



U.S. Department of the Interior

PRIVACY IMPACT ASSESSMENT

Introduction:

The Department of the Interior (DOI) requires the DI-4001 Privacy Impact Assessments (PIA) form to be conducted and maintained for all IT systems that collect, maintain, use, or share personally identifiable information (PII), whether the system is new, undergoing significant modification, or already in operation as well as electronic collections under the Paperwork Reduction Act. The PIA is a critical tool for evaluating privacy risks, documenting safeguards, ensuring compliance with the E-Government Act of 2002 (Section 208) and OMB Guidance. This form must be completed electronically and submitted to the Department Privacy Office for review and determination via our [Privacy Office Support Request Page](#). For further guidance, consult the [DOI PIA Guide](#).

System Information

System or Project Name:	Verkada Command Platform
System or Project Acronym:	VERK
Bureau or Office:	OCIO
Date submitted for review:	September 4, 2026
System Operational Status:	Operational

Point of Contact

Name:	Dianna Taylor
Title:	Privacy Officer
Office:	Department Privacy Office
Phone:	(202) 208-1605
E-mail:	DOI_Privacy@ios.doi.gov
Address:	U.S. Department of the Interior, 1849 C Street NW, Room 7112, Washington, DC 20240

Section 1: System Overview

1. What triggered this PIA? (Check one)

- | | |
|--|---|
| ☒ New System | ☐ Significant Modification |
| ☐ New Electronic Collection | ☐ Other: Describe below |

This PIA is triggered by the implementation of the Verkada Command Platform as a new DOI information system that collects, maintains, uses, and processes personally identifiable information (PII) in support of physical security, facility access, public safety, and related authorized mission activities. The platform also includes AI-enabled video analytics and other capabilities that may process information about identifiable individuals.

2. What is the purpose of the system or project?

The purpose of the Verkada Command Platform is to provide DOI with an integrated physical-security and facility-management capability that supports the protection of people, facilities, property, and other

Department resources.

The platform enables authorized DOI personnel to manage security cameras and recorded videos, control access to facilities, support visitor-management activities, and use approved search and analytic capabilities to identify and review information relevant to physical security, public safety, resource protection, investigations, and other authorized mission needs.

Individual DOI locations may use different platform capabilities based on their operational requirements and authorized uses.

3. Is the system registered in BisonGRC?

- ☒ Yes: If applicable What is the project's UII code?
☐ No: Explain why this is not either done or required.

The Verkada Command Platform is registered in BisonGRC under Project UII Code OCIO-0120-MIN.

4. What legal authorities authorize the collection and use of data in this system or project?

The Verkada Command Platform supports authorized DOI physical-security, public-safety, resource-protection, facility-access, visitor-management, investigative, law-enforcement, and related mission activities under authorities applicable to the DOI bureau or office, facility, land, resource, or program for which the platform is used.

Applicable authorities include the Federal Property and Administrative Services Act, including 40 U.S.C. § 1315, where applicable to the protection of Federal property and persons, as well as applicable DOI authorities, delegations, and bureau- or office-specific statutory and mission authorities.

The Privacy Act of 1974, E-Government Act of 2002, and applicable Federal and DOI privacy, cybersecurity, records-management, and AI-governance requirements govern how information processed through the platform is assessed, protected, maintained, used, and disclosed. These requirements do not independently provide the underlying authority for a particular physical-security, facility-access, visitor-management, investigative, or law-enforcement activity.

5. Does the system or project require a published Privacy Act System of Records Notice (SORN)?

- ☒ Yes: If yes, list the applicable citations below.
☐ No

The Verkada Command Platform processes physical-security video and images, vehicle and license-plate information, workforce account information, access-control information, audit information, and other information that may be associated with identifiable individuals.

Certain platform capabilities permit authorized retrieval of information using personal identifiers or identifying characteristics, including image-based or biometric matching where enabled and authorized.

Records maintained and retrieved through the platform are covered by DOI System of Records Notices, including

INTERIOR/DOI-46, Physical Security Access Files, and INTERIOR/DOI-10, Law Enforcement Records Management System, depending on the type of record, purpose, retrieval practice, and authorized use.

Records incorporated into an authorized DOI law-enforcement investigation or case are maintained under the appropriate law-enforcement system of records.

6. Does this project involve an information collection that requires OMB approval under the Paperwork Reduction Act?

- ☐ Yes
☒ No

Based on the information described in this PIA, the Verkada Command Platform does not involve a collection of information from members of the public that requires OMB approval under the Paperwork Reduction Act. Information is primarily captured or generated through authorized security cameras, access-control functions, and other platform capabilities used for physical security, public safety, resource protection, facility access, investigations, and related authorized mission purposes.

Any new or materially different collection directly from members of the public will be evaluated to determine whether Paperwork Reduction Act requirements apply.

