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: Unmanned Aircraft System (UAS) Program

Date: 01-12-2016

Bureau/Office: Office of Aviation Services

Bureau/Office Contact Title: National UAS Specialist

Point of Contact Email	First Name	M.I.	Last Name	Phone
Bradley_Koeckeritz@ios.doi.gov	Bradley		Koeckeritz	(208) 433-5091

Address Line 1: 300 E. Mallard

Address Line 2: Ste. 200

City	State/Territory	Zip
Boise	Idaho	83706

Section 1. General System Information

A. Is a full PIA required?

Yes

Yes, information is collected from or maintained on

All

B. What is the purpose of the system?

The Department of the Interior (DOI) Office of Aviation Services (OAS) is responsible for the development of a comprehensive and actionable strategy for the use of Unmanned Aircraft Systems (UAS). A UAS consists of an unmanned aircraft, command and control network, and personnel who operate the unmanned aircraft from the ground. OAS is conducting a privacy impact assessment (PIA) to identify and address privacy implications for the use of UAS, particularly surveillance, image and video capabilities. This PIA covers the general use of UAS as authorized by OAS in accordance with Federal and Departmental policy. Due to the broad scope of DOI missions and UAS program activities,

it is not feasible to detail each specific bureau or office use of data obtained from UAS technology. Each DOI bureau or office that uses UAS in a way that is inconsistent or outside the scope of this PIA will ensure a separate PIA is conducted for the specific legitimate purpose and address any distinct privacy risks related to the specific use, as well as meet any additional privacy and security compliance requirements for the use of the UAS technology and collection and maintenance of data within their systems. DOI UAS activities are conducted in accordance with Federal UAS policy and DOI Operational Procedures Memorandum (OPM)-11, DOI Use of Unmanned Aircraft Systems (UAS), which may be viewed at the DOI OAS UAS website: https://www.doi.gov/aviation/uas. OPM-11 is reviewed and updated annually to ensure policy, procedures and protections regarding DOI official use of UAS is current and in alignment with Federal government-wide requirements.

DOI UAS are principally operated over public lands and waters and with permission over public and private lands of our Federal, State, Local, Tribal, and private partners. This includes millions of acres of land and waters administered by DOI bureaus and offices for conservation, management, preservation, and restoration of national parks, national conservation lands, national monuments, wildlife refuges, and Outer Continental Shelf waters. The use of UAS allows DOI bureaus and offices, including the National Park Service, Bureau of Land Management, Fish and Wildlife Service, Bureau of Indian Affairs, Bureau of Reclamation, Bureau of Ocean Energy Management, Office of Surface Mining Reclamation and Enforcement, U.S. Geological Survey and the Office of the Secretary, to cover wide geographic areas during these activities in support DOI's mission to protect the nation's natural and cultural resources.

UAS technology possesses the ability to significantly expand DOI's ability to obtain remote data critical to fulfilling many mission requirements with less cost, less environmental impact, and enhanced safety. UAS also promotes safety and reduces risks to employees engaging in potentially hazardous operations, particularly for emergency responders for rapid response and situational awareness. UAS are valuable tools that allow DOI to achieve mission objectives to include scientific, environmental and land-management applications, as well as increased situational awareness for law enforcement efforts. Current uses of UAS at DOI include:

- Population surveys of threatened and endangered species
- Wildlife habitat and migration surveys (including marine mammals)
- Geology and geophysical surveys and scientific study
- Erosion mapping
- Monitoring breeding
- Boundary assessment and invasive species detection
- Abandoned solid waste assessments
- Run-off and coal seam fire assessment
- River impact monitoring during dam removal
- Burned area assessment and wildland fire precision mapping and suppression
- Weather reconnaissance – temperature, humidity, wind speed
- Search and rescue
- Emergency response and disaster recovery – landslides, earthquakes, floods
- Regulatory compliance – wetland protections, easement protections, refuge protections, encroachments, illegal dumping, illegal residences on DOI lands, pre and post mining surface comparisons, mine inspections, abandoned mine lands feature determinations and other mining related compliance .
- Law Enforcement – aerial assistance for law enforcement situational awareness
- National security – joint operations related to activities impacting DOI lands

DOI UAS employed for law enforcement assistance or national security purposes may include surveillance for situational awareness and aerial reconnaissance, support for investigative operations, and support joint operations with other law enforcement organizations for activities that impact DOI lands, to promote safety and reduce risk to law enforcement officers. Information collected during these activities may include PII that will be processed and analyzed by authorized personnel for law enforcement purposes, and may be shared with law enforcement organizations as appropriate for the specific case.

