U.S. Department of the Interior
PRIVACY IMPACT ASSESSMENT

Introduction

The Department of the Interior requires Privacy Impact Assessments (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: Video Surveillance System (Closed Circuit Television)
Bureau/Office: National Park Service, U.S. Park Police
Date: November 16, 2022
Point of Contact:
Name: Felix Uribe
Title: NPS Associate Privacy Officer
Email: nps_privacy@nps.gov
Phone: (202) 354-6925
Address: 12201 Sunrise Valley Drive, MS 242, Reston, VA 20192

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 U.S. Park Police (USPP) operates video camera systems used to support nationwide law enforcement, security and emergency services. The system supports the Washington, DC area for the National Icons (memorials in the National Mall area) and the New York City area for the Statute of Liberty and Ellis Island. These systems are collectively referred to as the USPP Video

Surveillance System (VSS), previously known as the Closed-Circuit Television (CCTV) System. VSS consists of multiple cameras, network video recorders (NVRs), a local area network, multiple workstation computers or server hardware, software required to store and view the video, and monitoring capabilities that capture video feeds in and around the National Icons and the Statute of Liberty/Ellis Island. VSS components reside on the Department of the Interior (DOI) National Park Service (NPS) network and/or local closed networks but may use encrypted communications to transmit to central stations.

The purpose of the VSS is to help USPP secure and regulate physical access around the National Icons and the Statute of Liberty/Ellis Island. The system also serves to enhance officer safety, prevent crimes, detect and respond to emergencies, and assist in the investigation of criminal acts committed on NPS lands and inside and on the perimeter of protected NPS facilities. Video surveillance also supports terrorism prevention and facility protection with its visible presence and detects and deters unauthorized intrusion at NPS facilities. This privacy impact assessment (PIA) covers the general use of VSS in accordance with Federal and Departmental policy and to identify and address privacy implications for the use of VSS, particularly surveillance, image, and video capabilities.

In general, the VSS captures video of the general public on the exterior and interior of some NPS facilities as well as at selected ingress/egress points and locations on or adjacent to NPS lands. Video of the public may be collected in public areas such as entrance drive up fee booths, museum collection areas, walkways, outdoor areas such as parking lots or trailheads, and in areas adjacent to NPS properties, such as roadways or neighboring businesses or government properties. The VSS captures video of all persons on or in the immediate observable vicinity of NPS properties. NPS staff may be recorded while in their office area, on the job (fee collection, visitor centers, and similar) or while handling cash. Cameras may be placed to observe traffic in hallways and rooms that are considered sensitive to the operations of the NPS.

These video recordings are saved and allow for play-back for event reconciliation, records retrieval, and quality assurance. The organization of historical data and the ability to immediately maintain and recall information along with access to the above-mentioned information systems will directly result in added safety to the general public and park visitors as well as law enforcement and other NPS staff and contractors. By utilizing the VSS, Law Enforcement staff will be able to handle emergency and hazard incidents in a safe and efficient manner consistent with national and department standards. The chronological nature of this video recording prevents NPS from retrieving video information by the name of an individual or some identifying number, symbol, or another identifier assigned to the individual.

This information will be used to collaborate with Federal, state and local law enforcement activities. VSS will enhance the following abilities:

- Provide surveillance of the National Icons and the Statute of Liberty/Ellis Island lands and facilities including buildings and physical infrastructure

- Identify, respond, and manage public safety, security, and emergency events on NPS lands
- Assist in managing visitor use and protection programs
- Protect natural and cultural resources
- Prevent, detect and investigate known and suspected criminal activity.

NPS VSS users are categorized as either: (1) Operators or (2) System Administrators (collectively, NPS Users). Operators of the VSS consist of authorized NPS staff with the ability to view live and recorded video from the facility at which they are located. For the National Icons and the Statute of Liberty/Ellis Island, the VSS automatically records for 30 days to the server. The system will overwrite data over 30 days old. An officer/supervisor in the USPP Icon Protection Unit (IPU) or at the Statute of Liberty/Ellis Island may designate selected records as evidentiary, and these records will be maintained in accordance with the incident's disposition schedule. As needed to support law enforcement investigations, USPP may export evidentiary records to a portable media device to transfer to the appropriate evidence custodian. System Administrators, comprised solely of NPS personnel, have the capability to copy video from the video collection hardware/software to portable electronic media. Only System Administrators who are NPS supervisors are authorized to delete video, and deletion occurs at the NVR itself.

