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: Bureau of Land Management, Office of Law Enforcement & Security, Digital Evidence Management System (BLM OLES DEMS)

Bureau/Office: Bureau of Land Management (BLM)
Date: April 16, 2021
Point of Contact:
Name: Ashanti Murphy-Jones
Title: Acting Associate Privacy Officer
Email: a1jones@blm.gov
Phone: (202) 912-7012
Address: 1849 C Street NW, Washington, D.C., 20240

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:

B. What is the purpose of the system?

The Bureau of Land Management, Office of Law Enforcement & Security, Digital Evidence Management System (BLM OLES DEMS) is an enterprise, commercial-off-the-shelf, end-to-end law enforcement camera and digital evidence management system. Body worn cameras, dash-mounted vehicle cameras, handheld cameras, and closed-circuit

television are camera systems currently used by law enforcement officers in the performance of their duties. Digital evidence can come from several sources and is not limited to body worn cameras. Still images and other digital evidence are also obtained and collected from the public as evidence during an investigation. BLM OLES DEMS will provide an integrated system of cameras, compatible software and mobile applications to enable law enforcement officers to download, catalogue, tag, manage, store, retain and dispose of the digital evidence in a FedRAMP approved, cloud-storage system.

The system includes:

- Collecting and uploading content in any file format, from any device;
- Transferring the data by automatically uploading content from body worn camera devices and hard drives;
- Managing - Keep information organized and tag it with the correct metadata;
- Retrieving - Find evidence quickly with search features;
- Sharing - Grant access to authorized persons, like prosecutors, or share content with a secure link;
- Scalable - Increase storage space as needed;
- Effortlessly tag video with correct metadata;
- Integrating with DOI computer-aided dispatch (CAD) systems and the DOI's law enforcement records management system through automation of the process of tagging videos with complete, correct metadata;
- Ensuring evidence receives the appropriate automatic retention and disposal periods; and
- Redacting data in response to Freedom of Information Act (FOIA) requests for information.

BLM OLES DEMS may use mobile applications designed to upload video, photo, and audio recordings captured on the users' mobile devices (smartphone and tablets) directly into a secure cloud-based metadata storage system. They also allow an agency to register, assign, and reassign BLM OLES DEMS devices and allow a user to wirelessly interact with a camera to view recorded videos, preview live video capture, and apply metadata to video files. Officers using the BLM OLES DEMS may or may not make use of the mobile applications as part of the law enforcement activities. BLM OLES DEMS Mobile applications are only authorized to be installed and utilized on DOI government issued mobile devices used for law enforcement purposes. These devices meet DOI requirements for IT security protection. This PIA also covers the mobile applications listed in question 1.F.

C. What is the legal authority?

- Criminal Justice Information Systems 28 C.F.R. § 20;
- Uniform Federal Crime Reporting Act 28 U.S.C. § 534;
- Intelligence Reform and Terrorism Prevention Act of 2004 (Pub. L. 108–458);
- Homeland Security Act of 2002 (Pub. L. 107–296);
- USA PATRIOT ACT of 2001 (Pub. L. 107–56);

- USA PATRIOT Improvement Act of 2005 (Pub. 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 C.F.R. § 23;
- Computerized Criminal Information Systems DOI DM 446 Chapter 14;
- Records maintained on individuals 5 U.S.C. § 552a (j) (2);
- Tribal Law and Order Act of 2010 (Pub. L. No. 111-211);
- Bureau of Land Management: 43 U.S.C. § 1733 – Enforcement Authority – Federal Land Policy & Management Act of 1976 (a);
- The Wild Free-Roaming Horse and Burro Act (16 U.S.C. § 1331-1340)

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:
UII code: 010-000002500; The System Security and Privacy Plan (SSP) is under development and will be completed as part of the security assessment and authorization process to obtain an Authority to Operate (ATO) this system.

☐ No

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

BLM OLES DEMS is a network of devices and software applications. Below is the "ecosystem" of software and applications that falls within the BLM OLES DEMS security boundary. These software and applications are only uploaded and utilized on government issued devices that meet DOI requirements for IT security protection.

Subsystem Name	Purpose	Contains PII *(Yes/No)*	Describe *If Yes, provide a description.*
Axon View Mobile Application	Axon View is a mobile application for mobile devices (smartphones and tablets) that allows an agency user to wirelessly interact with a camera to view recorded videos, preview live video capture, and apply metadata to video files. It wirelessly connects with a camera to provide instant playback of unfolding events in the field. The user of the application sees what the camera sees.	No	Axon View does not retain PII or video files on the mobile device, but only views video stored on a paired camera. It cannot transfer, delete or alter original video files that are stored on a camera. Physical access to the camera is required to initiate pairing with Axon View and requires persistent close proximity to a camera to provide functionality.
Axon Capture Mobile Application	Axon Capture is a mobile application for mobile devices (smartphones) that allows an agency user to upload video, photo, and audio recordings captured on the users' smartphone directly to Evidence.com, the secure cloud-based metadata storage system. Rather than utilizing a separate recording device, such as a body-worn camera or in-vehicle camera, Axon Capture uses the recording capabilities of the smartphone. The user must be signed into an agency prior to uploading the digital data to their Evidence.com tenant. The evidence will be stored in the Axon Capture application before being uploaded to Evidence.com. Once the user has the feature enabled in their Axon Capture settings, the user can import video, photo, and audio data from their smartphone digital library or the default repository on their device to Axon Capture, where it can then be uploaded into the user's Evidence.com tenant. The Capture application allows	Yes	The Axon Capture application allows the user to capture, store, process, and upload video/audio data, which may contain PII, from the user's government issued mobile device. Rather than use a separate camera device, such as a body worn camera or in-vehicle camera, to capture digital data, the user's government issued mobile device is the camera.