UAS by definition are considered aircraft regardless of size or weight. While the methods of control and airspace utilization procedures are different than manned aircraft, the overall responsibility for management of UAS within the DOI rests within OAS. Ownership of all DOI owned or contracted aircraft, including UAS, is a function and responsibility of OAS. Additionally, OAS will coordinate with other Federal agencies on UAS policy and cooperate with the Federal Aviation Administration (FAA) on existing and proposed rulemaking. DOI bureaus and offices must follow Federal and DOI policy when using any UAS, either DOI-owned or DOI contract vendor-owned and operated under DOI operational

control.

DOI currently owns UAS that include small unmanned aircraft typically under 55 pounds with wingspans of 3 to 6 feet or less that are typically operated using a wireless ground control stations. These UAS are equipped with sensors and cameras that can capture and store images or other data, or can transmit them to ground control systems to provide aerial views in support of numerous DOI missions.

Information collected by or on behalf of DOI bureaus and offices using UAS that may contain personally identifiable information (PII) will not be retained for more than 180 days unless retention of the information is determined to be necessary to an authorized mission of the retaining agency, is maintained in a system of records covered by the Privacy Act, or is required to be retained for a longer period by any other applicable law or regulation.

C. What is the legal authority?

49 U.S.C. 40125, Qualifications for public aircraft status; OMB Circular A-16, Coordination of Geographic Information, and Related Spatial Data Activities; and Executive Order 12906, Coordinating Geographic Data Acquisition and Access: The National Spatial Data Infrastructure

D. Why is this PIA being completed or modified?

Other

Describe

To assess privacy implications for use of UAS that are equipped with technology that may capture information associated with individuals in support of DOI missions.

E. Is this information system registered in CSAM?

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	Describe
None	None	No	

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)

DOI UAS employed for law enforcement assistance or national security purposes may include PII that will be processed and analyzed by authorized personnel for law enforcement purposes and may be shared with law enforcement officials as appropriate for the specific case. Any PII collected for this law enforcement purpose and associated with a case is maintained in DOI's Department-wide law enforcement system of records, DOI-10, Incident Management, Analysis and Reporting System.

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

No

Section 2. Summary of System Data

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

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

Specify the PII collected.

Data collected through the use of UAS for DOI natural resources missions consists of still images, videos, and sensor or radar data that may include incidental images of persons, buildings, vehicles and residences that may be associated with persons. Data may be collected in support of law enforcement surveillance or emergency response purposes, and may include still images, videos, and sensor or radar data that identifies persons, vehicles, and private residences.

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

Some data may be obtained from scientific studies conducted with agency partners, such as universities, contractors, academic or research institutions through cooperative agreements. In these cases, data collected is used to develop scientific studies as part of the agency's environmental mission, and PII is not intentionally collected. Research data is shared with Federal partners and the finalized studies with the public.

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

- ☐ Paper Format
- ☐ Email
- ☐ Face-to-Face Contact
- ☐ Web Site
- ☐ Fax
- ☒ Other
- ☐ Telephone Interview
- ☐ Information Shared Between Systems

Describe

Information is collected via live streaming data collection or on-board data recording.

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

The vast majority of DOI missions consist of natural resources and public land management responsibilities. Airborne data collection activities from UAS conducted in support of these responsibilities include, but are not limited to:

- Geology and geophysical surveys and scientific study
- Erosion mapping
- Monitoring breeding
- Boundary assessment and invasive species detection
- Abandoned solid waste assessments
- Run-off and coal seam fire assessment
- River impact monitoring during dam removal
- Burned area assessment and wildland fire precision mapping and suppression
- Weather reconnaissance – temperature, humidity, wind speed
- Search and rescue
- Emergency response and disaster recovery – landslides, earthquakes, floods

• Regulatory compliance – wetland protections, easement protections, refuge protections, easement encroachments, etc. on DOI lands

As these activities are conducted (by definition of DOI's responsibilities) on public lands and waters of the Outer Continental Shelf, there exists the possibility that information collected during these non-law enforcement missions may contain PII inadvertently collected in the course of the public's use of public lands and water.