Access to video through the VSS is restricted. Authorized users of the VSS will be able to access the system and/or view video in one of two ways: (1) through a VSS workstation located at the National Icons and the Statute of Liberty/Ellis Island or (2) by viewing live video displays at certain guard posts or offices at the National Icons and the Statute of Liberty/Ellis Island. A VSS workstation is a computer terminal on which VSS monitoring software has been installed to allow it to logon to the VSS and view other VSS component systems (e.g., cameras). Cameras with pan/tilt/zoom capabilities may be controlled using a joystick and keyboard attached to a workstation. Workstations may be located in individual office areas or in a security command center staffed by NPS staff. A security command center allows NPS staff to monitor real-time and recorded video using multiple workstations and display screens located in the center.

In addition, at certain facility guard stations and offices, VSS video displays may show live video feeds from cameras to authorized users. These video displays only show live video feeds; recorded video is not available, and video may not be saved to external electronic media. As with workstations, authorized personnel at these guard stations and offices may only view video from the NPS facility at which they are located. VSS video feed at the National Icons and the Statute of Liberty/Ellis Island facilities is continuously monitored by NPS staff. If suspicious activity is observed, NPS personnel are dispatched to the scene to investigate. Relevant video may then be saved to DVD or other digital media in the event it is needed for further investigation of the incident. Video saved to portable electronic media is used to support criminal, terrorism, or internal disciplinary investigations.

Though VSS may cover areas where access controls or access control systems are implemented (e.g., building ingress and egress points), VSS does not interface with access control systems.

VSS PIA does not include assessment for webcams for viewing wildlife, cultural or natural resources, or other activities not directly associated with law enforcement, security, or emergency services. VSS also does not employ audio recording or facial recognition technology. Audio recording is prohibited.

C. What is the legal authority?

- 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 CFR part 23
- Executive Departments, 5 U.S.C. 101
- 5 U.S.C. 301, Departmental Regulations (Pub. L. 89-554)
- Public Buildings, Property, and Works, 40 U.S.C., paragraph 486(c)
- Federal Property Management Regulations, 41 CFR part 101
- Department of the Interior, 41 CFR part 114
- Executive Order 12977, Interagency Security Committee, 60 FR 54411
- Executive Order 13587, Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information, 76 CFR 63811
- REAL ID Act of 2005, (Pub. L. 109-13)
- Federal Information Security Modernization Act of 2014 – FISMA (Pub. L. 113-283)
- National Defense Authorization Act of 2019 (Pub. L. 115-232)
- National Defense Authorization Act of 2020 (Pub L. 116-92)
- National Park Service and Related Programs, 54 U.S.C. §100101, §1022701

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: 010-000000590
System Security Plan (SSP): USPP Video Surveillance System Security and Privacy Plan

☐ No

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

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

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

☐ Yes
☒ No

VSS is not a Privacy Act system of records as the videos may only be searched by date, time, and location. However, information related to the recordings that are used for law enforcement investigation purposes are covered under the INTERIOR/DOI-10, Incident Management, Analysis and Reporting System, SORN, 79 FR 31974 (June 3, 2014); modification published 86 FR 50156 (September 7, 2021).

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.

☒ Gender
☒ Group Affiliation
☒ Medical Information
☒ Disability Information

☒ Employment Information
☒ Race/Ethnicity

☒ Other
Data collected in support of law enforcement, security or emergency response purposes and may include still images, videos, date/time stamp, location, and incidental images of persons, buildings, vehicles and residences that may be associated with persons. Collected video images may contain facial images and images of an individual's personally identifiable information (PII) such as car license plate numbers, written text or documents on person's belongings. Information captured in video and images may include incidental PII, such as group affiliation, which may be covered by First Amendment rights. Incidental PII associated with First Amendment rights will be used for the sole purpose of identifying and recording the presence of individual engaged in unlawful conduct.