Subsystem Name	Purpose	Contains PII *(Yes/No)*	Describe *If Yes, provide a description.*
	the user to add tags, titles, or GPS coordinates to any recording prior to uploading the data directly into Evidence.com.		
Axon Device Manager Mobile Application	Axon Device Manager (ADM) is a mobile application for mobile devices (smartphones and tablets) that allows an agency user to register, assign, and reassign Axon devices. In order to use the ADM application, the role of the user in Evidence.com must have a Device Administration permission, or Conducted Electrical Weapons (CEW) Administration permission, or both permissions set to 'Allowed' to use the ADM application. Though ADM is the preferred method for registering, assigning, and reassigning Axon devices, devices can also be registered, assigned, and reassigned directly in Evidence.com. This will be used by a very limited sub-set of users who are System Administrators or have elevated privileges to provision hardware devices.	No	ADM does not create, collect, use, process, maintain or disseminate PII or specific information about individuals. The ADM application is used to register, assign, or reassign Axon devices which do collect, use, process, maintain, and disseminate PII, but does not itself collect, process, store, or interface with any of this collected data.
Axon Aware Manager Mobile Application	The Axon Aware is a mobile application for mobile devices (smartphones and tablets) and is a secure and powerful tool that provides additional flexibility for agencies using Axon Aware. It boosts situational awareness by notifying commanders in real-time when urgent events occur. With the Axon Aware mobile app commanders and supervisors can see the location of officers and view livestream broadcasts from an officer's	No	Axon Aware does not retain PII or video files on the mobile device, but only views video stored on a paired camera. It cannot transfer, delete or alter original video files that are stored on a camera. Physical access to the camera is required to initiate pairing with Axon

Subsystem Name	Purpose	Contains PII *(Yes/No)*	Describe *If Yes, provide a description.*
	body camera. All of this happens seamlessly and instantly with just a few clicks on their mobile device.		Aware and requires persistent close proximity to a camera to provide functionality.
Axon Evidence Sync Desktop Application	Evidence Sync is a desktop-based application that enables management of evidence from one location and access it anytime, anywhere. New and old sources – from Axon devices to SD cards and CDs that all files will sync. With Evidence Sync, hard drives and desktop folders can be scheduled to sync automatically and continue to upload even after logging out. That means at the end of a shift, users must sign off and sign out. Evidence Sync will finish uploads in the background.	Yes	Evidence Sync does not retain PII or video files on the desktop device but does temporarily store it for transfer to the cloud. It cannot alter original video files that are stored on a camera.
Axon Evidence Upload XT Desktop Application	Evidence Upload XT is a Windows-based desktop application that enables users to easily upload non-Axon generated digital evidence to their agency's Evidence.com account. The Evidence Upload XT settings page allows administrators to configure the bandwidth setting options for Evidence Upload XT.	Yes	The Axon Evidence Upload XT application allows the user process and upload video/audio data, which may contain PII, from a variety of recording devices and/or digital media. Rather than use a separate camera device, such as a body worn camera or in-vehicle camera, to capture digital data, evidentiary data can be obtained from a variety of sources.
Axon View XL Desktop Application	The Axon View XL application is used to control and support Axon Fleet cameras. It is designed for use with a mobile data terminal (MDT) or mobile digital computer (MDC) within a police vehicle. The Axon View XL application	Yes	The Axon View XL application allows the user to capture, store, process, add meta-data and upload video/audio data, which may contain PII, from the user's government issued

Subsystem Name	Purpose	Contains PII *(Yes/No)*	Describe *If Yes, provide a description.*
	is used to control and support Axon Fleet cameras. Axon View XL lets users start and stop camera recording, play recorded videos, and add metadata to videos. Additionally, Axon View XL also supports user sign-in and wireless offloading of Axon Fleet camera videos. Axon View XL requires that the Axon provided Bluetooth low-energy (BLE) dongle be inserted into the MDT/MDC USB port in order to communicate with the cameras. If the dongle is missing or not correctly inserted an error message is shown. Insert the dongle or ensure the dongle is securely seated in the MDT USB port to continue. Axon View XL supports the ability for two officers to be signed into the same View XL session. Video evidence that is recorded when two officers are signed in will have dual ownership when uploaded to Axon Evidence. This allows both officers to access evidence that was created while both were signed into View XL. Additionally, this option provides officers with the ability to shift which body camera is active in View XL and which body camera evidence can be reviewed, tagged, and uploaded.		Axon Fleet in vehicle camera and Axon Body Worn Camera.
Axon Report Fetcher Local Server Application	Axon Report Fetcher is a very limited scope executable application with use for Application Programming Interface (API) integration to extract JSON files for audit automation. The "fetcher" retrieves database information from the Axon Evidence.Com FedRAMP cloud application and extracts it to a "local	Yes	The Axon Report Fetcher application retrieves data from the FedRAMP cloud and transfers it to a local server. This data contains all types of data maintained

Subsystem Name	Purpose	Contains PII *(Yes/No)*	Describe *If Yes, provide a description.*
	server" for analysis and ingestion into a tool which allows for searching, monitoring, and analyzing machine-generated data via an interface, such as Splunk. This application will only be used by Administrators and Information Technology Security Specialists and Risk Managers. This software is only available directly from the manufacturer to existing customers.		within the system and may contain PII, such as name, Date of Birth, Individual name, username, email address, phone number, etc.

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)*

The records in this system are covered under DOI-10, Incident Management, Analysis and Reporting System (IMARS), SORN which can be found at https://www.doi.gov/privacy/doi-notices.

