U.S. Department of the Interior
PRIVACY IMPACT ASSESSMENT

Introduction

The Department of the Interior requires PIAs to be conducted and maintained on all IT systems whether already in existence, in development or undergoing modification in order to adequately evaluate privacy risks, ensure the protection of privacy information, and consider privacy implications throughout the information system development life cycle. This PIA form may not be modified and must be completed electronically; hand-written submissions will not be accepted. See the DOI PIA Guide for additional guidance on conducting a PIA or meeting the requirements of the E-Government Act of 2002. See Section 6.0 of the DOI PIA Guide for specific guidance on answering the questions in this form.

NOTE: See Section 7.0 of the DOI PIA Guide for guidance on using the DOI Adapted PIA template to assess third-party websites or applications.

Name of Project: National Fee Collection Point of Sale System (POSS)
Date: April 15, 2021
Bureau/Office: National Park Service
Point of Contact
Name: Felix Uribe
Title: NPS Associate Privacy Officer (APO)
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: *Information is NOT collected, maintained, or used that is identifiable to the individual in this system. Only sections 1 and 5 of this form are required to be completed.*

B. What is the purpose of the system?

The purpose of the National Fee Collection Point of Sale System (POSS) was to collect, process, remit, account for, and report on, recreation fees collected from visitors on-site at the National Park Service (NPS) fee-collecting sites, including entrance stations, campground and

backcountry offices, and visitor centers. It provided the Recreation Fee Program management the ability to quickly have access to fee revenue data and track revenue collected at locations where fees are collected; provided a means for collecting statistical information about park visitation; and tracked serialized/accountable stock (primarily park and interagency pass) inventory.

The POSS has been replaced by the Recreation Business Management System (RBMS) which has been assessed and documented under National Fee Collection Point of Sale (POS) System PIA (doi.gov).

The assets of the POSS system were disposed of in the following manner:

Software: The Scoria software ran on virtual machines hosted in the Denver data center. All virtual machines that comprised the system were decommissioned by the WASO Data Centers, and were decommissioned during the period 2020-01-20 through 2021-01-21.

Hardware: Hardware (point of sale devices) and peripherals were decommissioned and sanitized in accordance with DOI sanitization procedures.

Data: In production, the transactional data in the POSS system was hosted in a SQL Server database in the Denver data center. Upon decommissioning, this data was sanitized to remove NPS employee user information (there was never any visitor information in the database), and migrated into the NPS RBMS (Azure) environment. No PII was migrated to the RBMS database. The SQL Server database was decommissioned on 2021-01-12. PII remaining in the system was limited to employee cashier user name and has been destroyed.

Documentation: System and project documentation was archived (removed from the NPS Fee Collection Solutions SharePoint site) and is now stored for reference in the Recreation Fee Program Point of Sale Program SharePoint Site. This project documentation does not contain PII. The decommissioning plan provides details on the disposal of the information technology resources.

C. What is the legal authority?

Public Law 108-447 (118 Stat. 2809) Federal Lands Recreation Enhancement Act (REA)

D. Why is this PIA being completed or modified?

☐ New Information System
☐ New Electronic Collection
☐ Existing Information System under Periodic Review
☐ Merging of Systems
☐ Significantly Modified Information System
☐ Conversion from Paper to Electronic Records

☒ Retiring or Decommissioning a System
☐ Other: *Describe*

E. Is this information system registered in CSAM?

☒ Yes: *Enter the UII Code and the System Security Plan (SSP) Name*

UII: 010-000000553; POSS 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	**None**	N/A	**N/A**

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

☐ Yes: *List Privacy Act SORN Identifier(s)*
☒ No

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

☐ Yes: *Describe*
☒ No

Section 2. Summary of System Data

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

☒ Other: The POSS has been decommissioned. PII is no longer being collected or hosted in this legacy environment.

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: The POSS has been decommissioned. PII is no longer being collected or hosted in this legacy environment.

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

☐ Paper Format
☐ Email
☐ Face-to-Face Contact
☐ Website
☐ Fax
☐ Telephone Interview
☐ Information Shared Between Systems
☒ Other: The POSS has been decommissioned. PII is no longer being collected or hosted in this legacy environment.

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

The POSS has been decommissioned. PII is no longer being collected or hosted in this legacy environment.

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

☒ Within the Bureau/Office: The POSS has been decommissioned. PII is no longer being collected or hosted in this legacy environment.

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

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

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

☒ Contractor: *Describe the contractor and how the data will be used.*
The POSS has been decommissioned. PII is no longer being collected or hosted in this legacy environment.

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

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

☐ Yes: *Describe the method by which individuals can decline to provide information or how individuals consent to specific uses.*

☒ No: *State the reason why individuals cannot object or why individuals cannot give or withhold their consent.*

The POSS has been decommissioned. PII is no longer being collected or hosted in this legacy environment.

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

☐ Privacy Act Statement: *Describe each applicable format.*

☐ Privacy Notice: *Describe each applicable format.*

☐ Other: *Describe each applicable format.*

☒ 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 POSS has been decommissioned. PII is no longer being collected or hosted in this legacy environment.