For use of visual recordings, individuals who enter on Federal properties and public areas do not have a reasonable expectation of privacy. NPS 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 images captured during law enforcement operations or activities. Due to the purpose and nature of the system, to support law enforcement, security and emergency services operations, individuals generally will not have the opportunity to consent to the collection or use of the recording of their images or activities. For use of video recordings, individuals who enter on Federal properties and public areas do not have a reasonable expectation of privacy. In some instances, providing notice to individuals whose information is being collected would interfere with NPS's ability to carry out its law enforcement, security, and emergency services mission by potentially compromising emergency response or frustrating the confidential nature of investigations, methods, or sources.

Entering on NPS lands implies consent to use of video surveillance for the stated purposes. NPS may post signs that inform individuals of surveillance activities, but in some cases, an individual may not have seen or had an opportunity to view posted signage before being observed or recorded on video. Implied consent occurs where individuals' behavior or failure to object indicates agreement with the collection or use of PII (e.g., by entering and remaining in a building where notice has been posted that security cameras are in use, the individual implies consent to the video recording). If an individual remains in an area with posted signs, they are granting implied consent. Individuals may take action to prevent the new or continued collection or use of PII by removing themselves from the area under surveillance. Offering individuals the opportunity to affirmative action to allow collection or use of PII is not feasible for the specified use of the system and purposes of the law enforcement, security, and emergency services mission.

Exceptions to this policy and practice can occur when individuals have a reasonable expectation of privacy, to protect their identity, to obtain voluntary statements from a sexual assault victim, when a juvenile is involved, or as stipulated by policy.

PII for Government Users (NPS employees and other NPS badged staff) is required for authentication, account management and logging purposes. NPS users use their government issued Personal Identity Verification (PIV) card authenticated through the Enterprise Active Directory (AD). VSS collects the subsystem user's name, email address, username, and role or access level for authorized users.

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

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

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

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

Information is collected via live streaming data collection. Some residual images could be retained on a Secure Digital (SD) card in a physical camera which could be recovered in the event of a failure of the connection to the primary system; however, when the connection is restored, the images are transmitted to the primary system, and these residual images are over written.

For NPS Users, information is collected from the individual during onboarding or generated as DOI records (e.g., work email address, UPN, username) during operational activities at the individual park sites by park staff.

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

PII collected will be used to support the nationwide law enforcement, security and emergency services. Data collection activities include, but are not limited to:

- Search and rescue
- Emergency response and disaster recovery
- Law enforcement investigations
- Regulatory compliance

Images may be provided to law enforcement, security, and emergency services officials for processing, use, and dissemination as appropriate. Access to the images is given only to authorized persons who have an official "need to know".

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

☒ Within the Bureau/Office

NPS may use VSS in support of emergency response, security, or for increased situational awareness for law enforcement, security, and emergency services operations. Data sharing may occur with security, law enforcement and emergency services within and between park and office units to respond to common threats or incidents. Data sharing will be restricted within the NPS based on the user's role and permission and park, program or office assignment.

☒ Other Bureaus/Offices

Data may be shared with other bureaus within DOI as authorized and necessary to support law enforcement, security, and emergency services and the DOI mission. Video and still images collected may be used for enhanced situational awareness and to provide evidence of a violation of law. Case files on individuals or incidents are not maintained in the VSS. Video and still images are not associated with an individual and are only used to indicate where an individual or group of individuals may be for emergency response purposes. Video and still images of private citizens or property outside the National Icons and the Statute of Liberty/Ellis Island may be incidentally captured and will not be used for any purpose. Data sharing will be restricted between and within the DOI Bureaus based on the user's role and permission and organizational assignment.

☒ Other Federal Agencies

Case files on individuals or incidents are not maintained in the VSS. Data from the system that is associated with an event or case file in a system of records may be shared with other Federal agencies for law enforcement or emergency response purposes when authorized and as described in the routine uses in the DOI-10 SORN. Data may be shared with Federal partners under a cooperative agreement or during cooperative operations. Information shared may include still images, video feeds, or downloaded video recordings. Video and still images collected may be used for enhanced situational awareness and to provide evidence of a violation of law. Case files on individuals or incidents are not maintained in the VSS. Video and still images are not associated with an individual and are only used to indicate where an individual or group of

individuals may be for emergency response purposes. Video and still images of private citizens or property outside the National Icons and the Statute of Liberty/Ellis Island may be incidentally captured and will not be used for any purpose. Data sharing will be restricted between and within the agencies based on the user's role and permission and organizational assignment.