☐ No

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

☐ Yes:
☒ 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
☒ 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
☒ Other: *Specify the PII collected.*

Digital evidence collected as part of the BLM OLES DEMS will be in the form of video recordings, audio recordings, and photographs that have been captured in the normal course of law enforcement duties. Due to the nature of these recordings from in-person contacts with individuals and groups, it is both possible and probable that all types of PII will be captured and collected, including License Plate Numbers; Vehicle Identification Number; Passport Numbers; Alien Registration Numbers; FBI Universal Control Numbers (UCN); State Identification Numbers (SID); Work Addresses; Other Contact Information; location or GPS data; Tribal Enrollment Data; Work History; Educational History; Fingerprints; Hair and Eye Color and any other Physical or Distinguishing Attributes of an Individual; Arrest and incarceration records; Prior Contacts with Law Enforcement; Criminal History

Record Information (CHRI); Photographs; Audio Recordings; and Video Recordings. The system contains images and videos collected from audio/visual recording devices such as surveillance cameras, closed circuit television located at DOI 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) or a DEMS mobile application authorized for law enforcement operations.

Individual names; usernames; passwords; email addresses; phone numbers and Single-Sign On (SSO) information is collected as part of the system account management process.

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: Open-Source Data Collection, Internet, Social Media, etc.

PII is captured on law enforcement camera systems when the recording device is activated during law enforcement citizen interactions. Data recorded is directly related to law enforcement activities and emergency response, and may include video images of people, driver licenses, personal information verbally requested for the purposes of violation notices and/or arrests during a lawful contact, and criminal history information provided over the radio by the dispatch communications center. Information may also be obtained from publicly available websites, witnesses, concerned citizens, and the general public providing images and recordings from their personally owned devices.

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

The BLM OLES DEMS is capable of sharing information between agencies using a similar DEMS system if they are both on the Evidence.Com platform and the agencies allow and authorize sharing functionality. The sharing permissions are specific and granular, and permissions must be enabled for each piece of evidence being shared and each specific individual it is being shared with. The type of sharing allowed or prohibited must be indicated, such as "view," "download," "view audit trail," "add notes," "reshare allowed," etc. The duration of sharing must also be set in days, after which sharing will automatically be disabled. Digital evidence from BLM OLES DEMS will be uploaded to the DOI's law enforcement records management system, to meet law enforcement business needs for investigations and case management. At this time there is not an automated sharing process between BLM OLES DEMS and DOI's law enforcement records management system and all transactions will be completed manually. The DOI is exploring future automated integration in their acquisition of future law enforcement records management products.

☐ Other: *Describe*

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

Data collected in the BLM OLES DEMS system is used to record and document information related to public safety events, incidents and/or investigations on land/areas governed by the DOI, as well as tribal lands, and land/areas governed by the U.S. Department of Agriculture (USDA), Forest Service. Data is held in a database repository controlled and maintained by authorized personnel. The information collected, including audio, video and photos, is considered "digital evidence" and will be used in furtherance of investigations and court proceedings. The PII collected through this "digital evidence" will be used to identify suspects, witnesses, victims, officers, investigators and other involved parties, and will be used to verify the identity of individuals through validation with other external records systems and databases. PII is also used to obtain individuals' criminal activity and/or involvement in previous events, incidents and/or investigations from internal and external law enforcement systems for the purposes of identifying past criminal behavior.

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

☒ Within the Bureau/Office:

PII is shared within the BLM for investigation, prosecution, apprehension, recordkeeping, and possible arrest and/or conviction of crimes committed on BLM managed lands and/or against BLM personnel.

☒ Other Bureaus/Offices:

PII is shared with DOI bureaus and offices for investigation, prosecution, apprehension, recordkeeping, and possible arrest and/or conviction of crimes committed on DOI and Tribal properties and/or against DOI and/or Tribal Members or employees.

☒ Other Federal Agencies:

PII is shared with other Law Enforcement agencies for investigation, prosecution, apprehension, recordkeeping, and possible arrest and/or conviction of crimes committed on DOI properties. Information may also be shared between Law Enforcement and other Federal agencies. Information from this system is primarily shared with the USDA Forest Service, the United States Department of Homeland Security and its subordinate agencies, and the United States Department of Justice and its subordinate agencies. The purpose of sharing data with other Federal agencies is to increase efficiency and probability of success of enforcement and/or investigative actions and/or prosecution by cooperating agencies. For example, during an arson, drug smuggling, or other investigation information may be requested from this system that meets the parameters of their investigation, such as whether bureaus had any law enforcement contact with a specific individual(s). If information is available and relevant, it would be shared with the requesting agency to assist in their investigation. If no relevant information were available, nothing would be shared. Digital evidence, including PII, will be routinely shared with the Executive Office of the United States Attorneys (EOUSA) for evidentiary review by prosecutors. PII is shared only when necessary, which means only when the receiving agency has a lawful purpose and a bona fide need to know, as authorized and outlined in the routine uses section of the DOI-10, Incident Management, Analysis and Reporting System (IMARS), SORN which may be viewed at https://www.doi.gov/privacy/doi-notices

☒ Tribal, State or Local Agencies:

PII is shared with other Law Enforcement agencies for investigation, prosecution, apprehension, recordkeeping, and possible arrest and/or conviction of crimes committed on DOI properties, other properties and/or against DOI personnel and/or other personnel. Information may also be shared between Tribal, State and Local Law Enforcement Agencies, including prosecutors within these agencies. PII is shared only when necessary, which means only when the receiving agency has a lawful purpose and a bona fide need to know, as authorized and outlined in the routine uses section of the DOI-10, Incident Management, Analysis and Reporting System (IMARS), SORN which may be viewed at https://www.doi.gov/privacy/doi-notices

☒ Contractor:

PII is shared with DOI contractors who facilitate technical operation of this “system” including maintenance, development, data validation, accuracy checking, archiving and purging. These contractors conduct work on behalf of DOI and are authorized to have access to the information / data maintained in the system. Due to the sensitive nature of the data and the PII stored in this system, these contractors receive specific training courses

designed to prevent unauthorized access to and or improper use of this data. These contractors are also required to sign Federal Bureau of Investigation, Criminal Justice Information System, Security Addendums acknowledging the sensitivity of this information, the risks and responsibilities associated with accessing this data and the potential criminal and/or civil penalties associated with unauthorized access and/or improper use.