7. List all minor applications or subsystems that are hosted on this system and covered under this PIA.

No separately registered DOI-developed minor applications or subsystems are hosted on the Verkada Command Platform. Verkada Video Security, Access Control, Air Quality Sensors, Verkada Guest, and associated AI-enabled analytics are components of the system covered by this PIA.

Section 2: Data Description and Use

1. What categories of PII and sensitive data types will the system collect, use, or store? Check all that apply.

- | | | |
|--|---|---|
| ☒ Name (full, first or last) | ☐ Home telephone number | ☐ Employment or resume info |
| ☐ Aliases/nickname | ☐ Personal Email | ☐ Full or Truncated SSN |
| ☐ Driver's license | ☐ Mailing or home address | ☒ Physical characteristics |
| ☐ Citizenship | ☐ Religious preference | ☒ Biometrics/facial recognition |
| ☐ Legal Status | ☐ Mother's maiden name | ☒ Vehicle information |
| ☐ Sex | ☐ Marital status | ☐ Passport information |
| ☐ Race or ethnicity | ☐ Spouse Information | ☐ Travel information |
| ☐ Date of birth | ☐ Child or family information | ☐ Parent's name |
| ☐ Place of birth | ☐ Emergency contact info | ☐ Credit card number |
| ☐ Personal cell phone number | ☐ Financial information | ☐ Nationality |
| ☒ Username / user ID / acct ID | ☒ IP address / network ID | ☒ Device ID / online ID |
| ☐ Geolocation / GPS / location | ☒ Photos / video / audio | ☐ Health / medical information |
| ☐ Tribal or other ID number | ☐ Education information | ☐ Disability Information |
| ☐ Criminal / disciplinary info | ☐ Military records | ☒ Other: Describe below |

The Verkada Command Platform may process different categories of personally identifiable information (PII) depending on the capabilities and configurations deployed at a particular DOI location.

Camera-based capabilities may collect or maintain images, video, and, where enabled, audio involving DOI employees, contractors, volunteers, visitors, and members of the public. Recorded information may include observable physical characteristics, vehicles, license plates, and related activities. Certain enabled capabilities may also generate biometric facial representations and searchable metadata used to locate potentially relevant recorded footage.

The platform may also process workforce account and access-control information, including names, usernames or account identifiers, government email addresses, authentication information, assigned roles or permissions, access events, audit logs, and user activity.

Other PII may include license-plate information, access-control records, audit information, and AI-generated search or analytic metadata

2. What is the source for the PII collected? Check all that apply.

- | | |
|---|--|
| ☐ Individual | ☒ DOI Records |
| ☐ Federal Agency | ☐ Third Party Records |
| ☐ Tribal Agency | ☐ State Agency |
| ☐ Local Agency | ☒ Other: <i>Describe Below</i> |

PII processed by the Verkada Command Platform may originate from DOI employees, contractors, volunteers, visitors, and members of the public whose information is captured through authorized platform functions.

Information may also be generated by Verkada devices and system functions, including security cameras, access-control systems, user accounts, audit logs, and AI-enabled analytics. Where authorized, information may also be obtained from DOI records or approved system integrations.

3. How will the information be collected? Check all that apply.

- | | |
|---|--|
| ☐ Paper Format | ☐ Fax |
| ☐ Email | ☐ Telephone Interview |
| ☐ Face-to-Face Contact | ☐ Shared Between Systems: <i>Describe</i> |
| ☐ Website | ☒ Other: <i>Describe</i> |

Information is collected through DOI-authorized Verkada devices and platform functions deployed at participating DOI locations. For camera-based deployments, security cameras capture video, images, and, where enabled, audio within designated coverage areas. Recorded information may include individuals, observable physical characteristics, vehicles, license plates, and other activities occurring within the monitored environment.

Recorded footage is transmitted to and maintained within the Verkada Command Platform, where authorized personnel may review and search information using available platform capabilities. Certain supported camera configurations may use AI-enabled computer vision and video analytics, including biometric or other image-based matching where enabled and authorized, to assist users in locating potentially relevant recorded footage.

AI-generated results are advisory and are subject to human review and validation before they are relied upon for operational, investigative, administrative, physical-security, fee-collection-oversight, or law-enforcement purposes.

Other supported platform components, including access-control and related administrative functions, may collect, receive, or generate information associated with authorized users, credentials, access permissions, facility-access events, system accounts, administrative activity, and related audit information, depending on the deployed product and configuration.

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

Personally identifiable information (PII) processed by the Verkada Command Platform is used to support authorized DOI physical-security, public-safety, resource-protection, facility-access, fee-collection-accountability, investigative, administrative, and law-enforcement activities.

Recorded video, images, audio where enabled, vehicle and license-plate information, and other observable information may be used to review security or operational events, locate relevant footage, support incident response and investigations, manage facility access, and protect DOI personnel, visitors, facilities, lands, resources, and property.

Accounts, authentication, access-control, administrative, and audit information may be used to authenticate users, administer system and facility access, support accountability, investigate security or operational events, and document authorized activity.