PII may be shared with other Law Enforcement agencies as part of the information sharing environment under the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), 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 DOI.

☒ Tribal, State or Local Agencies

Case files on individuals or incidents are not maintained in the VSS. VSS data that is associated with an event or case file in a system of records may be shared with other Tribal, State or local agencies for law enforcement, security, or emergency response purposes when authorized and as described in the routine uses in the DOI-10 SORN. Data may be shared under a cooperative agreement or during cooperative operations with these organization and may include still images, video feeds, or downloaded video recordings. Any joint operation or information sharing is in accordance with a Memorandum of Understanding or other sharing agreement in accordance with DOI policy. Recipients of data gathered by VSS are subject to Federal policy, regulations, and DOI policy governing use of VSS.

PII may be shared with other Law Enforcement agencies as part of the information sharing environment under the IRTPA, 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 DOI.

☒ Contractor.

NPS parks and offices may use contractors to support various program areas. NPS contractors are subject to Federal policy, regulations, and DOI and NPS policy governing use of video camera systems and data and must meet all statutory and policy requirements for information management and security and privacy.

Contractors that provide law enforcement, security and/or emergency services which may include viewing of live stream or recorded video or images are trained and certified in the appropriate specialty. Contractors providing law enforcement or security services are registered and bonded peace officers or security officers, respectively.

Contractors are responsible for the operations and maintenance of the VSS components. NPS may contract with other commercial organizations to provide configuration, operations and maintenance of the system components. Contractors have access to the components to provide support and maintenance for the applications that host PII but will not have access to the actual

PII data. This maintenance is critical to protecting the system and the PII contained within the system.

Only authorized contractors with the necessary background and training for their specific roles will be granted access to the system. All contractor staff will be required to undergo a wants/warrants check as well as a criminal history check. Contractor staff access will be restricted to data on a need-to-know basis.

☒ Other Third-Party Sources

VSS data that is associated with an event or case file in a system of records may be shared with the news media and the public in support of law enforcement, security and emergency services activities, including obtaining public assistance with identifying and locating criminal suspects and lost or missing individuals, providing the public with alerts about dangerous individuals, or protecting the integrity of DOI, NPS, or any DOI employee acting in his or her official capacity. Information may also be shared with other third parties as authorized and as described in the routine uses in the DOI-10 SORN.

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

☐ Yes

☒ No

Due to the purpose and nature of the system to support law enforcement, security and emergency services operations, individuals generally will not have the opportunity to consent to the collection or use of the recording of their images or activities. For use of video recordings, individuals who enter on Federal properties and public areas do not have a reasonable expectation of privacy. In some instances, providing notice to individuals whose information is being collected would interfere with NPS's ability to carry out its law enforcement, security, and emergency services mission by potentially compromising emergency response or frustrating the confidential nature of investigations, methods, or sources.

Entering on NPS lands implies consent to use of video surveillance for the stated purposes. NPS may post signs that inform individuals of surveillance activities, but in some cases, an individual may not have seen or had an opportunity to view posted signage before being observed or recorded on video. Implied consent occurs where individuals' behavior or failure to object indicates agreement with the collection or use of PII (e.g., by entering and remaining in a building where notice has been posted that security cameras are in use, the individual implies consent to the video recording). If an individual remains in an area with posted signs, they are granting implied consent. Individuals may take action to prevent the new or continued collection or use of PII by removing themselves from the area under surveillance. Offering individuals the

opportunity to affirmative action to allow collection or use of PII is not feasible for the specified use of the system and purposes of the law enforcement, security, and emergency services mission

Exceptions to this policy and practice can occur when individuals have a reasonable expectation of privacy, to protect their identity, to obtain voluntary statements from a sexual assault victim, when a juvenile is involved, or as stipulated by policy

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

☐ Privacy Act Statement

☒ Privacy Notice

Notice is provided through publication of this PIA.