Information collected by or on behalf of DOI bureaus and offices using UAS that may contain PII will not be retained for more than 180 days unless retention of the information is determined to be necessary to an authorized mission of the retaining agency, is maintained in a system of records covered by the Privacy Act, or is required to be retained for a longer period by any other applicable law or regulation

For law enforcement purposes, images may be provided to law enforcement officials for processing, use, and dissemination as appropriate. Access to the image and analysis of a particular area, including any associated PII, is given only to authorized persons who have an official "need to know". In these cases, PII associated with persons who were video recorded from a UAS may be associated with a case file and incorporated into DOI's law enforcement system, DOI-10, Incident Management, Analysis and Reporting System (IMARS) or other bureau/office system of records. Please review the IMARS PIA for assessment of privacy implications for use of IMARS. The DOI IMARS SORN and PIA may be viewed on the DOI Privacy Program website at https://www.doi.gov/privacy/privacy-program.

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 or office and how the data will be used.

Data obtained from UAS operated over public lands and waters, and with permission, public and private lands of our Federal, State, Local, Tribal, and private partners may be shared within the originating DOI bureau or office utilizing the UAS technology to achieve mission objectives, including scientific, environmental and land-management applications. These uses generally do not involve any collection or maintenance of PII.

DOI may use UAS in support of Federal, Tribal, State or local agencies for emergency response, natural disasters, or for increased situational awareness for law enforcement efforts. In these cases, data may be obtained or shared under a cooperative agreement or during cooperative operations with these organization and may include still images, video feeds, or downloaded video recordings that may be shared with authorized officials within the originating bureau or office.

☒ Other Bureaus/Offices

Describe the bureau or office and how the data will be used.

Data from UAS collected in support of Federal, Tribal, State or local agencies for emergency response, natural disasters, or for increased situational awareness for law enforcement efforts, or to achieve mission objectives, including scientific, environmental and land-management applications may be shared with other bureaus within DOI as authorized and necessary to support the DOI mission.

Video, still images, and/or radar images collected during investigative operations as part of a law enforcement investigation are used for enhanced situational awareness and may be used to provide evidence of a violation of law and shared with the Office of Law Enforcement and Security. These images are maintained in association with the investigative or case file that they support. Video, still images, and/or images collected in natural disaster and/or emergency situations are used for relief work and disaster reconnaissance. Video, still images, and/or radar images are not associated with an individual and are only used to indicate where an individual or group of individuals may be for emergency response purposes. Video, still images, and/or radar images of private citizens or property may be incidentally captured and will not be used for any purpose.

☒ Other Federal Agencies

Describe the federal agency and how the data will be used.

Data may be shared with other Federal agencies for law enforcement or emergency response purposes when authorized. Data may be obtained or shared from Federal partners under a cooperative agreement or during cooperative operations. Information shared may include still images, video feeds, or downloaded video recordings.

☒ Tribal, State or Local Agencies

Describe the Tribal, state or local agencies and how the data will be used.

DOI may use UAS in support of Tribal, State or local agencies for emergency response, natural disasters, for law enforcement and other resource purposes. Data may be obtained or shared under a cooperative agreement or during cooperative operations with these organization and may include still images, video feeds, or downloaded video recordings. Any joint operation or information sharing is in accordance with a Memorandum of Understanding or other sharing agreement in accordance with DOI policy. Recipients of data gathered by DOI UAS are subject to Federal policy, regulations, and DOI policy governing use of UAS.

☒ Contractor

Describe the contractor and how the data will be used.

DOI bureaus and offices may use contractors to support various program areas. DOI contractors are subject to Federal policy, regulations, and DOI policy governing use of UAS, and must meet all statutory and policy requirements for information management and security and privacy.

☒ Other Third Party Sources

Describe the third party source and how the data will be used.

Data may be shared with scientific studies conducted with agency partners, such as universities, contractors, academic or research institutions through cooperative agreements. In these cases, data collected is used to develop scientific studies as part of the agency's environmental mission, and generally does not include PII. In these cases, the partner entities are governed by Federal policy, regulations, and DOI policy regarding UAS and information management, privacy, and security. Research data is shared with Federal partners and the finalized studies with the public.