Where enabled and authorized, AI-assisted search and analytic capabilities may be used to help locate potentially relevant recorded information. AI-generated results are advisory and require human review before official reliance.

PII is used only for authorized purposes consistent with the applicable DOI mission and the scope evaluated in this PIA.

5. How does this project limit the collection and use of PII to only what is necessary?

DOI limits the collection, processing, access, and use of personally identifiable information (PII) within the Verkada Command Platform to information necessary for authorized physical-security, public-safety, resource-protection, facility-access, fee-collection-accountability, investigative, administrative, and law-enforcement activities.

Camera placement, field of view, recording settings, retention, and enabled analytic capabilities are configured based on authorized operational needs and, where practicable, to reduce unnecessary collection of PII.

Access to recorded footage, access-control information, account information, audit data, and AI-assisted analytics is restricted through role-based access controls, need-to-know, and least-privilege principles.

Materially different collection practices, information types, analytics, integrations, or uses are evaluated to determine whether additional privacy review is required.

Section 3: Data Sharing and Individual Rights

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

- ☒ **Within the Bureau/Office:** Describe how the data will be used below.
- ☐ **Tribal, State or Local Agencies:** Describe how the data will be used below.
- ☒ **Other Bureaus/Offices:** Describe how the data will be used below.
- ☒ **Contractor:** Describe how the data will be used below.
- ☐ **Other Federal Agencies:** Describe the federal agency and how the data will be used
- ☐ **Other Third-Party Sources:** Describe how the data will be used below.

Information maintained in the Verkada Command Platform may be accessed or shared within DOI by authorized employees and contractors whose official duties require the information for physical security, public safety, resource protection, facility access, investigations, law enforcement, system administration, or related authorized mission activities.

Verkada and other authorized service-provider personnel may have limited access when necessary to provide hosting, maintenance, troubleshooting, security, system administration, or other approved support services. Such access is limited to authorized purposes and is subject to applicable contractual requirements, access controls, logging, and need-to-know restrictions.

Information may also be disclosed outside DOI when authorized by law and consistent with applicable Privacy Act requirements, published System of Records Notices, and other governing authorities.

2. Does this system have an MOU/MOA/ISA with other Federal Agencies or State/Local/Tribal Agencies with which it shares information?

- ☐ Yes
- ☒ No

The Verkada Command Platform does not rely on an MOU, MOA, or ISA for routine sharing among participating DOI bureaus and offices. Information sharing within DOI occurs under applicable Department authorities, policies, access controls, and authorized purposes.

Any future recurring external sharing arrangement or system interconnection will be evaluated to determine whether an MOU, MOA, ISA, or other agreement is required before implementation.

3. Do individuals have the opportunity to decline to provide information or to consent to the specific uses of their PII? If not, what steps are in place to ensure individuals are aware of how their information is being used?

- ☐ Yes: Describe the method by which individuals can decline to provide information or how individuals consent to specific uses.
- ☒ No: State the reason why individuals cannot object or why individuals cannot give or withhold their consent.

Individuals generally cannot decline collection when entering or remaining in areas covered by authorized

security cameras or when participating in required facility-access processes. Collection supports authorized physical-security, public-safety, resource-protection, facility-access, fee-collection-accountability, investigative, and related mission purposes.

Where applicable, individuals are informed of monitoring through posted notices or other appropriate privacy or security notifications. Notice does not constitute consent where collection is required for authorized security, access-control, or mission purposes.

New or materially different direct-collection practices will be evaluated to determine whether additional notice, consent, Privacy Act Statement, PRA review, or other privacy requirements apply.

4. How does the project provide notice to individuals prior to the collection of information? Check all that apply.

- | | |
|---|--|
| ☐ Privacy Act Statement: | ☒ Other: <i>Describe Below</i> |
| ☒ Privacy Notice: | ☐ None: <i>Example - law enforcement cases.</i> |

Individuals are provided notice through posted signage, this published PIA, and other applicable privacy or security notices.

Posted notices at monitored locations inform individuals that video surveillance or other security monitoring may be in use for authorized security and mission purposes.

Where new or materially different direct-collection practices are introduced, DOI will evaluate whether additional notice, including a Privacy Act Statement where required, is necessary.

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

Information in the Verkada Command Platform may be retrieved using search criteria associated with the applicable product, configuration, and authorized use.

Recorded videos may be retrieved using date, time, camera location, vehicle or license-plate information, observable person or vehicle characteristics, and AI-generated metadata. Where enabled and authorized, biometric or image-based matching may also be used to locate potential appearances of the same individual within recorded footage.

Access-control and administrative records may be retrieved using user or account identifiers, credentials, facility or door location, date and time, access-event information, assigned roles or permissions, and related audit information.

AI-generated search results and image-based or biometric matches are treated as potential results and require human review before official reliance.

6. Will reports be produced on individuals, whose PII is contained in this system? If yes, who has access and what is the purpose of these reports?