☒ Other

Notice may be provided by posted signs for areas that use VSS and the NPS Policy Statements posted on National Park websites. Parks using VSS may display a copy of the VSS policy as part of their compendium on the park website.

Formal written notice is not provided to individuals at the point of collection of this information because of the law enforcement, security, and emergency services context in which it is collected. In some instances, providing notice to individuals whose information is being collected would interfere with NPS's ability to carry out its law enforcement, security, and emergency services mission by potentially compromising emergency response or frustrating the confidential nature of investigations, methods, or sources.

In some cases, such as for use of visual recordings, individuals who enter on Federal properties and public areas do not have a reasonable expectation of privacy. NPS controlled areas may have signs posted that inform individuals of surveillance activities, but in many cases, individuals may not see notices to consent for images captured during law enforcement activities.

Exceptions to this policy and practice can occur when individuals have a reasonable expectation of privacy or as stipulated by policy.

☐ None

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

The chronological nature of this video recording prevents NPS from retrieving video information by the name of an individual or an identifying number, symbol, or other particular assigned to the individual. Data is retrieved by date, time, or location.

I. Will reports be produced on individuals?

☐ Yes

☒ No

Section 3. Attributes of System Data

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

Video or images of individuals, automobiles, or other property is collected in real time and are not verified for accuracy. Individuals are not identified unless an event occurs and information used for identification is not captured in this system. Images or data collected that relates to individuals for an authorized purpose is verified and associated with a case file and is covered by a separate law enforcement system of records for that case file system or law enforcement system after the images are cross referenced to an investigation or case. Case files are not managed in the VSS.

B. How will data be checked for completeness?

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

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

The video and/or images of individuals are taken in real time are not checked for currency because any collection of PII in these instances is inadvertent and is not retained unless the information is determined to be necessary to an authorized mission, is maintained in a system of records covered by the Privacy Act or is required to be retained by other applicable law or regulation. If no event is identified, video not associated with a law enforcement action is overwritten after a storage period of 30 days. If an event is identified, video of that event is saved as evidence in a separate law enforcement system.

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

Records are retained in accordance with the NPS Records Schedule, Protection and Safety (Item 2), which has been approved by the National Archives and Records Administration (NARA) (Job No. Nl-79-08-02). Transitory, non-evidentiary records are disposed after 30 days of retention. NPS restricts the maintenance of images or video feeds not necessary for retention to the minimum necessary (30 days) in accordance with approved records retention schedules for routine surveillance, images, and video recordings.

Only the images or video needed to support official law enforcement operations to respond to unlawful activities or support investigations will be retained for evidentiary and/or forensic purposes, and evidence destruction is directed or completed by the evidence custodian following the adjudication of the case, receipt of a court order, or as part of evidence inventory management. Procedures for disposal/destruction of evidentiary records is specified in DOI policy.

VSS does not maintain case files, and evidentiary record may be maintained in a separate system of records for temporary or permanent records based on the subject of the record, applicable NARA approved records disposition schedule, and the needs of the agency. Records may be retained and disposed by a receiving agency pursuant to the applicable SORNs and records schedule(s).

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

After the retention period has passed, temporary records are disposed of in accordance with the applicable records schedule and DOI policy. Disposition methods include pulping, shredding, overwriting, erasing, and degaussing in accordance with Departmental policy. For the VSS, transitory, non-evidentiary footage is overwritten after 30 days. Permanent records that are no longer active will be transferred to the National Archives for permanent retention in accordance with NARA guidelines.

Records documenting incidents, investigations, or activities requiring retention as evidence are exported as a hashed copy and provided to the appropriate evidence custodian. Evidence destruction is directed or completed by the evidence custodian following the adjudication of the case, receipt of a court order, or as part of evidence inventory management. Procedures for disposal/destruction of evidentiary records is specified in DOI and NPS policy.

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

The privacy risks to individuals are considered moderate due to the PII collected, and VSS is rated as a FISMA Moderate system. Information access and retrieval through electronic means follows defined application security roles and permissions to ensure proper distribution and disclosure of information guided by the principle of least privilege to minimize the risk of improper information disclosure. The protection and maintenance of information for recovery and backup purposes is done following NPS data center policy and process for backup and retention of information. Disposition of all information are guided by the NPS records retention schedules for systems that manage information.