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

No

State the reason why individuals cannot object or why individuals cannot give or withhold their consent.

Individuals will not have an opportunity to consent to specific uses of their PII because any video, still images, and/or radar images of individuals are inadvertently captured during UAS non-law enforcement mission activities or captured in support of authorized law enforcement or national security activities. PII will not be retained, used or disseminated unless there is a legal reporting requirement, retention of the information is necessary to an authorized mission, the information is maintained in a Privacy Act system of records or retention is required by any other applicable law or regulation. Allowing an individual to consent to the collection, use, dissemination, and maintenance of information collected for law enforcement purposes would compromise operations and would interfere with DOI's mission.

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

☐ Privacy Act Statement ☐ Privacy Notice ☒ Other ☐ None

Describe each applicable format.

Notice of the intended collection, uses and sharing of personal information is governed by the Departmental, bureau and office programs that use UAS. Individuals receive notice of information handling practices through this UAS PIA, OAS policy regarding the official use of UAS, and the OAS UAS program website at http://www.doi.gov/aviation/uas_index.cfm. DOI UAS activities are conducted in accordance with Federal UAS policy and DOI OPM-11, DOI Use of Unmanned Aircraft Systems (UAS), which governs the Department's UAS program, including acquisition, training and privacy protections. OPM-11 is updated annually to ensure policy, procedures and protections regarding DOI official use of UAS is current and in alignment with Federal government-wide requirements.

Individuals may also review the IMARS PIA and SORN on the DOI Privacy Program website to learn more about how information is collected, maintained, and shared for law enforcement purposes: https://www.doi.gov/privacy/privacy-program.

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

Data retrieval is specific to the bureau/office program or individual project. It may be retrieved manually or via reports generated automatically. Image data used for general scientific, environmental, or land management purpose does not contain PII so will not be retrieved by name or other unique identifiers. These images may be retrieved by geographical search, mine name search/product type or by permit number, etc.

For data collected or maintained in support of law enforcement efforts that are associated with an incident report or case

file in the DOI law enforcement system, DOI-10, IMARS, data may be retrieved by name, case number, or other identifier related to the case file.

I. Will reports be produced on individuals?

Yes

What will be the use of these reports? Who will have access to them?

Generally, reports generated for data collected through UAS use for mission objectives related to scientific, environmental and land-management applications will not contain specific information about individuals. However, data collected in support of law enforcement efforts may include images or video relating to individuals that may be contained in reports used for official law enforcement purposes by authorized officials.

Section 3. Attributes of System Data

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

Video or images of individuals that is incidentally collected during non-law enforcement natural resources or public land management missions is not verified for accuracy, and in most cases video or image resolution is not sufficient to identify specific individuals. Images or data collected that relates to individuals for an authorized purpose is verified and associated with a case file, and is covered by a system of records for that case file system or law enforcement system after the images are cross referenced to an investigation or case.

B. How will data be checked for completeness?

The video and/or radar images of individuals collected during non-law enforcement natural resources or public land management missions are not checked for completeness because any collection of PII in these instances is inadvertent and is not retained unless the information is determined to be necessary to an authorized mission, is maintained in a system of records covered by the Privacy Act, or is required to be retained by other applicable law or regulation. Video and/or images used for law enforcement purposes are associated with a case file and checked in the law enforcement system or case file system to ensure the information is complete and there is no missing or incomplete data. Law enforcement officers undergo strict training on information handling and sharing procedures.

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

The video and/or radar images of individuals collected during non-law enforcement natural resources or public land management missions are not checked for currency because any collection of PII in these instances is inadvertent and is not retained unless the information is determined to be necessary to an authorized mission, is maintained in a system of records covered by the Privacy Act, or is required to be retained by other applicable law or regulation. Video and/or images used for law enforcement purposes are taken in real time and are associated with a case file, and checked in the law enforcement system or case file system to ensure there are current versions of the videos or images as indicated by the date.

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

UAS program general administrative records are maintained under the Departmental Records Schedule for Administrative records, which was approved by the National Archives and Records Administration (NARA) (DAA-0048-2013-0001). This DRS covers administrative records, routine aircraft operations, logistical support, general maintenance, training, accident reports, and other general management records, and these records have a temporary disposition. Records are cut off at the end of the fiscal year, when files are closed or superseded, then destroyed after the applicable retention period after cut off depending on the type of administrative record. Records on unique or modified aircraft are covered by General Records Schedules (GRS) for Motor Vehicle and Aircraft Maintenance and Operation Records (GRS 10-11a, N1-GRS-04-6, item 3a), and their disposition is permanent. These records are transferred to NARA when they are superseded.