- ☒ Yes: Describe the use of these reports and who will have access to them.
☐ No

The Verkada Command Platform may generate search results, activity summaries, exported video clips or images, access-event records, audit logs, and other records associated with individuals, vehicles, users, credentials, or facility-access activity.

These records may be used by authorized personnel for physical security, public safety, resource protection, facility access, investigations, law enforcement, system administration, and related authorized mission purposes.

AI-generated search results and other AI-assisted outputs are advisory and require human review before official reliance. Access to reports and related information is restricted to authorized personnel based on role and need to know.

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

Information obtained from sources outside DOI is reviewed by authorized personnel for relevance, accuracy, and reliability before official reliance.

Where appropriate, information may be compared with official government records or other reliable sources to corroborate relevant facts.

AI-assisted search results, biometric or image-based matches, and other derived analytics are treated as potentially relevant information rather than verified facts. Authorized personnel review the underlying footage or other source data and corroborate the information as necessary before taking official action.

New external data sources or integrations that materially change system data flows or retrieval practices will be evaluated before implementation.

Section 4: Data Management and Retention

1. What is the retention period for the data and under what records schedule?

Verkada records may include routine and evidentiary video, exported images or clips, AI-generated metadata or search results, access-control records, audit logs, visitor-management records, and related records. Retention depends on the function and use of each record category.

For NPS law-enforcement camera footage, records are retained under N1-079-08-002, Protection and Safety. Major case files are permanent and transferred to NARA 15 years after closure; Significant case files are destroyed 25 years after closure; Minor case files are destroyed 7 years after closure; and Routine, Non-Evidentiary case files are destroyed 3 years after closure. USPP camera footage is currently unscheduled and will be preserved until an applicable NARA-approved disposition authority is in effect.

Other Verkada records will be retained and disposed of in accordance with the applicable NARA-approved disposition authority based on their function and use.

2. What measures are in place to validate the accuracy and completeness of data received from external sources?

The Verkada Command Platform primarily processes information generated or captured through authorized Verkada devices, platform functions, and approved DOI integrations. The platform does not routinely rely on external-source PII as the primary basis for system operation. If external information is used to support an operational, investigative, administrative, physical-security, or law-enforcement activity, the following measures are used to validate its accuracy and completeness:

- **Manual Review by Authorized Personnel** – Information obtained from external sources is reviewed by authorized personnel before it is relied upon for official purposes.
- **Cross-Referencing with Authoritative Records** – Where appropriate and authorized, information may be compared with official government records or other reliable source information to corroborate its accuracy and completeness.
- **Human Validation of AI-Assisted Results** – AI-assisted search results, biometric or image-based matches, and other derived analytics are treated as potentially relevant information rather than verified facts. Authorized personnel review the underlying recorded footage or other source data before relying on the result for official action.
- **Correction of Discrepancies** – If discrepancies are identified between platform information and information obtained from external sources, authorized personnel verify the information through the originating source or other authoritative records before relying on it.

These measures help support the accuracy, relevance, timeliness, and completeness of information used for authorized DOI activities.

3. Does the project include logging capabilities to record and monitor access to PII?

- ☒ Yes
☐ No

The Verkada Command Platform includes audit logging capabilities that record supported user and administrative activity. Depending on the deployed configuration, logs may include authentication activity, access to recorded footage, AI-enabled searches, access-control events, changes to permissions, downloads, sharing, and other administrative actions.

Audit logs support accountability, security monitoring, incident response, and investigation of suspected unauthorized or inappropriate activity. Access to audit information is restricted to authorized personnel and retained in accordance with applicable DOI security and records-management requirements.

Section 5. Privacy Risks and Mitigation Strategies

1. What privacy risks are associated with the collection, use, retention, and disclosure of PII, and how are they mitigated at each stage of the information lifecycle?

The Verkada Command Platform processes video, access-control information, account information, audit data, biometric representations, and other PII in support of authorized DOI activities. Privacy risks may arise

throughout the information lifecycle.

Collection Risk: Cameras and other platform components may collect more information than necessary.

Mitigation: Camera placement, field of view, configuration, and enabled capabilities are based on authorized operational needs and, where practicable, configured to reduce unnecessary collection.

Use Risk: PII could be accessed or used by unauthorized personnel or for purposes beyond the authorized mission need.

Mitigation: Access is restricted through role-based access controls, least privilege, need to know, authentication, and audit logging.

Retention Risk: Retaining video, biometric representations, access-control records, auditing information, and exported records increases the amount of information available for potential misuse or disclosure.

Mitigation: Records are retained and disposed of under applicable records-management requirements and NARA-approved disposition authorities. Unscheduled records are preserved until an applicable authority is approved.

Disclosure Risk: Unauthorized sharing could expose sensitive information about individuals, vehicles, activities, or facility access.

Mitigation: Information is disclosed only for authorized purposes and is protected through applicable privacy, security, contractual, access-control, encryption, and logging requirements.