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, signs for areas that use VSS may be posted, and the NPS Policy Statements posted on National Park websites. Cameras are located in public areas where there is no reasonable expectation of privacy and no violation of the law. For use of video recordings, individuals who enter on Federal properties and public areas do not have a reasonable expectation of privacy. The NPS encourages public comments regarding its VSS policy and procedures contained in this policy, which we will periodically re-examine, and which is a matter of public record and discussion.

There are privacy risks related to unauthorized access to the system or data, inappropriate use, disclosure of information to unauthorized recipients, or that information may be used outside the scope of the purpose for which it was collected. NPS personnel with access to recorded material and digital evidence will be subject to strict NPS policy, bureau policy, and privacy control standards. Only authorized personnel with proper credentials can access the records in the system. NPS requires two-factor authentication for network access. System access is based on least privilege access and role-based access controls. NPS employees and contractors must take privacy, security, records management, Section 508, Paperwork Reduction Act, and Controlled Unclassified Information training prior to being granted access to NPS information and information systems, and annually thereafter. Personnel with significant privacy responsibilities must also take role-based privacy training initially and annually to ensure an understanding of the responsibility to protect privacy. Disclosure of sensitive information or PII to unauthorized recipients, failure to protect PII, mishandling of PII or misuse of PII may result in criminal, civil, and administrative penalties. Risk is also mitigated through system configuration controls that limit or prevent access to privacy information.

There is a risk of unauthorized sharing or loss of data or data integrity related to external sharing of data with other Federal, state, Tribal, and local law enforcement, security, and emergency services organizations. PII may be shared 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 DOI. The authorized sharing of information in support of law enforcement activities is described in the routine uses published in the INTERIOR/DOI-10 SORN, which may be viewed at: https://www.doi.gov/privacy/sorn. Examples of controls to mitigate these risks include:

- Utilizing Secure File Transfer Protocols for transmission of information

- 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

Data may be shared under a cooperative agreement or during cooperative operations with these organizations and may include still images, video feeds, or downloaded video recordings. Systems are configured to prevent audio recording. Any joint operation or information sharing is in accordance with a Memorandum of Understanding or other sharing agreement in accordance with DOI policy. Recipients of data gathered by VSS are subject to Federal policy, regulations, and DOI policy governing use of VSS. Data sharing is accomplished via encrypted physical media delivered to and signed for by the receiving evidence custodian. Records may be retained and disposed by a receiving agency pursuant to their applicable records schedule(s).

There is a risk that the system may collect, store or share more information than necessary to achieve the NPS mission or the information will be maintained longer than necessary to accomplish a legitimate purpose or in accordance with an approved records retention schedule. This risk is mitigated by maintaining and disposing of records in accordance with a records retention schedule approved by NARA. Users are reminded through policy and training that they must follow the applicable retention schedules and requirements of the Federal Records Act. Only the images or video needed to support official law enforcement operations to respond to unlawful activities or support investigations will be retained for evidentiary and/or forensic purposes, and evidence destruction is directed or completed by the evidence custodian following the adjudication of the case, receipt of a court order, or as part of evidence inventory management. Procedures for disposal/destruction of evidentiary records is specified in DOI policy. Records may be retained and disposed by a receiving agency pursuant to their applicable records schedule(s). All other images or video not required for retention will be automatically overwritten or disposed of per NPS records retention policy.

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. NPS restricts the maintenance of images or video feeds not necessary for retention to the minimum necessary (30 days) in accordance with approved records retention schedules for routine surveillance, images and video recordings.

There is a risk that the use of the visual recording devices may restrict First Amendment protected activities like freedom of speech or association. The purpose for use of the visual recording devices is to detect and deter criminal activity and support law enforcement, security and emergency service activities on lands/areas governed by NPS, not to record or restrict individuals lawfully engaged in First Amendment protected activities. First Amendment demonstrations will not be filmed for the sole purpose of identifying and recording the presence of individual participants engaged in lawful conduct. First Amendment demonstrations may be recorded where rangers/officers encounter them during routine law enforcement, security, and emergency services activities. Only the images or video needed to investigate unlawful activities or support investigations and prosecutions is retained, including litigation holds which may be

relevant to a new or imminent legal case. All other images or video not required for retention will be automatically overwritten or disposed of per NPS records retention policy.

