LEMIS. LEMIS maintains law enforcement personnel and training records as well as investigations and reports necessary for the enforcement of fish and wildlife laws and regulations. These privacy risks include unauthorized access, unauthorized disclosure and misuse of data in the system. There are also privacy risks inherent in data sharing with other law enforcement agencies; the use of audio/visual recording devices during surveillance; lack of notice to subjects of investigations, and in collecting more information than is relevant and/or storing information longer than necessary. These risks are addressed and mitigated through a variety of administrative, technical and physical controls.

Authorized FWS personnel are granted access to the system via the Department's Active Directory. Only authorized individuals with proper credentials can access LEMIS secure modules. eDecs and eLicense public users are verified and authenticated before granted access. eLicense requires two-factor authentication for public users to login. (eDecs plans to implement two-factor authentication in the near future.) Once logged in, user access to data and/or modules

is controlled by the system's in-house Access Control System. Access levels are based on least privilege and role-based controls. For example, a wildlife inspector by default is given read/write access to the Investigations and Declarations modules. A program analyst by default receives read only access to Investigations and Declarations, but read/write access to the Property and Employee Information modules.

Audit trails exist for the creation and modification of data within LEMIS. All system changes or modifications are documented. The documentation details the nature of the change, steps taken to make the modification, and, if appropriate, procedures to restore the original configuration if necessary. Output is restricted in all modules. Of particular note, the Investigations module uses case and report distribution lists to strictly control access while open. The Employee Information System limits access to regional personnel.

LEMIS functions as a case management system and is not the official repository for all case information. The official case files are retained in hard copy at OLE and RLE regional offices. As such, LEMIS maintains certain key information. It uses mandatory data fields and commonly populated drop-down lists to ensure the accuracy and completeness of its data. As a final review, all investigative case files and shipment information go through a series of approval and review stages prior to closure. Employee records are closely controlled and are also subject to supervisory review.

Privacy risks from sharing with other law enforcement agencies include loss of data integrity; loss of data and data confidentiality for data shared and controlled by other organizations. Memoranda of Understanding or Agreement (MOU/A) are established with CBP and States to ensure controls are in place to protect privacy on joint task forces or investigations. All authorized disclosures of PII outside of the Department are documented in the case file by the investigating case officer in accordance with the Privacy Act of 1974 (5 U.S.C. 552a(c)(1)) and to help maintain the integrity of the data.

There is also a privacy risk for the use of audio/visual recording devices, such as body cameras, dashboard cameras, and hand-held cameras, used for routine law enforcement purposes, to enhance officer safety, promote cost savings, assist in crime prevention, and support law enforcement investigations. These cameras are worn by Federal Wildlife Officers; placed on the dashboard of their vehicles, or used by individual law enforcement officials on properties and locations within the jurisdiction of the FWS, including NWRS lands.

These devices may capture audio and images of persons, places and events occurring in real time as part of ongoing law enforcement operations, such as identifying persons involved in potential criminal activity, or persons or vehicles fleeing from law enforcement officials. Some devices may capture metadata about the audio, images or recordings, such as time, location and date the audio, images or video were captured. Users may use settings to zoom in for persons or objects of specific interest, or pan areas of interest. Images or recordings could be used in any appropriate law enforcement investigation related to a potential criminal activity, including identification of suspects and providing evidence that may be used in proceedings.

Some privacy concerns are that devices may collect more information that is necessary to accomplish law enforcement purposes. The devices are used only by authorized law enforcement officials and only to support law enforcement activities and investigations, prevent crime, and enhance officer safety. Only the images or video feed needed to investigate unlawful activities or support investigations and prosecutions are retained. Audio/video recording not related to an investigation is automatically overwritten or disposed of every 30 days or as soon as remote officers are able per DOI/FWS policy.

Another concern is that the use of the audio/visual recording devices may restrict First Amendment protected activities like freedom of speech or association. The recordings are used to detect and deter criminal activity and enhance officer and citizen safety, and are not used for the sole purpose of restricting or investigating lawful activities conducted by members of the public. First Amendment activities will not be filmed for the sole purpose of identifying and recording the presence of individual participants engaged in lawful conduct. First Amendment activities may be recorded, however, for purposes of (1) documenting violations of law or civil wrongs; (2) aiding future coordination and deployment of law enforcement units; or (3) training; or (4) to mitigate or relieve overcrowding to enhance public safety.

All information collections by or for FWS law enforcement are authorized and thoroughly reviewed for accuracy and relevancy by trained law enforcement personnel and their supervisors before opening or closing investigations, and before including the information in the local case file or in the LEMIS case management file. Information derived at through different sources may provide more information about an individual and this data may be outdated or inaccurate; however, aggregated data is verified and also thoroughly reviewed for accuracy, relevancy and completeness before becoming part of an investigation. These verification and assurance procedures are documented in FWS Service Policy Series 400, Evaluations, Investigations and Law Enforcement. Archival and disposition of LEMIS records is accomplished within the automated records retention functions built in the system and following from applicable NARA, Federal Records Act, DOI and FWS policies and guidance.

Several notices of routine uses, authorized disclosures and all the permissible ways that FWS may collect, use, distribute or maintain information about individuals in LEMIS are provided in this PIA, the applicable SORNs, and DOI's privacy program and policies available at https://doi.gov/privacy. Individualized notice to persons under investigation however would interfere with OLE/RLE's ability to obtain, serve, and issue subpoenas, warrants and other court documents that may be filed under seal, and could result in disclosure of investigative techniques, procedures, and evidence. In addition, providing notice in certain situations could impede law enforcement by compromising the existence of an investigation or reveal the identity of witnesses or confidential informants. The Final Rule for the FWS-20 Investigative Case Files SORN exempts this system from portions of the Privacy Act (40 FR 50432).