AI and Biometric Risk: AI-assisted search or image-based matching may produce inaccurate or incomplete results, and cross-camera searches may allow reconstruction of an individual's movements.

Mitigation: AI-generated results are treated as potential leads rather than verified facts and require human review before official reliance.

Function-Creep Risk: New analytics or platform capabilities could expand beyond the uses evaluated in this PIA.

Mitigation: Materially different capabilities, integrations, data processing, or intended uses are subject to additional privacy and other applicable review before implementation.

2. Does the system generate new data or inferences through aggregation or analytics that may influence decisions or individual records? If so, how are those data verified, used, and protected?

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

☐ No

The Verkada Command Platform may generate AI-assisted metadata, search results, alerts, matches, and other derived information from recorded video and related platform data.

These outputs may create or suggest associations concerning an individual's identity, location, movements, activities, or relationship to an event. AI-generated results are treated as potentially relevant information rather than verified facts and require human review before official reliance.

Derived information retained for official business is subject to applicable access controls, audit logging, privacy protections, and records-management requirements.

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

- ☒ Yes: *Provide explanation below*
☐ No

AI-assisted search results and other derived information are not automatically placed in an individual's official record. However, if a search result, match, screenshot, exported image or video, or other derived information is retained to document an official security, administrative, investigative, or law-enforcement action, it may become part of the applicable official record based on its function and use.

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

- ☐ Yes: *Provide explanation below*
☒ No

The Verkada Command Platform does not independently make final determinations about an individual's identity, intent, behavior, legal status, eligibility, rights, benefits, employment, access to services, or law-enforcement outcome.

AI-assisted search results, matches, alerts, and other derived information may inform operational, investigative, administrative, physical-security, or law-enforcement activities, but authorized DOI personnel review the underlying information and remain responsible for any resulting determination or action.

5. How will the new data be verified for relevance and accuracy? Enter N/A if new data is not derived or created.

AI-generated metadata, search results, matches, alerts, and other derived information are treated as potentially relevant information rather than verified facts.

Authorized personnel review the underlying recorded footage or other source information to determine whether the result is relevant and sufficiently accurate for the authorized purpose. Where appropriate, results are corroborated with other reliable information before official reliance.

Authorized DOI personnel remain responsible for any resulting determination or action. AI-generated metadata, search results, and other derived information are treated as potential leads rather than verified facts.

Section 6: Automated Decision-Making and AI Risk Management

1. Does the system use AI, machine learning, automated analytics, inference, scoring, ranking, recommendation, summarization, content generation, or have a non-operational AI component?

- ☒ Yes, describe the AI capability, how it is used
☐ No, *Proceed to Section 7.*

The Verkada Command Platform uses AI-enabled computer vision and video analytics to assist authorized DOI personnel in locating and reviewing recorded footage. Depending on the deployed configuration and authorized use, capabilities may include People History, Person Attributes, Face Detection, Person of Interest Alerts, Vehicle

History, License Plate Recognition, and AI-powered Search.

Where enabled and authorized, users may search recorded footage for individuals, faces, vehicles, license plates, animals, objects, and other observable characteristics. Face Detection may also be used to locate potential matches to a face appearing in recorded footage or an uploaded image.

AI-generated results are treated as potential leads and require human review before official reliance. The platform does not independently make final determinations regarding identity, rights, benefits, eligibility, employment, access to services, or law-enforcement outcomes. Authorized DOI personnel remain responsible for any resulting determination or action.

2. How are models validated for fairness, accuracy, and transparency?

DOI does not develop or train the underlying Verkada AI models and has not independently validated model performance, training data, demographic performance, or model-specific error rates.

AI-generated results are reviewed against the underlying video and other available information before official reliance. Face Detection and other image-based matching results are treated as potential matches or investigative leads rather than confirmed identification.

DOI considers available vendor documentation, known limitations, reported performance information, observed errors, and operational experience when evaluating whether an enabled AI capability remains appropriate for its authorized use. Vendor information may inform that evaluation but does not constitute independent DOI validation.

3. Are individuals notified of AI-based decisions that affect them?

- ☐ Yes
☒ No

Individuals are not separately notified of AI-based decisions because the Verkada Command Platform does not independently make final determinations regarding an individual's rights, benefits, eligibility, employment, access to services, law-enforcement outcomes, or other consequential matters.

AI-generated matches, search results, alerts, and analytics may assist authorized DOI personnel, but any consequential determination or action is made by authorized DOI personnel after reviewing the underlying information and other relevant evidence.

4. Are safeguards in place to prevent bias or unintended consequences?

- ☒ Yes
☐ No

AI-enabled capabilities are subject to role-based access controls, least-privilege and need-to-know restrictions, authentication, audit logging, and authorized-use limitations.

AI-generated search results, matches, alerts, and other derived information are treated as potential leads rather

than verified facts and require human review of the underlying footage or other source information before official reliance.