Information collected through UAS for use by bureaus and offices in support of mission requirements is covered by bureau and office records schedules specific to the mission or program area utilizing the UAS. Given the scope of the mission areas supported by UAS, there may be numerous varying records retention schedules as these areas include scientific, environmental and land-management applications, as well as law-enforcement and regulatory efforts. In these cases, data collected is incorporated into the records maintained under approved mission schedules for each bureau and

office program. However, in accordance with Federal policy and DOI OPM-11 on UAS operational activities, information collected by or on behalf of DOI using UAS that may contain PII will not be retained for more than 180 days unless retention of the information is determined to be necessary to an authorized mission, is maintained in a system of records covered by the Privacy Act, or it is required to be retained for a longer period by any other applicable law or regulation. Data retention for records incorporated into a case file or system of records is maintained in accordance with the specific records retention schedule and system of records notice that covers the record.

Law enforcement records are retained and disposed of in accordance with Office of the Secretary Records Schedule 8151, Incident, Management, Analysis and Reporting System, which was approved by NARA (N1-048-09-5), and other NARA approved bureau or office records schedules. The specific record schedule for each type of record is dependent on the subject matter and records series and the needs of the bureau or office program.

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

Temporary records are disposed of in accordance with the applicable records schedule and DOI policy. Approved disposition methods include burning, pulping, shredding, erasing and degaussing in accordance with the applicable records schedule, DOI 384 Departmental Manual 1, and NARA guidelines. Permanent records that are no longer active or needed for agency use are transferred to the National Archives for permanent retention in accordance with NARA guidelines.

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.

The use of UAS and accompanying surveillance technologies presents several privacy concerns and as UAS technology continues to evolve it will be critically important to address any potential implications for the privacy, civil rights, and civil liberties of the public. The UAS systems within DOI at this time contain technology packages that are very similar to what is available to the general public, and include capabilities such as cameras with enhanced visual acuity (optics), image enhancement technology (night vision), and thermal imaging technology capture (infrared), and any new technology or capability will require a re-evaluation of the scope and purpose of the mission and the impacts on privacy. While the current DOI program is based upon mission profiles that are not law enforcement specific beyond providing situational awareness, monitoring and evaluation will be important to recognize missions that have the potential to create privacy concerns. The OAS and UAS Program Manager work closely with Departmental privacy and security officials to ensure DOI UAS activities adhere to Federal requirements and appropriate controls are implemented to protect individual privacy.

One area of concern for privacy is ensuring that DOI's collection and use of data from aerial surveillance remains within the scope of its authorities and responsibilities to manage public lands and waters. An additional privacy concern is the proper handling of any data provided to support law enforcement activities, while continuing to preserve a person's right to privacy. DOI's use of UAS to conduct aerial observations is consistent with DOI's authorities and obligations. There is a minimal risk that a person's privacy might be unintentionally violated when UAS are flying over public lands or waters. The images captured during these non-law enforcement missions are not personally identifiable without further investigative analysis. UAS do not physically intrude upon or disturb private property without permission. Further, the cameras deployed on DOI UAS do not have the capability to see through walls or otherwise collect information regarding what occurs in the interior of a building, nor is that their purpose.

Additionally, UAS present a perceived risk to privacy because some are able to fly for longer hours than manned aircraft and due to the small size and low noise signature of some models, UAS may conduct surveillance undetected. UAS are useful for monitoring remote land areas not accessible by people and where infrastructure is difficult or impossible to build. Also, UAS are operated by personnel on the ground, which allows some UAS to provide long-range surveillance for greater lengths of time than manned aircraft. Because UAS can be small and can operate at very low altitudes, their presence can be concealed allowing UAS to monitor a moving target or a fixed location for relatively longer periods of time without the likelihood of detection. While some UAS can fly for longer periods of time, they are equipped with the same technology to conduct surveillance that is presently deployed on a manned aircraft. Other technologies on the UAS are shared by DOI manned aircraft. Putting these technologies on a UAS only enhances DOI's ability to perform its existing functions at a lower cost and reduced risk to personnel.