☒Other Third-Party Sources:

Information that may contain PII may be shared through an agency public disclosure and release process after an incident and/or through the official Freedom of Information Act process. This would be based solely on the need to release information and would done in compliance with law, policy, and process. Efforts would focus on not releasing any PII if possible, however, it is difficult to release an image or a video without exposing the identity of a person. The purpose and benefit of releasing this type of information will always be weighed against the rights of individuals as compared to public benefit.

PII is also 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 DOI-10, Incident Management, Analysis and Reporting System (IMARS), SORN which may be viewed at https://www.doi.gov/privacy/doi-notices

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

☒ Yes:

Individual members of the public have the opportunity/right to decline to provide information where providing information is voluntary and are informed of this right by officers or agency representatives verbally and/or in writing. If the individuals ask how their information will be used, it is explained to them by the officers. Often individuals will call or present in person to report crimes or incidents, in these situations they are categorized as a “reporting party” and/or “complainant” and they are routinely asked for PII to identify them and for the agency to be able to re-contact them. In this situation providing this information is voluntary. If the individual asks if they must provide the information, they are verbally informed they are not required or obligated to provide this information. If the individual asks to remain anonymous, their request is respected, and the agency / bureau is still typically able to complete its mission successfully. Routinely individuals will be contacted in the field by officers or investigators to provide supporting information, testimony and/or evidence, in these situations they are categorized as a “witness” and/or “other” and they are routinely asked for PII to identify them and for the agency to be able to re-contact them.

The primary use of this system and the information is related to "in-person" field contacts of suspects / criminal violators by law enforcement officers. In this situation individuals are detained for the purposes of identification and investigation related to an event and are not able to decline to provide their identifying information. If individuals do not provide the requested information, officers will follow protocol to address the situation. Law enforcement officials may also use photographs, biometrics, or other means to identify individuals involved in events or incidents.

Individuals in video/audio recordings will not have the opportunity to consent to the collection or use of the recording of their images or activities. Some DOI controlled areas may have signs posted that inform individuals of surveillance activities, but in many cases, notice may not be provided, or consent obtained for audio or images captured during law enforcement operations or activities.

☐ No:

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

☒ Privacy Act Statement:

A Privacy Act Statement will be provided verbally by officers upon request by individuals.

☒ Privacy Notice:

Notice is provided through the publication of this PIA and the DOI-10, Incident Management, Analysis and Reporting System (IMARS), SORN, which is available on the DOI SORN website at https://www.doi.gov/privacy/doi-notices

Authorized users are provided notification when downloading and installing authorized mobile applications. There is an "APP Privacy" notification which provides detailed information regarding what data is used by the application and how it will or will not be used related to the user. Information is provided under the headings of "Data Used to Track You", "Data Linked to You", and "Data Not Linked to You." There are also links provided to the global privacy of the vendor which can be easily referenced.

☒ Other:

In some cases, such as for use of audio and visual recordings, individuals who enter on Federal properties and public areas do not have a reasonable expectation of privacy. Some DOI controlled areas may have signs posted informing individuals of surveillance activities, but in many cases, notice may not be provided, or consent obtained for audio, video or images captured during law enforcement activities.

BLM may deny a request or procedural benefits pursuant to 43 C.F.R. § 2.23.

DOI has also exempted certain law enforcement records in IMARS from one or more provisions of the Privacy Act under 5 U.S.C. 552a(j)(2) and (k)(2), in order to preclude an individual subject's access to and amendment of information or records related to or in support of an investigation.

☐ None

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 through manual and automated queries of the BLM OLES DEMS. Specific retrieval identifiers, including event / case / ID number, location, date, officer number, name, camera serial number, categories and tags are used, and the system uses keyword searches to search by any and all of the identifiers listed in Section 2A of this PIA.

I. Will reports be produced on individuals?

☒Yes:

Reports will be produced on individuals who are users of the system, e.g., a "user report" on agency employees. The reports will be to count quantity and category of evidence for each user and data utilization monitoring. These PII in these reports will be limited to employee name, email address and employee number.

Reports may be produced on individuals who are subjects of an investigation, through the use of "tagging" a particular piece of evidence with a subject name or partial name. The PII in these reports would be limited to the tags used by the evidence owner and would typically be limited to full name or last name only.

☐ No

Section 3. Attributes of System Data

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

BLM OLES DEMS provides basic accuracy checking. The individual collecting the data will verify the accuracy of data collected per defined policy and procedures defined by each participating organization. Supervisors will also review data for accuracy through an established Quality Assurance Program and review process. The information stored in BLM OLES DEMS is limited to video, photo, and audio recordings, accuracy verification of data would be limited to visual or auditory review of the evidence. There are no database fields in BLM OLES DEMS which are specifically intended for storing PII data about an individual. There are, however, database fields which could inadvertently have PII put into them such as the ID, Title and Tag fields. The BLM OLES Policy for system use instructs

users to not input PII into these fields. This policy is reinforced through user training. The bureau Technology Administrator / System Administrator will also routinely review and audit data for accuracy, completeness and currency.