DOI also limits privacy risk through configuration controls, purpose limitations, records-management requirements, security monitoring, and additional privacy, cybersecurity, or AI-governance review when materially different capabilities or uses are proposed.

5. Are models periodically reviewed or retrained to ensure ongoing reliability?

- ☒ Yes
☐ No

DOI does not train, fine-tune, or retrain Verkada's underlying AI models. DOI periodically reviews the continued suitability of AI capabilities enabled for Department use, including material vendor or model changes, reported errors or false matches, changes to authorized use cases, and other information relevant to continued use.

Material changes to AI functionality, data processing, or intended use are subject to appropriate review before continued operational use.

6. Is federated learning used for privacy-preserving model training?

- ☐ Yes
☒ No

Federated learning is not used by the Verkada Command Platform. DOI does not develop, train, fine-tune, or retrain the AI models used by the platform.

AI-enabled capabilities are provided and maintained by Verkada and are used by DOI to assist authorized personnel in searching and reviewing recorded information.

Section 7: Security and Access Controls

1. Who will have access to project data and how is access determined, authorized, and restricted? Check all that apply and respond in the space below.

- | | |
|---|--|
| ☒ Users | ☒ System Administrator |
| ☒ Contractors | ☐ Other: <i>Describe below</i> |
| ☐ Developers | |

Access to the Verkada Command Platform is limited to authorized DOI employees and contractors whose official duties require access. Permissions are assigned based on job responsibilities, operational needs, privilege, and role-based access controls.

System administrators manage accounts, configuration, and other administrative functions. Authorized users may access recorded footage, AI-enabled search capabilities, access-control information, or other platform data necessary for their assigned duties. Access is periodically reviewed and removed when no longer required, and

relevant user and administrative activity is logged.

Verkada support personnel may have limited access when necessary for authorized support or maintenance. Support access is granted by an authorized DOI administrator, is time-limited and revocable, and is logged. Access to images, video, or audio is disabled by default unless needed for the approved support activity.

2. What data protection policies apply to cloud-based PII storage?

The Verkada Command Platform stores and processes PII within a FedRAMP-authorized cloud environment and is subject to applicable Federal and DOI security and privacy requirements.

PII is protected through safeguards that include encryption in transit and at rest, role-based access controls, authentication, audit logging, security monitoring, and other controls implemented under DOI's security risk-management process.

FedRAMP authorization supports DOI's security assessment and authorization activities but does not by itself authorize every data type, capability, integration, configuration, or operational use.

Applicable security requirements and guidance include DOI cloud-security requirements, FedRAMP requirements, NIST SP 800-53 security and privacy controls, and NIST cloud-security guidance.

3. How does the system monitor and detect unauthorized access, use, or exfiltration of PII?

The Verkada Command Platform uses audit logging, access controls, authentication, security monitoring, and incident-response procedures to help detect and investigate unauthorized access, use, disclosure, or exfiltration of PII.

Audit logs supported user and administrative activity, including authentication, access to recorded footage, AI-enabled searches, downloads, sharing, access-control events, and changes to permissions or system configuration.

Authorized system administrators and security personnel may review audit and security information for suspicious or unauthorized activity. Where configured, audit information may also be exported or integrated with DOI security-monitoring tools.

Suspected or confirmed unauthorized access, disclosure, loss, or exfiltration of PII is handled under applicable DOI security-incident and privacy-breach procedures.

4. Does the project include any monitoring of user activity or tracking of individuals? If so, what controls ensure the appropriate use of this capability by authorized personnel?

☒ Yes: describe what controls ensure authorized and appropriate use of this capability.

☐ No

The Verkada Command Platform may enable authorized personnel to locate and follow individuals, vehicles, or other subjects across recorded footage using camera location, date and time, observable characteristics, license-plate information, and AI-assisted search capabilities.

Where enabled and authorized, biometric or image-based matching may also be used to identify potential appearances of the same individual across multiple cameras.

These capabilities are limited to authorized operational purposes and personnel with a documented need for access. AI-generated matches and tracking results are treated as potential leads and require human review before official reliance.

Relevant user and administrative activity are logged, and materially different tracking or analytic capabilities are subject to additional review before implementation.

5. Will contractors be involved in the following project activities? Check all that apply.

- ☒ Design
- ☒ Development
- ☒ Maintenance

Authorized contractor personnel may have access to PII only when necessary to perform approved design, development, maintenance, or support activities and only after appropriate authorization has been granted. Contractor access is limited to the minimum information and system privileges necessary to perform assigned duties and is subject to least privileged requirements.

Contractor personnel with authorized access to PII are required to sign non-disclosure agreements, comply with applicable Federal Acquisition Regulation Privacy Act clauses, complete DOI-approved annual privacy and security awareness training as applicable, and comply with Department Rules of Behavior and contractual security requirements.

Contractor access is restricted through role-based access controls, protected by audit logging, and periodically reviewed by the System Owner and Information System Security Officer to confirm continued operational need. Verkada support access is time-limited, revocable, and logged.