I. Will reports be produced on individuals?

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

☒ No

Section 3. Attributes of System Data

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

The POSS has been decommissioned. PII is no longer being collected or hosted in this legacy environment.

B. How will data be checked for completeness?

The POSS has been decommissioned. PII is no longer being collected or hosted in this legacy environment.

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

The POSS has been decommissioned. PII is no longer being collected or hosted in this legacy environment.

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

The POSS has been decommissioned. PII is no longer being collected or hosted in this legacy environment.

The record retention schedule for fee collecting data is N1-79-08-9 Management and Accountability, retention plan C (Routine Fiscal, Contracting, and Purchasing Records), which requires destruction/deletion of records 7 years after closure.

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

The POSS has been decommissioned. PII is no longer being collected or hosted in this legacy environment. Approved disposition methods include degaussing or erasing for electronic records, in accordance with NARA Guidelines and 384 Departmental Manual 1.

Server hard drives remained within the NPS Data Center organizational control until destroyed on site. SAN storage in the NPS data centers was professionally disposed of in accordance with NIST guidelines. Storage devices were excessed and drives shredded in accordance with DOI policy or will receive sanitization, verification, and certification services. All tapes remained within the NPS Data Center's organizational control and were shredded based on DOI and NPS policies and procedures.

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 POSS has been decommissioned. PII is no longer being collected or hosted in this legacy environment.

There is a limited privacy risk for the decommissioning of the POSS infrastructure related to potential unauthorized access or mishandling of the residual data that remains in the POSS before it can be destroyed. PII was limited to employee cashier names and usernames, and was destroyed prior to migration to RBMS and deletion of the virtual machine. NPS professionally

disposed of data in SAN storage and shredded the backup tapes in accordance with DOI and NPS policy to mitigate this risk. NPS implemented physical, administrative and logical controls to protect the devices, equipment and any residual data from unintended or unauthorized access until final disposal. Prior to excessing, the residual data was located on the SAN devices and tape backups under the NPS Data Center control in secured NPS controlled facilities that are monitored 24 hours a day and are limited to authorized personnel with PIV card and password.

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

☒ No

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

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

☒ No

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

☐ Yes: *Explanation*

☒ 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?

The POSS has been decommissioned. PII is no longer being collected or hosted in this legacy environment.

F. Are the data or the processes being consolidated?

☐ Yes, data is being consolidated. *Describe the controls that are in place to protect the data from unauthorized access or use.*

☐ Yes, processes are being consolidated. *Describe the controls that are in place to protect the data from unauthorized access or use.*

☒ No, data or processes are not being consolidated.

G. Who will have access to data in the system or electronic collection? Indicate all that apply.

☐ Users
☐ Contractors
☐ Developers
☐ System Administrator
☒ Other: *Describe*
The POSS has been decommissioned. PII is no longer being collected or hosted in this legacy environment. Only authorized NPS personnel had access to the equipment and residual data pending final destruction.

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

The POSS has been decommissioned. PII is no longer being collected or hosted in this legacy environment.

I. Are contractors involved with the design and/or development of the system, or will they be involved with the maintenance of the system?

☒ Yes. *Were Privacy Act contract clauses included in their contracts and other regulatory measures addressed?*
Privacy Act contract clauses were included in the contract. In addition, all contractors with access to the system and/or data were required to have full NPS background investigations, NPS credentials, PIV cards, and government-furnished equipment (including data-at-rest pre-boot authentication) used to access the system.

☐ No

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

☐ Yes. *Explanation*

☒ No

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

☐ Yes
☒ No
The POSS has been decommissioned. PII is no longer being collected or hosted in this legacy environment.

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

The POSS has been decommissioned. PII is no longer being collected or hosted in this legacy environment.

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

The POSS has been decommissioned. PII is no longer being collected or hosted in this legacy environment.

N. How will the PII be secured?

(1) Physical Controls. Indicate all that apply.

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

The POSS has been decommissioned. PII is no longer being collected or hosted in this legacy environment. The decommissioning plan provides details on the disposal of the information technology resources.

(2) Technical Controls. Indicate all that apply.

☐ Password

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

The decommissioning plan provides details on the disposal of the information technology resources.

(3) Administrative Controls. Indicate all that apply.

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

The decommissioning plan provides details on the disposal of the information technology resources.

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 Associate Director for Business Services is the Information System Owner. The POSS Information System Security Officer manages the security controls in the system. These officials are responsible for ensuring appropriate security and privacy controls are implemented and managed in accordance with Federal and DOI policy. The NPS Associate Privacy Officer is responsible for addressing any privacy related complaints.

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 Associate Director for Business Services (Information System Owner) and Information System Security Officer are responsible for managing the security and privacy controls in the

system, and ensuring proper use of the system and data. These officials and the NPS Associate Privacy Officer are responsible for reporting any loss, compromise, unauthorized disclosure, or unauthorized access of privacy protected information to DOI-CIRC, DOI's incident reporting portal.