To mitigate the risk presented by possible longer sustained surveillance that implicates individual privacy, DOI has implemented strict policies and procedures for mission priorities for UAS operations. DOI UAS activities are conducted in accordance with Federal UAS policy and DOI OPM-11, DOI Use of Unmanned Aircraft Systems (UAS), which may be

viewed at the DOI OAS UAS website: https://www.doi.gov/aviation/uas. OPM-11 addresses the authorized uses of UAS at DOI and includes requirements for acquisition, operations, training, and the protection of privacy and civil liberties. OPM-11 is reviewed and updated annually to ensure policy, procedures and protections regarding DOI official use of UAS is current and in alignment with Federal government-wide requirements. OAS requires operators and UAS program officials to successfully complete training on the proper operation of the recording equipment on the UAS, the handling and transfer of imagery data, and other UAS program requirements.

DOI UAS may only be used in support of an authorized mission or investigation, and the video or other data collected may only be accessed by authorized personnel with an official need to know. DOI-held video or other data is controlled through procedures, chain of custody, and stored in secure locations until it is destroyed. Currently, DOI and FAA have a memorandum of agreement that allows operation of DOI UAS for mission-related purposes, excluding law enforcement and emergency response purposes. This agreement establishes procedures for DOI to provide notice to FAA prior to each official use of UAS. In addition, the FAA requires DOI to construct a Certificate of Authorization (COA), in the instance of deploying a UAS for law enforcement activity or emergency response circumstances, before conducting an operation. Additionally, UAS operators will receive training that includes policy and procedural guidance on individual privacy, civil rights, and civil liberties. DOI requires all personnel to complete annual privacy training, and role-based privacy training as assigned to specific groups, to ensure individual privacy is protected and personal information is collected and maintained only when authorized in accordance with privacy laws and Department policy.

Another privacy concern pertains to the security of the system itself and the potential for hijacking of the unmanned aircraft. DOI has taken several steps to protect UAS against potential hackers or interference. The radio frequency for both wireless uplink control and streaming video downlink is encrypted in accordance with advanced encryption standards to ensure security of the communications. All UAS are controlled and monitored at all times by operators in ground control stations through an encrypted data feed. The ability to interfere with such an encrypted data feed requires disrupting the signal from the ground control station to the UAS, for the purpose of acquiring the data feed or controlling the UAS. In order to protect the airspace, the FAA is notified immediately if a UAS loses its signal through intentional hacking or interference. The FAA is required to be notified within 24 hours for accidents and incidents involving a flyaway, which is an interruption of loss of the control link, or when the pilot is unable to effect control of the aircraft. Loss of link is defined as loss of the command-and-control link contact with the UAS such that the remote pilot can no longer manage the aircraft's flight. Lost link is not considered a fly-away. Furthermore, if lost link occurs, the UAS are pre-programmed to fly to a pre-coordinated point in a remote location to orbit while waiting for the signal to be reestablished or land at a predetermined location.

Individuals are not intentionally monitored during the course of DOI natural resources or land management missions unless it is part of an active criminal investigation. Inadvertent collection of PII is possible during these missions. If any data collected during these missions is forwarded to law enforcement officials relative to possible observed criminal activity, the data will be handled in accordance with appropriate law enforcement policies and stored in the appropriate law enforcement system or case file system. Images collected during non law enforcement natural resources or public land management missions that may contain PII are only retained for over 180 days if the information is determined to be necessary to an authorized mission, is maintained in a system of records covered by the Privacy Act, or is required to be retained by other applicable law or regulation.

If imagery is to be for a law enforcement purpose then the operating bureau or office must conduct training that includes correct techniques to copy recorded evidence from a non-portable hard drive to portable digital media and procedures to ensure that such evidence is not co-mingled with data from other investigations. The training also includes procedures to maintain an adequate chain of custody for all recorded evidence. Each pilot making a recording must ensure that the time and date shown in the original recording is accurate. After a mission is completed, the pilot must ensure that the original record is transferred entirely, in its original format, to portable media. The transferred data must not be edited or altered. The pilot making the recording must label all copies of portable media with the corresponding case number (if available), the date and place of the original recording, and the names of the pilot and aircraft commander. The pilot making the recording must also label, initial, and maintain possession of the evidence until custody is properly transferred to the appropriate designated evidence custodian, law enforcement official or other government official. As with any information associated with a case file, once the images are cross referenced to an investigation or case, they are incorporated into the system of records for that case file system and subject to the retention, access and amendment provisions of that system.