6. What physical, technical, and administrative controls are implemented to protect PII? Check all that apply.

Physical Controls

- | | |
|---|---|
| ☒ Security Guards | ☐ Cipher Locks |
| ☐ Key Guards | ☒ Identification Badges |
| ☐ Locked File Cabinets | ☐ Safes |
| ☒ Secured Facility | ☐ Combination Lock |
| ☒ Closed Circuit Television | ☐ Other: <i>Describe Below</i> |

Describe the other types of controls implemented.

Technical Controls

- | | |
|--|---|
| ☒ Password | ☐ Intrusion Detection Systems (IDS) |
| ☒ Firewall | ☐ Virtual Private Network (VPN) |
| ☒ Encryption | ☐ Public Key Infrastructure (PKI) Certificates |

- ☒ User Identification
☐ Other: *Describe Below*

☐ Biometrics

Describe the other types of controls implemented.

Administrative Controls

- | | |
|--|---|
| ☒ Periodic Security Audits | ☒ Methods to Ensure Only Authorized Personnel Have Access |
| ☒ Backups Secured Off-site | ☒ Encryption of Backups Containing Sensitive Data |
| ☒ Rules of Behavior | ☒ Mandatory Security, Records and Privacy Training |
| ☒ Role-Based Training | ☒ Regular Monitoring of Users' Security Practices |
| ☐ Other: <i>Describe Below</i> | |

Describe the other types of controls implemented

7. What processes are in place for individuals to file a Privacy Act complaint relating to the project?

Individuals may file a Privacy Act complaint regarding the Verkada Command Platform through the Department of the Interior's established Privacy Act complaint process.

- **Submission Methods** – Complaints may be submitted by email to privacy@doi.gov, by mail to the Departmental Privacy Office, U.S. Department of the Interior, 1849 C Street NW, Washington, DC 20240, or by submitting a request through the Department's [FOIA and PA Public Access Link](#).
- **Responsible Office** – The DOI Departmental Privacy Office receives Privacy Act complaints and coordinates with the appropriate Bureau Privacy Officer, System Owner, and program officials to review the matter.
- **Review Process** – The complaint is evaluated to determine whether a Privacy Act issue or privacy violation has occurred. The Privacy Office coordinates with the appropriate officials to investigate and determine any necessary corrective actions.
- **Resolution and Response** – DOI provides a written response to the complainant describing the outcome of the review and any corrective actions taken, as appropriate.
- **Notice to Individuals** – Individuals are informed of available privacy rights through posted camera signage, applicable Privacy Act notices, and Department privacy policies, where applicable.

This process is conducted in accordance with the Privacy Act of 1974 (5 U.S.C. § 552a) and 43 CFR Part 2, Subpart K.

8. What processes are in place for individuals to access their information?

Individuals may request access to records maintained by the Verkada Command Platform by submitting a request under the Privacy Act or the Freedom of Information Act (FOIA), as applicable.

- **Request Methods** – Requests may be submitted by email to privacy@doi.gov, by mail to the Departmental Privacy Office, U.S. Department of the Interior, 1849 C Street NW, Washington, DC 20240, or electronically through the Department's [FOIA and PA Public Access Link](#). Requests should include the individual's full name, contact information, a description of the records sought, and proof of identity, as required.

- **Responsible Office** – The DOI Departmental Privacy Office, in coordination with the appropriate Bureau Privacy Officer and System Owner, processes Privacy Act and FOIA requests.
- **Processing and Review** – Upon receipt, the Privacy Office verifies the identity of the requester, determines whether responsive records exist, and coordinates with the System Owner and appropriate program officials to locate and review responsive records.
- **Response** – DOI responds in accordance with applicable Privacy Act and FOIA requirements, providing access to records or explaining any applicable exemptions or limitations.

This process is conducted in accordance with the Privacy Act of 1974 (5 U.S.C. § 552a), the Freedom of Information Act (5 U.S.C. § 552), and 43 CFR Part 2, Subpart K.

9. What processes are in place to allow the subject individual to correct inaccurate or erroneous information?

Individuals may request correction or amendment of inaccurate or erroneous information maintained by the Department in accordance with the Privacy Act of 1974 (5 U.S.C. § 552a) and 43 CFR Part 2, Subpart K.

- **Request Methods** – Requests for amendment may be submitted by email to privacy@doi.gov, by mail to the Departmental Privacy Office, U.S. Department of the Interior, 1849 C Street NW, Washington, DC 20240, or through the Department's [FOIA and PA Public Access Link](#). Requests must include sufficient identifying information, a description of the information to be corrected, and verification of identity.
- **Processing and Review** – The DOI Departmental Privacy Office reviews the request, verifies the identity of the requester, and coordinates with the System Owner and appropriate program officials to determine whether an amendment is warranted.
- **Response** – DOI responds in accordance with applicable regulations by either correcting the information or providing a written explanation if the request is denied, including information regarding the individual's right to appeal.
- **Limitations** – Requests to amend recorded video footage or associated evidentiary records are evaluated in accordance with applicable legal, investigative, and records management requirements. Where appropriate, supplemental or clarifying information may be added to the record rather than altering the original evidentiary footage.