DOI is committed to protecting the privacy, civil liberties and other legal rights of the American people to the greatest extent possible consistent with the DOI mission and operational requirements. DOI fulfills this responsibility through policy, monitoring, training, and oversight of the Department's privacy and civil liberties operations and participation in the information sharing environment (ISE). DOI provides redress in a manner that is compatible with legal authorities and mission requirements to individuals whose privacy, civil rights or civil liberties may have been affected in the ISE, which includes complaints related to privacy, civil rights and civil liberties protected by the U.S. Constitution or other laws, and complaints alleging racial, ethnic, or religious profiling, or retention of information that has been expunged or determined to have been illegally collected. Redress inquiries are investigated, and erroneous information or deficiencies are corrected to ensure data integrity and protections for individual privacy, civil rights and civil liberties. DOI procedures for complaints or requests to amend records that implicate protected information are outlined in the DOI Privacy Act regulations at 43 CFR 2.246, in accordance with the Privacy Act of 1974, 5 U.S.C. § 552a, and the DOI ISE Privacy Policy. Individuals may also submit a complaint or a request to correct erroneous information in writing to the DOI ISE Privacy Official. To see the DOI Privacy Policy for the ISE or for additional information, visit the DOI Privacy and Civil Liberties website at https://www.doi.gov/privacy/privacy-civil-liberties.

B. How will data be checked for completeness?

The system provides basic completeness checking on individual files. The individual collecting the data will verify the completeness of data collected per defined policy and procedures defined by each participating organization. Supervisors will also review data for completeness through an established Quality Assurance Program and review process. The information stored in BLM OLES DEMS is limited to video, photo, and audio recordings, completeness of data would be limited to visual or auditory review of the evidence. The bureau Technology Administrator / System Administrator will also routinely review data for accuracy, completeness and currency.

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

Individual BLM OLES DEMS users, including supervisors, are responsible for ensuring the data is current. Law Enforcement Officers ensure information is current during upload and review of evidence files. Users may review evidence accessible to their profile at any time. The bureau Technology / System Administrator will also routinely review data for accuracy, completeness and currency.

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

Video records are managed in accordance with DAA-0048-2015-0002-0001, Routine Surveillance Recordings, which provides that recordings of a non-evidentiary value are temporary and will be destroyed after a period of time. The BLM Records Officer issued a Standing Retention Extension Authorization pursuant to the authority of BLM MS-1270 §2.2d, allowing for the retention of non-evidentiary recordings for up to 6 months. Videos, photos or files with an evidentiary value which may be associated with criminal incidents will be maintained as evidence while the case is open and may be transferred to DOI's law enforcement records management system, and will be maintained in accordance with the incident's disposition schedule.

System user records for BLM OLES DEMS are managed in accordance with DAA-0048-2013-0001-0013, System Maintenance and Use, which contains electronic files and hard copy printouts created to monitor system usage, including, but not limited to, log-in files, password files, audit trail files, system usage files, and cost-back files used to assess charges for system use. These records are temporary and will be destroyed no later than 3 years after cutoff when the records are no longer needed for administrative, legal, audit, or other operational purposes.

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

All data in the BLM OLES DEMS system is electronic and has a temporary disposition. Approved disposition methods are erasing for electronic records, in accordance with NARA guidelines and DOI policy. Archival and disposition of records will be accomplished within the automated records retention and disposal functions built in the system and procedures will follow applicable guidance by NARA, applicable legislation such as the Federal Records Act, and Departmental guidance. BLM OLES DEMS uses the "Categories" feature to retain or dispose of records and data based on the agency ruleset established for the "Categories" as set by the Technology / System Administrator.

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 is a risk to the privacy of individuals in BLM OLES DEMS due to the amount of sensitive PII maintained for law enforcement incidents and investigations. The risks are mitigated by controls implemented to limit unauthorized exposure of PII.

There is a risk of unauthorized access to the system or data, inappropriate use, or disclosure of information to unauthorized recipients. Only authorized personnel with proper credentials can access the records in the system. DOI requires two-factor authentication for network and system access; system access is based on least privilege access and role-based access controls; access control lists were created and segmented; users cannot view information for other users unless specifically authorized. The system has been designed and built, in compliance with NIST Special Publication (SP) 800-53, Security and Privacy

Controls for Federal Information Systems and Organizations. A Security and Privacy Assessment & Authorization has been conducted on the system to verify, validate and monitor compliance of this system.

Privacy risks exist with authorized data sharing with other law enforcement organizations. Risks may include but are not limited to data integrity, loss of data and data confidentiality for data shared and controlled by other organizations. A Memorandum of Understanding (MOU) addressing the information sharing environment will be established with agencies and organizations to ensure adequate controls are in place to protect privacy. Some examples of these controls include those listed above as well as the following:

- MOUs established between Agencies defining system access rules and policies
- Limiting information at the source (connection) deployed to outside agencies
- Utilizing encryption on data transmission and data at rest
- Utilizing Secure File Transfer Protocols for transmission of information
- Security of systems receiving information shared
- Access restrictions to authorized officials
- Authorized use of information shared
- Limits on uses and additional sharing
- Retention periods and authorized destruction or return of information shared

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 will be worn by law enforcement officials, placed on the dashboard of law enforcement vehicles, or used by individual law enforcement officials on properties and locations within the jurisdiction of the DOI and cooperating agencies, including Federal facilities, national monuments, National Parks, tribal lands, and public lands to include buildings, housing units, roadways, trails, and bridges/tunnels, and law enforcement offices and jail units; National Wildlife Refuges; national dams and hydroelectric power plants.