There is a risk that devices may collect more information than is necessary to accomplish law enforcement, security and emergency services purposes. The devices are used only by authorized personnel and only to support law enforcement, security, and emergency services purposes. Only the images or video needed to investigate unlawful activities or support investigations and prosecutions is retained. Video recording not related to an investigation is overwritten or disposed of every 30 days.

There is a risk of proactive release of visual information and/or that PII may not be redacted properly and that individuals identified may experience identification, misidentification, harm, inconvenience, or embarrassment. Proactive release may occur as deemed necessary by DOI or NPS to prevent harm to the public or to DOI, NPS or NPS personnel or contractors, or when authorized under the Freedom of Information Act (FOIA). DOI has established redress procedures through regulation and policy to ensure individuals are able to submit requests to amend inaccurate records. However, the period for redress in the VSS is extremely limited due to the short period of retention of 30 days for images considered as non-evidentiary. Images related to events or associated with case files may be maintained for longer retention periods in other systems of records, such as INTERIOR/DOI-10, which may be covered by other NARA approved records schedules. These records maintained in other systems of records may be subject to additional requirements or exemptions under the Privacy Act of 1974. Individuals have the opportunity to correct records through the redress process provided on the DOI Privacy and Civil Liberties website at https://www.doi.gov/privacy/privacy-civil-liberties.

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

Federal agencies are provided authority to maintain and collect PII in support of agency's mission. Information on individuals is necessary to support law enforcement, security and emergency services. The use of VSS is necessary for the collection, transfer, management, retrieval, sharing, redaction, release, and records management associated with evidentiary and non-evidentiary data in support of law enforcement, security and emergency services activities.

The intended use of the information collected is both relevant and necessary to accomplish the specific purposes of the system and will be used by Law Enforcement staff in daily operations to receive and facilitate emergency response to public and employee safety incidents in addition to assisting Law Enforcement staff in completing criminal investigations. Organization of historical data and the ability to immediately maintain and recall that information along with access to the related information systems will directly result in added safety to the public and park visitors as

well as law enforcement, security, emergency services and other NPS staff. This corresponds directly to the underlying mission of the park.

☐ No

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

☐ Yes

☒ No

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

☐ Yes

☒ No

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

☐ Yes: *Explanation*

☒ No

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

Not applicable. This system does not derive new data or create previously unavailable data about an individual through data aggregation.

F. Are the data or the processes being consolidated?

☐ Yes, data is being consolidated.

☐ 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:

When a video image is recorded, it shall be documented and stored in a secure location with controlled access that is limited to authorized personnel. Access to recorded images will be limited to authorized law enforcement and security personnel and park managers for law enforcement and public safety purposes, and to government attorneys and police managers for civil litigation and disciplinary purposes.

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

Access is restricted by a role-based and least privilege principles. Users will not have access to all data, but they will have access to the data required to perform their duties based on their roles and park unit or office. System administrators will assign levels of access. VSS supports law enforcement activities at NPS and shares PII with other Law Enforcement agencies as part of the information sharing environment, for the purpose of investigation, recordkeeping, and arrest and/or conviction for crimes committed on NPS lands and/or against NPS personnel.

System management staff may on occasion be required to view PII in the performance of their duties for troubleshooting or system maintenance purposes. Employee or contractor staff with privileged accounts will be subject to routine auditing to ensure compliance with policies and procedures for managing data confidentiality and integrity.

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

VSS is not a Privacy Act system; however, contractors are responsible for designing, developing and maintaining the system, and in accordance with DOI policies, Privacy Act contract clauses are included in all contractor agreements in accordance with and subject to the Privacy Act of 1974 and applicable agency regulations.

Contractor employees are required to sign the NPS's Rules of Behavior and complete security and privacy training prior to accessing a NPS computer system or network. Information security and role-based security training must be completed on an annual basis as an employment requirement. Contractor and/or contractor personnel are prohibited from divulging or releasing data or information developed or obtained in performance of their services, until made public by the Government, except to authorized Government personnel. Contractors are also subject to Federal Acquisitions Regulations (FAR) regarding sensitive data.