Requests for UAS support are directed to the OAS Director for authorization, and each request follows a standard process to ensure legitimacy, appropriate authority, purpose and uses for the UAS. Additionally, DOI users must

complete UAS training and sign Rules of Behavior before they can utilize UAS or the information obtained from use of UAS. External partners and users must enter into information sharing agreements that apply the same legal and policy requirements to their use of DOI-owned and operated UAS. Once the OAS Director authorizes UAS operations in response to a vetted DOI bureau/office request, the applicable DOI bureau/office assumes responsibility for the proper conduct of the mission and handling and protection of the data obtained through the use of UAS in accordance with all relevant Federal, DOI, and applicable bureau/office policies.

The DOI OAS UAS website at https://www.doi.gov/aviation/uas provides an overview of the DOI UAS Program and contains policies, procedures, and information regarding UAS activities to promote transparency on how DOI uses UAS technology to support its missions. DOI will publish annual reports for public viewing on UAS operations each fiscal year describing the types of missions flown and assistance provided to our partners.

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

The use of UAS significantly expands DOI's ability to obtain remote data critical to fulfilling many mission objectives including scientific, environmental and land-management applications, with less cost, less environmental impact, and enhanced safety. UAS also promotes safety and reduces risks to employees engaging in potentially hazardous operations, particularly for emergency responders for rapid response and situational awareness.

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

No

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

No

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

No

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

New data is not being created. However, video or images of individuals that is incidentally collected during non-law enforcement natural resources or public land management missions is not verified for accuracy, and in most cases video or image resolution is not sufficient to identify specific individuals. Images or data collected that relates to individuals for an authorized purpose is verified and associated with a case file, and is covered by a system of records for that case file system or law enforcement system after the images are cross referenced to an investigation or case. OAS requires operators to successfully complete training on the proper operation of the recording equipment on the UAS, and the handling and transfer of imagery data.

F. Are the data or the processes being consolidated?

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 ☐ Developers ☒ System Administrator

☒ Contractors ☒ Other

Describe

Pilots, operators at ground stations, law enforcement officials, and Federal, State, Tribal, or local partners under a cooperative agreement or during cooperative operations.

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

Requests for UAS support are directed to the Director, OAS, for authorization. Each request follows a standard process to ensure legitimacy, appropriate authority, purpose and uses for the UAS. Additionally, DOI users must complete UAS training and sign Rules of Behavior before they can utilize UAS or the information obtained from use of UAS. External partners and users must enter into information sharing agreements that apply the same legal and policy requirements to their use of DOI-owned and operated UAS. Once the OAS Director authorizes UAS operations in response to a vetted DOI Bureau/Office request, the applicable DOI Bureau/Office assumes responsibility for the proper conduct of the mission and handling of the data obtained through the use of UAS in accordance with all relevant Federal, DOI, and applicable Bureau/Office policies.

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?

Appropriate provisions will be included in DOI contracts to ensure adequate protections in compliance with Federal law, the Presidential Memorandum, and Departmental policy.

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

No

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

No

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

Individuals are not intentionally monitored during the course of DOI natural resources or land management missions unless it is part of an active criminal investigation. Inadvertent collection of PII is possible during these missions. If any data collected during these missions is forwarded to law enforcement officials relative to possible observed criminal activity, the data will be handled in accordance with appropriate law enforcement policies and stored in the appropriate law enforcement system or case file system.

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

Individuals are not intentionally monitored during the course of DOI natural resources or land management missions. Inadvertent collection of images containing PII is possible during these mission related activities as UAS enables DOI to monitor large areas of public lands. Data collected during these missions relative to possible observed criminal activity may be forwarded to law enforcement officials to be handled in accordance with appropriate law enforcement policies and procedures, and stored in the appropriate law enforcement system or case file system in accordance with the Privacy Act.

Images collected during non law enforcement natural resources or public land management missions that may contain PII are only retained for over 180 days if the information is determined to be necessary to an authorized mission, is maintained in a system of records covered by the Privacy Act, or is required to be retained by other applicable law or regulation.