These devices will 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 court proceedings.

Some privacy concerns are that devices may collect more information than 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 respond to unlawful activities or support investigations and prosecutions will be retained for use, all other video feed not required for retention will be automatically disposed of per records disposal 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.

Strict privacy controls are utilized to protect individual privacy, including limiting access to images or video feed that identifies individuals or to specific events or investigations that are linked to individuals, to authorized users and law enforcement officials, establishing controls on the retention of images and video feeds to the approved period necessary for law enforcement purposes in accordance with approved records retention schedules, restricting the maintenance of images or video feeds not necessary for retention to the minimum necessary in accordance with the DRS/GRS/BLM Combined Records Schedules for routine surveillance motion picture and video recordings; and ensuring proper disposal at the end of the retention period; establishing specific use policy and rules of behavior for the use of these audio/visual recording devices.

There is a risk that information may be used outside the scope of the purpose for which it was collected. Law enforcement personnel with access to recorded material and digital evidence will be subject to strict DOI policy, bureau policy, and Privacy Act standards. BLM employees and contractors must take privacy, security and records management training prior to being granted access to BLM information and information systems, and annually thereafter. Personnel with significant privacy responsibilities, such as law enforcement personnel, must also take role-based privacy training initially and annually, to ensure an understanding of the responsibility to protect privacy. Failure to protect PII captured in digital evidence, to include the mishandling or misuse of this PII may result in criminal, civil and administrative penalties.

The BLM OLES DEMS is undergoing a formal Assessment and Authorization and is anticipating an Authority to Operate in accordance with FISMA and NIST standards. This system is rated as FISMA moderate based upon the type of data, and it requires strict security and privacy controls to protect the confidentiality, integrity, and availability of the sensitive PII contained in the system.

The use of DOI IT systems is conducted in accordance with the appropriate DOI use policy. IT systems, in accordance with applicable DOI guidance, will maintain an audit trail of

activity sufficient to reconstruct security relevant events. The audit trail will include the identity of each entity accessing the system; time and date of access (including activities performed using a system administrator's identification); and activities that could modify, bypass, or negate the system's security controls. Audit logs are reviewed on a regular, periodic basis and any suspected attempts of unauthorized access or scanning of the system are reported to IT Security. All access is controlled by authentication methods to validate the authorized user. DOI employees and contractors are required to complete security and privacy awareness training, and DOI personnel authorized to manage, use, or operate the system information are required to take additional role-based training. All employees must agree to DOI Rules of Behavior before being allowed to access the DOI network or any information systems. A general warning banner is displayed upon first logging into the DOI network that informs users that misuse of any system may subject employees to penalties.

There is a risk that data may not be appropriate to store in a cloud service provider's system, or that the vendor may not handle or store information appropriately according to DOI policy. The data collected by law enforcement cameras and uploaded into the evidence management system will be considered sensitive and will contain PII. The provider will implement protections and controls to restrict access to unauthorized parties, as will be required to attain the necessary FedRAMP Authority to Operate (ATO). The provider will be required to submit to additional security accreditation to attain the DOI ATO to ensure the vendor's system handles and stores sensitive information in accordance with Federal and DOI privacy and security standards.

There is a risk to the privacy of individuals with the use of the mobile applications due to the nature of law enforcement interactions with the public and the amount of PII that the mobile applications can access for viewing, processing and storage from videos, photos, audio, and metadata such as GPS data. There is a risk to the privacy of authorized users of the mobile applications due to the GPS features used from the mobile device by the mobile application to record location information. This risk exists while the applications are in use and also when the applications are not in use due to GPS background tracking. The mobile devices use a combination of technical and operational controls to mitigate the privacy risks such as government approved encryption for storage, least privileges for authorized users of the system, and persistent close proximity to a camera for functionality. The risk of GPS background tracking can be mitigated by turning this function off when the applications are not in use. In addition, mobile applications are only authorized to be installed and used on authorized government issued mobile devices which meet DOI requirements for IT security protection. Authorized users are notified of potential privacy implications when downloading and installing authorized mobile applications. There is an "APP Privacy" notification which provides detailed information regarding what data is used by the application and how it will or will not be used related to the user. Information is provided under the headings of "Data Used to Track You", "Data Linked to You", and "Data Not Linked to You." There are also links provided to the global privacy of the vendor which can be easily referenced.

There is a risk that individuals may not know how to seek redress or correction of their records. Individuals seeking redress may submit requests for correction through established procedures outlined in DOI Privacy Act regulations at 43 CFR 2.246 and in the Contesting Records Procedures section of the DOI-10 SORN. The DOI Privacy and Civil Liberties web page at https://www.doi.gov/privacy/privacy-civil-liberties also provides information on how individuals may submit a complaint or a request to correct erroneous information. However, DOI has exempted certain law enforcement records from one or more provisions of the Privacy Act under 5 U.S.C. 552a(j)(2) and (k)(2), in order to preclude an individual subject's access to and amendment of information or records related to or in support of an investigation.

There is a risk that the system may collect, store or share more information than necessary, or the information will be maintained longer than necessary to accomplish a legitimate purpose or in accordance with an approved records retention schedule. Additionally, controls are established in accordance with approved records retention schedules to ensure retention of images and video feeds does not exceed approved periods necessary for law enforcement purposes. DOI restricts the maintenance of images or video feeds not necessary for retention to the minimum necessary (6 months) in accordance with approved records retention schedules for routine surveillance motion picture and video recordings, as extended by the BLM Bureau Records Officer (BRO). The DOI policy and records retention schedules dictate proper disposal of recordings at the end of the retention period and establishes specific policy and rules of behavior for the use of these audio/visual recording devices. Video records are managed in accordance with DAA-0048-2015-0002-0001, Routine Surveillance Recordings, only data with evidentiary relevance will be uploaded into the DOI's law enforcement records management system and retained beyond 6 months. This evidentiary data will be maintained according to the incident's disposition schedule. Video and audio recordings of non-evidentiary value is transitory and will be destroyed after 6 months in accordance with approved records retention schedules for routine surveillance motion picture and video recordings, as extended by the BLM BRO.

