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: Recreation Business Management System (RBMS)
Bureau/Office: NPS Recreation Fee Management Program
Date: 4/29/2020
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, 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 Recreation Business Management System (RBMS) is a cloud-based Point of Sale (POS) system with on-site point of sale hardware (cash register, receipt printer, Personal

Identification Number (PIN) pad, etc.) that supports the collection of, accounting for, and reporting on user recreation fees from visitors at all NPS fee collection sites in order to increase the capacity for recreation fee management, increase the efficiency of the operation, and decrease the total cost of ownership of systems and equipment. It will replace all other point of sale equipment/systems in the National Park Service for over the counter (non-reservation-based) fee collecting activities.

User fees are paid by park visitors in the form of cash, checks, or payment (credit or debit) cards. RMBS enables a complete accounting of all fee payments. However, no privacy information on park visitors is retained in the RBMS. Payment card information used to process visitor payment transactions is encrypted automatically by the payment card PIN pad devices, and the encrypted information is sent to the payment card processor for authorization in accordance with Payment Card Industry (PCI) data security standards. The encrypted information is not accessible to NPS. Checks are manually collected and secured following the program-defined process for ensuring chain of custody and appropriate safeguards of paper financial instruments until the physical check is submitted to an appropriate financial institution or an electronic check is submitted to the Department of Treasury via the OTC.net. The NPS does not retain any version of the check either physical or electronic. The system consists of:

- Point of sale hardware terminals (running Windows 10 enterprise)
- Point of sale peripherals, including receipt printers, bar code scanners, encrypting payment card PIN pads, and cash drawers
- Point of sale software Microsoft Modern Point of Sale (MPOS), running on the Windows 10 hardware terminals
- Microsoft Dynamics 365 for Commerce, running as a Software as a Service (SaaS) tenant both for back-end processing and for management/reporting
- Microsoft Azure Commercial Cloud providing Federal Risk and Authorization Management Program (FedRAMP) authorized public cloud Infrastructure as a Service (IaaS) and Platform as a Service (PaaS)

Azure Commercial Cloud is FedRAMP-authorized at High Impact Level. High Impact data is usually in Law Enforcement and Emergency Services systems, Financial systems, Health systems, and any other system where loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals. FedRAMP introduced their High Baseline to account for the government's most sensitive, unclassified data in cloud computing environments, including data that involves the protection of life and financial ruin. [1]

C. What is the legal authority?

The Federal Lands Recreation Enhancement Act (FLREA), Public Law 108-447 (118 Stat. 2809), most recently extended on September 28, 2018 (P.L. 115-245, Div. C, §130).

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*
010-000001985 - System Security and Privacy Plan for NPS Recreation Business Management System

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

[1] Federal Risk and Authorization Management Program, 'Understanding Baselines and Impact Levels in FedRAMP', General Services Administration, https://www.fedramp.gov/understanding-baselines-and-impact-levels/, (accessed 16 November 2017).

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.

☒ Name
☒ Personal Cell Telephone Number
☒ Financial Information
☒ Home Telephone Number
☒ Credit Card Number
☒ Mailing/Home Address
☒ Other:

Park visitors may pay entrance fees by cash, payment card or check. Information collected from fee-paying park visitors may include:

- Check information may include name/s, address, personal phone number, and/or bank account number. Check information is not entered into the RBMS. Checks are manually collected and secured following the program-defined process for ensuring chain of custody and appropriate safeguards until the physical check is submitted to an appropriate financial institution and/or scanned into the Department of Treasury OTC.net system. The NPS does not retain any version of the check either physical or electronic.
- Payment card information used to process visitor payment transactions are encrypted automatically by the payment card PIN pads, and the encrypted information is sent to the payment card processor for authorization. Neither the RBMS nor NPS staff possess the decryption keys, and the information can only be decrypted by the payment card processor. Only an authorization token which does not provide any identifying information is stored in the RBMS. The NPS and RBMS comply with Payment Card Industry (PCI) control standards for handling of payment card information.
- Park visitors are not users of and do not have accounts in the RBMS.

PII for Government Employees, Contractors, and Volunteers or Partners (collectively, Government Users) is required for authentication, account management and logging purposes. This PII includes name, NPS email address, userid, telemetry identifier, and/or

NPS User Principle Name (UPN). Cashier Identifier is collected for fee collecting users, but the value of this field is the username.

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:

Park visitors may pay entrance fees by cash, payment card or check. Payment card and check information are collected from members of the public who present a payment card or check to an NPS Visitor Use Assistant (cashier) as payment for entrance or other recreational fees; however, neither the payment card information nor the check information are entered in the RBMS or retained by NPS, physically or electronically.

For Government Users, information is collected from the individual during onboarding or generated as DOI records (e.g. email address, UPN, username) during operational activities. To establish an account for a Government User, an authorized NPS manager emails (encrypted) a user account request to the Artic ticketing system. The RBMS system administrator creates the user account with the information provided, and the RBMS queries the Active Directory Federated Services to validate and complete the account creation.