These privacy risks are mitigated. LEMIS has undergone a formal Assessment and Accreditation and has been granted an authority to operate in accordance with the Federal Information Security Modernization Act (FISMA) and National Institute of Standards and

Technology (NIST) standards. LEMIS is 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. LEMIS has developed 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 LEMIS is conducted in accordance with the appropriate DOI, FWS and law enforcement or intelligence 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 DOI 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. All 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. Additionally, LEMIS users must agree and sign a Statement of Responsibility, Password Control Document, and LEMIS Rules of Behavior.

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 authority to regulate the importation, exportation, and transportation of wildlife. FWS' inspection program is framed by the Endangered Species Act and the Lacey Act amendments of 1981. FWS is also charged with enforcing Federal wildlife laws and protecting natural resources, visitors and employees on NWRS lands.

☐ 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.*

LEMIS uses a third-party Commercial-off-the-Shelf (COTS) product to search eDecs & Declarations, eLicense, and Investigative modules for information related to investigative subjects in effort to identify previously unknown historical violation patterns and/or associations within the system. This information, if discovered, is thoroughly reviewed by supervisors and law enforcement officials before being entered into a case file or individual's record. This review process helps to mitigate the risk that aggregate data may be irrelevant, outdated or inaccurate. LEMIS does not engage in data mining as defined by the Federal Agencies Data Mining Report Act of 2007. LEMIS searches are primarily subject-based and use personal identifiers of a specific individual, or inputs associated with a specific individual or group of individuals, to retrieve information.

☐ No

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

☐ Yes: *Explanation*

☒ No – new data discovered through data aggregation is not automatically placed into a case file or an individual's record. It is reviewed by supervisors and law enforcement officials for veracity, relevancy and completeness before being entered into any case file or individual record.

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

☐ Yes: *Explanation*

☒ No – Data aggregation in LEMIS does not make determinations about individuals possible. OLE/RLE make determinations about individuals with and without aggregate data. LEMIS does not make any automated determinations or decisions.

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

New data is thoroughly reviewed for accuracy and relevancy by trained law enforcement personnel and their supervisors before adding to the official record pursuant to FWS law enforcement procedures and policies documented in Series 400, Evaluations, Investigations and Law Enforcement. Data may be verified with other Federal, State or local information databases or law enforcement agencies.

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
☒ System Administrator
☐ Other: *Describe*

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

LEMIS uses the Department's Active Directory and its customized Access Control System to assign role-based access for FWS employees and contractors. Importers and exporters have read/write access to their applications and declarations. Once submitted, the data is locked and users' access changes to read-only.

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?*

LEMIS contracts include the required privacy clauses pursuant to Federal Acquisition Regulations.

☐ 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, accessible only to system administrators with elevated privileges, provides the capability to identify users in the event of inappropriate usage. The investigative and intelligence modules maintain information on case subjects, such as physical attributes, photos, videos, and personal or professional physical addresses, that authorized users and law enforcement officers may use to analyze crimes or criminal activity and investigate case subjects as part of authorized law enforcement operations, but the purpose of the system itself is not to identify, locate and monitor individuals.

☐ No

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

The system audit log records the username, login date and time. The investigative and intelligence modules audit logs also capture the username and time of last change made to data. This is the only information collected on the system audit log.

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

LEMIS 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 LEMIS Information System Owner is the official responsible for oversight and management of the LEMIS security controls and the protection of agency information processed and stored in LEMIS. The Information System Owner and LEMIS Privacy Act System Manager 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 LEMIS system. These officials and authorized LEMIS 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 bureau and office Associate Privacy Officers.

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 LEMIS Information System Owner is responsible for oversight and management of the LEMIS security and privacy controls, and for ensuring to the greatest possible extent that DOI and FWS data in LEMIS 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.

Section 5. Review and Approval

Information System Owner

Name: George Volentir
Title: System Security Supervisor
Bureau/Office: OLE
Phone: (303) 275-240 Email: george_volentir@fws.gov
Signature: GEORGE VOLENTIR Digitally signed by GEORGE VOLENTIR Date: 2020.05.07 07:14:29 -06'00'

Information System Security Officer

Name: Travis Hay
Title: Information System Security Officer
Bureau/Office: Information Resources and Technology Management
Phone: Email: travis_hay@fws.gov
Signature: TRAVIS HAY Digitally signed by TRAVIS HAY Date: 2020.05.07 07:20:08 -06'00'

Privacy Officer

Name: Jennifer L. Schmidt
Title: Associate Privacy Officer
Bureau/Office: Information Resources and Technology Management
Phone: (703) 358-2291 Email: jennifer_schmidt@fws.gov
Signature: JENNIFER SCHMIDT Digitally signed by JENNIFER SCHMIDT Date: 2020.05.07 06:45:53 -04'00'

Reviewing Official

Name: Teri Barnett
Title: Departmental Privacy Officer
Bureau/Office: Department of the Interior
Phone: (202) 208-5681 Email: teri.barnett@ios.doi.gov
Signature: Digitally signed by NGOC THUY BARNETT Date: 2020.05.07 17:23:48 -04'00'