There is risk that data from different sources may be aggregated and may provide more information about an individual. This data may become outdated or inaccurate. This system supports law enforcement activities. Due to the nature of law enforcement operations and investigations, data collected about individuals from sources may be aggregated during the course of an investigation. Some mitigation occurs at the time of entry through data validation. Records are disposed based upon the records management schedule. Law enforcement records are created based upon the available information at the time, which may not be complete and precise. Through the course of an investigation additional records are created. The judicial process requires the law enforcement bureau/agency to provide records at the direction of a court and redress or correction of the records can be available through these proceedings (for example discovery, depositions, trial). Records are subject to release through the Freedom of Information Act. Supplemental reports can be added to the record.

There is a risk related to external sharing of data with other Federal, state, Tribal, local, international law enforcement organizations and sharing incorrect, inaccurate or outdated

records misidentification. The system incorporates secure communication using Transport Layer Security (TLS) for all transmission of data to the internal repository as well as external agency repositories. Interconnection agreements are established through DOI's law enforcement records management system and enable bureaus to share authorized data with other Bureaus and other law enforcement organizations. The service agreements ensure the proper documentation of the technical requirements for connectivity and compliance with secure communications for Federal Information Systems in accordance with NIST SP 800-47 "Security Guide for Interconnecting Information Technology Systems." In addition, a continuous monitoring program is in place through boundary protection mechanisms as well as the data repository hosting facility.

There is a risk that individuals may not have notice regarding the collection of information, the purposes for collection or how the information will be used. Notice is provided through the publication of this privacy impact assessment, the IMARS privacy impact assessment, published IMARS SORN, posted signs for areas that use CCTV, and the CCTV Policy Statements posted on agency websites. The body-worn cameras are worn openly on the officer's uniform. Case law has established that an in-vehicle camera is in a public area where there is no reasonable expectation of privacy and does not violate the law. No law or DOI policy requires a notification to the public of officers recording video in public spaces while performing their law enforcement duties.

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:

The BLM OLES DEMS was developed with the purpose of collecting and storing PII to support and enhance the Law Enforcement mission of the BLM, DOI and cooperating agencies. The use of the system and the data is both relevant to the mission and necessary for the accomplishment of the mission.

☐ No

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

☒ Yes:

This system is associated with records in DOI's law enforcement records management system, and/or computer aided dispatch systems (CAD). Data in the DOI's law enforcement records management system and CAD may be obtained from multiple sources instead of the individual. There is risk that data from different sources may be aggregated

and may provide more information about an individual. This data may become outdated or inaccurate. Mitigation occurs at the time of entry through data validation. Records are disposed based upon the records management schedule.

☐ No

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

☒ Yes:

Recorded data collected in support of law enforcement efforts may include video relating to individuals that are contained in incident reports and used for official purposes. Those case files are in DOI's law enforcement records management system and are associated with individuals. Digital content is tagged and associated with incidents that are associated with individuals.

☐ No

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

☒ Yes:

Digital evidence (images) could be used to assist law enforcement with identifying individuals during investigations and prosecutions.

☐ No

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

Law Enforcement Officers and their supervisors are responsible for the relevance and accuracy of the data. Supervisors will also review data for accuracy and completeness during the investigation process, which may include subject or witness interviews and verifying information with other law enforcement agencies and organizations.

F. Are the data or the processes being consolidated?

☒ Yes, data is being consolidated.

Criminal Justice and open-source data in the form of photos, videos and audio containing information on individuals related to incidents and/or events is obtained and consolidated from government and law enforcement organizations and private citizens. Methods used to limit exposure of PII:

- Role-based access controls for authorized personnel with proper DOI credentials

- Least privilege access
- 2-factor authentication into system
- Users cannot view information for other users unless specifically authorized
- Access Control Lists
- MOUs established between Agencies defining system access rules and policies
- Limiting information at the source (connection) deployed to outside agencies
- Utilizing encryption on data transmission and data at rest
- Utilizing Encryption Protocols for hardware-to-hardware handshake
- FedRAMP approved, cloud-storage system

☐ Yes, processes are 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
☒ 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?

Access Requests for users are initiated by authorized bureau/office personnel. A representative will evaluate the request and follow procedures to determine and grant individuals access to the system and data. Least privileges determine that only the minimum levels of access to perform job functions are granted to users based on the users' job requirements. Role based security further limits access to system resources and data based on the users' role in the system.

Access to the BLM OLES DEMS requires an active DOI email account. Law enforcement officials require supervisor authorization to establish user accounts to access the system. Users will not have access to all data, they will have access to the data required to perform their duties based on their roles. System administrators will assign levels of access. BLM OLES DEMS supports law enforcement activities at DOI and shares PII with other Law Enforcement agencies as part of the information sharing environment, for the purpose of investigation, apprehension, recordkeeping, and arrest and/or conviction for crimes committed on DOI lands and/or against DOI personnel. DOI establishes information sharing agreements with partners for any sharing outside of DOI. Information from BLM OLES DEMS may be associated with an event or incident in DOI's law enforcement records management system and shared with DOI bureaus and offices and other law

enforcement agencies through Interconnection Security Agreements, Memorandums of Understanding, or other information sharing agreement as part of the information sharing environment. The authorized sharing of information in support of law enforcement activities is described in the routine uses published in the DOI-10, Incident Management, Analysis and Reporting System (IMARS), SORN which may be viewed at https://www.doi.gov/privacy/doi-notices.