NPS contractor staff are required to undergo background checks as defined by NPS policy and procedures. Contractor staff access will be restricted to data on a need-to-know basis. Privileged

accounts will be audited, and authentication and other security and privacy controls will be enforced as defined in published procedures.

☐ 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

☒ No

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

☒ Yes

The purpose of VSS is to provide surveillance in support of law enforcement, security, and emergency services operations, investigations, and prosecutions. The nature of the system will include monitoring individuals as it provides law enforcement, security, and emergency services officials video recording capability to document activities on lands/areas governed by NPS. The content within the system can provide the capability to identify and locate individuals; however, the process for identifying individuals is conducted outside the VSS.

Additionally, system monitoring will target users with privileged accounts, such as system administrators who can change configuration settings or escalate access permissions or roles; however, login history is recorded for all users, and field history tracking is recorded for select data fields, including some PII data elements.

The video camera systems identify and monitor user activities within the system through audit logs. Audit logs automatically collect and store information about a user's visit. The system tracks IP addresses of initiator machines, and audit logs may be used to identify unauthorized access or monitoring.

☐ No

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

Digital information including video captured from VSS may be evidentiary in nature. The data collected may include physical attributes of an individual, vehicle information, associations with other persons, and other PII. Non-evidentiary digital media is transitory and destroyed.

Login history collects information for detecting and resolving authentication or login issues. This includes information for assisting users in accessing their accounts or for researching unauthorized access attempts. Information collected may include data such as time, verification

attempt ID, username, identity verification method, action attempted, status of the attempt, IP address, and location.

A minimum number of system administrators will be able to access platform configuration settings, and all platform configuration settings will be monitored for changes. All privileged accounts will be monitored and routinely audited.

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

Separation of duties, permission restrictions, and audit controls are implemented to prevent unauthorized monitoring. Procedures are published for granting accounts, and privileged accounts are routinely audited for compliance. Audio recording is prohibited and further prevents unauthorized monitoring.

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.

(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

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 USPP Chief of Police serves as the VSS Information System Owner and the official responsible for oversight and management of the security and privacy controls and the protection of the information processed and stored in the VSS. The Information System Owner and Information System Security Officer are responsible for addressing privacy rights and complaints, and ensuring adequate safeguards are implemented to protect individual privacy in compliance with Federal laws and policies for the data managed and stored within VSS, in consultation with NPS and DOI Privacy Officials.

These officials and authorized VSS personnel are responsible for protecting individual privacy for the information collected, maintained, used, shared and disposed of in the system, and for meeting the Federal privacy requirements. Senior law enforcement officers (Chief, Assistant Chief, Deputy Chiefs, Majors) are responsible for issuing appropriate guidance, establishing procedures, adhering to department and bureau policy, reporting violations and investigation of violations.

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 VSS Information System Owner and VSS Information System Security Officer are responsible for daily operational oversight and management of the security and privacy controls, for ensuring to the greatest possible extent that data is properly managed and that all access to the data has been granted in a secure and auditable manner. The VSS Information System Owner and Information System Security Officer are responsible for ensuring that any loss, compromise, unauthorized access or disclosure of PII is reported to DOI-CIRC and appropriate NPS and DOI

officials in accordance with DOI policy and established procedures, and appropriate remedial activities are taken to mitigate any impact to individuals in coordination with the NPS Associate Privacy Officer.

System administrators and contractors are required to report any potential loss or compromise to the Information System Owner and Information System Security Officer.

The senior law enforcement officer (Chief, Assistant Chief, Deputy Chiefs, Majors) is responsible for overseeing the video recording and storage system, ensuring compliance with NPS and DOI policies. Each bureau and office is responsible for ensuring that all employees with access to a system of records are aware of the privacy requirements concerning the handling, disclosure, and alteration of such records and the possibility of disciplinary action for improper disclosure. All NPS and DOI employees and contractors are responsible for safeguarding privacy, reporting any compromise of PII, and complying with Federal and Departmental privacy requirements.