This process ensures compliance with the Privacy Act while preserving the integrity of official Department records.

10. 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?

Responsibility for ensuring the proper use and protection of information processed by the Verkada Command Platform is shared among Department officials with privacy, security, and operational responsibilities.

- **System Owner** – Ensures the Verkada Command Platform is operated in accordance with applicable federal laws, Department of the Interior policies, privacy requirements, records management requirements, and security controls. The System Owner is responsible for approving appropriate system access, ensuring information is used only for authorized purposes, and overseeing the operational use of the platform.
- **Information System Security Officer (ISSO)** – Oversees the implementation and effectiveness of system security controls, monitors security events, reviews audit logs, and coordinates security incident

response activities in accordance with Department cybersecurity policies.

- **Privacy Officer** – Provides oversight to ensure compliance with the Privacy Act of 1974, the E-Government Act of 2002, Department privacy policies, and applicable privacy requirements. The Privacy Officer coordinates the assessment and reporting of privacy incidents and provides guidance on the appropriate handling and safeguarding of personally identifiable information (PII).
- **Authorized Users** – Access and use information only for official government purposes consistent with their assigned duties. Users are responsible for protecting PII, complying with Department Rules of Behavior, completing required privacy and security training, and promptly reporting suspected or confirmed privacy incidents.
- **Incident Reporting** – Any suspected or confirmed loss, compromise, unauthorized disclosure, or unauthorized access to PII must be reported immediately in accordance with Department incident reporting procedures. Privacy incidents are reported to the **Department of the Interior Computer Incident Response Center (DOI-CIRC)** and the Departmental Privacy Officer for investigation, assessment, mitigation, and notification, as required.

These responsibilities help ensure that information processed by the Verkada Command Platform is appropriately protected throughout its lifecycle and that privacy incidents are managed in accordance with applicable federal and Department requirements.

Section 8: Incident Response and Review

1. In the event of a privacy breach, what steps will be taken to mitigate harm, notify affected individuals, and report to oversight agencies?

In the event of a privacy breach involving the Verkada Command Platform, the Department of the Interior will follow the procedures outlined in the **DOI Privacy Breach Response Plan**.

1. **Immediate Reporting** – Any suspected or confirmed privacy breach involving the Verkada Command Platform must be reported immediately, and no later than one hour after discovery, to the DOI Computer Incident Response Center (DOI-CIRC) and the Departmental Privacy Officer, in accordance with Department incident reporting procedures.
2. **Containment and Mitigation** – The Information System Security Officer (ISSO), System Owner, DOI-CIRC, and other appropriate officials will work to contain the incident by securing affected systems, restricting unauthorized access, preserving evidence, and implementing measures to prevent additional loss or unauthorized disclosure of personally identifiable information (PII).
3. **Risk Assessment** – The Department Privacy Officer, System Owner, ISSO, and incident response team will assess the nature and scope of the incident, including the type of information involved, the number of individuals affected, the likelihood of misuse, and the potential risk of harm to individuals and the Department.
4. **Notification** – When required, affected individuals will be notified without unreasonable delay in accordance with applicable law, OMB guidance, and Department policy. Notifications will describe the nature of the incident, the types of information involved, protective measures individuals may take to help protect themselves, and Department contact information for obtaining additional assistance.
5. **Oversight Reporting** – The Department will report privacy incidents to appropriate oversight organizations, including the Office of Management and Budget (OMB), the Department of Homeland Security (DHS), Congress, and other entities, as required by applicable federal laws, regulations, and

Department policies.

6. **Remediation and Prevention** – Following resolution of the incident, the Department will implement corrective actions, as appropriate, which may include enhancing technical or administrative safeguards, updating policies and procedures, conducting additional workforce training, and strengthening security controls to reduce the likelihood of similar incidents in the future.

These measures ensure a coordinated, timely, and compliant response to privacy incidents while protecting individuals and maintaining the confidentiality, integrity, and availability of information processed by the Verkada Command Platform.

2. How often will this PIA be reviewed and updated to reflect changes in privacy risks or system operations?

The Verkada Command Platform will be reviewed annually through the applicable DOI Privacy Threshold Analysis process and whenever a material change may affect privacy risk.

Material changes include new camera deployments or materially different fields of view, new categories of PII, changes to retention, new external sharing, material changes to Face Match or other AI analytics, use of reference images or watchlists, automated alerts, new data integrations, changes to cloud or vendor services, or expanded operational uses.

The PIA will be updated when a material change makes the current public assessment inaccurate or incomplete. When no material privacy change has occurred and the existing PIA remains accurate, it may be reaffirmed in accordance with DOI privacy procedures.