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.

The contractor / vendor who provides the system to DOI also designed and developed the system for BLM. The contractor / vendor and the system have been FedRAMP Authorized by the Joint Authorization Board as a Government Community Cloud Deployment Model at Moderate Impact Level. Privacy Act Clauses were included in the contract between the contractor / vendor and DOI and BLM.

☐ 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.

The purpose of BLM OLES DEMS is to provide surveillance in support of law enforcement operation, investigations and prosecutions. The nature of the system will include monitoring individuals as it provides law enforcement officials mobile video recording capability to document officer-citizen encounters while engaged in patrol functions, which are used in law enforcement activities on lands/areas governed by the DOI as well as tribal lands. The content within the system can provide the capability to identify and locate individuals. The data collected may include physical attributes of an individual, personal and professional address, telephone, any associated information, and other PII listed in Section 2.A.

The BLM OLES DEMS provides the capability to identify, locate, monitor and audit individuals based on a variety of criteria, including individual names; usernames; passwords; email addresses; phone numbers and Single-Sign On (SSO) information and Internet Protocol (IP) Address. The BLM OLES DEMS has robust auditing and security

features and reports capable of tracking and monitoring nearly every user action and transaction within the system. Since the nature of the system is housing "digital evidence," and the evidence needs to be "admissible" in legal proceedings. the BLM OLES DEMS creates reports and audit logs including username, time and date of logon, files accessed, evidence created, evidence deleted, evidence shared and many other user and elevated user actions.

☐ No

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

Digital information including audio and video is captured from CCTV and various media. Digital information captured and collected is evidentiary in nature. The data collected may include physical attributes of an individual, personal and professional address, telephone, any associated information, and other PII listed in Section 2.A. Non-evidentiary digital media is transitory and destroyed.

The BLM OLES DEMS collects and automatically logs username, date/time of log-in, as well as account changes and database changes including creation, modification, enabling, disabling, and removal for:

1) BLM OLES DEMS access and user accounts to a database table, which triggers an automatic addition to an audit trail which administrators can access at any time for review and verification, and

2) BLM OLES DEMS possesses the ability to integrate through an application programming interface automated auditing tool such as Splunk, which triggers an automatic email notification to system administrators for review and verification and the potential for automated auditing and reporting.

The BLM OLES DEMS has the ability to define customized settings and enforce limits associated with "Password History," "Password Aging," "Minimum Password Length," "Failed Login Limit," "Lockout Duration," and "Session Timeout."

The BLM OLES DEMS has Multi-Factor Authentication Settings which are applied "Agency-Wide" and can be authenticated through "SMS Text," "Automated Call Back," or "Email." The security challenge frequency can also be set from 2 minutes to 20 minutes.

The BLM OLES DEMS has Internet Protocol Active Session Security which can be used to limit access by IP address or IP address range.

The BLM OLES DEMS is capable of Single Sign-On (SSO) integration through the Department of the Interior Active Directory Federation Services (ADFS) for identity verification and authentication using DOI Active Directory.

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

Access granted to individuals is password-protected; each person granted access to the system must be trained and individually authorized to use the system. Each user is assigned to roles, which grant access to specific data within the system. BLM OLES DEMS also logs events including user login/logout, searches, views, downloads, sharing, and data alterations, which are reviewed on a regular scheduled basis. All users must accept the DOI Rules of Behavior before accessing the system and follow established internal security protocols. BLM OLES DEMS has a "Warning Banner" on the login screen notifying users of monitoring. Monitoring functions are limited by role to designated "monitors" and System Administrators. BLM OLES DEMS users are required to complete Annual Training including the following Cybersecurity / Federal Information Systems Security Awareness; Privacy; Records Management and Controlled Unclassified Information training. In addition to the minimum requirements for all users, any users with elevated accounts for system administration must also complete Annual Role Based Security (RBST) training and Annual Role Based Privacy (RBPT) training.

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.

The contractor / vendor who provides the system to DOI also employs a number of physical controls to protect their infrastructure for this BLM system. The contractor / vendor also has a host infrastructure provider who employs a number of physical controls to protect the infrastructure such as a secure controlled access data center.

(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.

(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.

All data is maintained in isolated storage accounts. All metadata and audit logs are maintained in databases on virtual machines. Both are replicated from the primary to the recovery environment which are geographically in separate states. The primary and recovery data centers are geographically separate as required by NIST and FedRAMP's CP-6 and CP-7 controls.

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 Director, BLM Office of Law Enforcement and Security, is the BLM OLES DEMS Information System Owner and the official responsible for oversight and management of the BLM OLES security and privacy controls and the protection of agency information processed and stored in the BLM OLES DEMS system. The Information System Owner, the Technical / System Administrator, the Information System Security Officer and the Associate Privacy Officer are responsible for ensuring adequate safeguards are implemented to protect the privacy, civil rights and civil liberties in compliance with Federal laws and policies for the data managed, used, and stored in the BLM OLES DEMS. These officials and authorized BLM OLES DEMS 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 amendments, as well as

addressing complaints and providing redress, in consultation with BLM and DOI Privacy Officials.

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 BLM OLES DEMS Information System Owner is responsible for oversight and management of the system security and privacy controls, and for ensuring to the greatest possible extent that agency data is properly managed and that all access to agency 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 agency PII is reported to DOI-CIRC within 1-hour of discovery in accordance with Federal policy and established procedures.

BLM 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 at 43 CFR Part 2, Subpart K for 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.