N. How will the PII be secured?

(1) Physical Controls. Indicate all that apply.

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

(2) Technical Controls. Indicate all that apply.

☒ Password	☒ Intrusion Detection System (IDS)
☒ Firewall	☒ Virtual Private Network (VPN)
☒ Encryption	☐ Public Key Infrastructure (PKI) Certificates
☒ User Identification	☒ Personal Identity Verification (PIV) Card
☐ Biometrics	
☒ Other	

Describe

The radio frequency for both wireless uplink control and streaming video downlink is encrypted in accordance with advanced encryption standards to ensure security of the communications. Data obtained from UAS technology are maintained in bureau or office systems by the specific program or office utilizing the UAS in accordance with Federal requirements and DOI policy.

(3) Administrative Controls. Indicate all that apply.

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

Describe

OAS provides UAS training to operators and UAS officials on how to handle information obtained by the UAS, to ensure that privacy, civil rights, and civil liberties are protected related to the collection, use, retention, and dissemination of such information.

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 UAS Program Manager is responsible for issuing appropriate guidance and establishing procedures for the use of UAS to ensure adequate privacy protections are implemented in consultation with the Departmental Privacy Officer. Bureaus and offices are responsible for conducting UAS activities in accordance with Federal regulations and Departmental UAS policy, and developing and implementing procedures for maintaining personal information in their systems of records subject to the provisions of the Privacy Act in such a way to ensure full compliance with the Privacy Act and with related laws, regulations and directives issued by the Department. Program officials who use UAS in support of their program or mission areas are responsible for the proper use and protection of the information collected, and protecting the privacy rights of individuals. Standards for the maintenance of records on individuals are described in the Departmental Privacy Act regulations at 43 CFR part 2, and involve the content of the records, data collection practices, and the use, safeguarding, and disposal of personal information in the records. Privacy Act System Managers are responsible for ensuring records are maintained, used, shared, and protected in accordance with Federal statutes and policies, DOI regulations and privacy policy. Bureau and Office Privacy Officers are responsible for ensuring the protection of individual privacy for their respective bureaus, and for addressing Privacy Act requests for amendment of records and complaints by individuals.

The Department promotes accountability by requiring its personnel to accept responsibility for the actions they undertake and to evaluate the potential consequences of their decisions, and imposes rules of behavior and codes of conduct to guide employees in UAS activities. The Department ensures that personnel are appropriately trained and supervised, and that personnel whose responsibility it is to manage, supervise, maintain, fly, and/or otherwise use UAS meet Departmental training requirements on UAS policy, privacy protections, and information management requirements to ensure information about individuals may only be collected and maintained when authorized, subject to the Privacy Act and related Federal laws and regulations, and DOI privacy policy.

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 UAS Program Manager is responsible for overseeing the DOI UAS program,ensuring compliance with Federal and Departmental UAS policy, and implementing privacy controls to protect individual privacy in consultation with the Departmental Privacy Officer. DOI bureau and office program officials who utilize UAS to collect information in support of their mission areas are responsible for the proper use and protection of that information, as well as for reporting any potential loss or compromise of the information. Privacy Act System Managers are responsible for ensuring records about individuals are maintained, used, shared, and safeguarded in accordance with Federal statutes and policies, DOI regulations and privacy policy, and for protecting PII against compromise, or unauthorized access or disclosure, in accordance with the Privacy Act and DOI privacy policy. These responsibilities are covered in the Department of the Interior Department Manual 383 DM 7. Each bureau and office is responsible for ensuring that all employees with access to a system of records are aware of the requirements of the Privacy Act (5 U.S.C. 552a) and the Departmental Privacy Act regulations (43 CFR part 2) concerning the handling, disclosure, and alteration of such records and the possibility of criminal penalties for improper disclosure. All DOI employees and contractors are responsible for safeguarding privacy, reporting any compromise of PII, and complying with Federal and Departmental privacy requirements.

The UAS Program Manager, bureau and office UAS Program officials, and program managers that utilize UAS technology and data obtained from UAS activities are responsible for ensuring that any loss, compromise, unauthorized access or disclosure of PII is reported to Departmental officials in accordance with Federal requirements as established by DOI privacy incident response policy and procedures. These requirements apply to all DOI employees and contractors.