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

PII collected from the general public is used to process fees to allow access to and use of park resources by members of the public. PII collected from the general public is limited to information encoded on the magnetic strip or chip on a payment card or printed on a check used for fee payment. Payment card information is immediately encrypted by the PIN pad device and transmitted to the card processor and is not stored in the RBMS. Check information is not entered in the RBMS and is handled manually outside the RBMS using the program-defined procedures for ensuring appropriate safeguards for chain of custody, accounting, and deposits.

PII collected from Government Users will be used by RBMS to securely authenticate individuals to the system, manage user permissions, and enable change and audit logging.

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

☒ Within the Bureau/Office: *Describe the bureau/office and how the data will be park used.*

The name of the Government User performing the transactions will only be used and shared for the following purposes:

- Shared with the employee's supervisory chain of command in the bureau fee collection program of the applicable employee, for purposes of basic accountability of funds collected, resolving shortages/overages/discrepancies in funds collected, and training.
- Shared with law enforcement in the case of a lawful investigation of criminal conduct surrounding fee collections (for example, suspected fraud).
- Shared with privacy and computer security personnel for auditing and incident management.

☐ 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.*

Systems provided by the United States Treasury's Bureau of Fiscal Service (https://fiscal.treasury.gov/) will be used to process visitor fees paid by payment card or personal check.

- Checks will be processed through the Over the Counter Channel Application (OTCnet). The OTCnet Privacy Impact Assessment is available at https://fiscal.treasury.gov/files/pia/otcnet-pclia.pdf. Dollar amounts are entered and/or checks are scanned into OTCnet to generate a deposit ticket. The resultant deposit tickets do not contain PII.

- Payment cards will be processed through Card Acquiring Services (CAS). The CAS Privacy Impact Assessment is available at https://fiscal.treasury.gov/files/pia/cas-pia.pdf.

□ 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.*

Contractors are responsible for the operations and maintenance of the software platform. Contractors need access to the platform to provide support and maintenance for the application. This maintenance is critical to protecting the system and the PII contained within the system. Azure, the cloud platform, maintains a Federal Risk and Authorization Management Program (FedRAMP) authorization and undergoes a security assessment by a third-party assessment organization each year.

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 procedures published on the RBMS Collaboration Portal.

□ 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.*

Members of the public may decline to provide PII by paying fees in cash. Members of the public are assumed to consent when offering a check or payment card when paying fees. NPS discourages the use of checks for fee payments.

For Government Users of the RBMS*,* PII is collected from Government Users who must use the system to perform the duties of their employee, contract or volunteer position. Government Users may decline to provide information during the onboarding process; however, this may result in reassignment to another position or a withdrawal of the offer of employment or opportunity to volunteer.

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

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.*

Privacy notice is provided through publication of this privacy impact assessment.

☒ Other: *Describe each applicable format.*

Government Users of the system must acknowledge the standard privacy and security notification banner before logging onto the system.

☐ None

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

Data collected from members of the public is not stored in the RBMS and cannot be retrieved in the system. The system CANNOT retrieve information on any identifier related to a member of the public, including name, payment card information and/or the information printed on a visitor's personal check,

Transaction data can be retrieved from the system by a Government User's cashier identifier, userid or username. A Government User's cashier identifier or username may also appear on reports retrieved by other identifiers, including:

- Transaction Date Range
- Park Identifier
- Shift Number

I. Will reports be produced on individuals?

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

No reports will be produced on members of the public.

Reports are produced on Government Users only. Reports of collections by cashier will be generated and used for employee evaluation (error rates – overages and shortages of collections) and fraud prevention and detection. All reports are access-controlled, and only Government Users with the appropriate need-to-know will be given access to the reports that include cashier employee name.

☐ No

Section 3. Attributes of System Data

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

Data collected from members of the public is not verified for accuracy by NPS; however, verification of payment card information is conducted by the card processor through Card Acquiring Services system, and check information is verified through the applicable financial institution before payment settlement and remittance of fees. The payment card and check information are provided directly by the individual who is responsible for accuracy of the data they provide. For Government Users, information is collected from the individual during onboarding or generated by NPS or DOI as DOI records (e.g. email address, UPN, username) during operational activities.

B. How will data be checked for completeness?

Data collected from members of the public is not verified for completeness by NPS; however, verification of payment card information is conducted by the card processor through Card Acquiring Services system, and check information is verified through the applicable financial institution before payment settlement and remittance of fees. The payment card and check information are provided directly by the individual who is responsible for completeness of the data they provide.

Government Users are responsible for ensuring the completeness of the data associated with their user accounts and content posted in the system. PII used for account creation is initially provided by the individual during onboarding. During the account creation process, the user account administrator will validate the account request against DOI Active Directory information, and incomplete data will result in an error preventing creation of the account. Incorrect data may prevent user authentication or may be identified by supervisors when reviewing activity reports. Users may contact the help desk for assistance to validate account information and follow published RBMS procedures to have the data updated.

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

Data collected from members of the public is not verified by NPS; however, verification of payment card information is conducted by the card processor through Card Acquiring Services system, and check information is verified through the applicable financial institution before payment settlement and remittance of fees. The payment card authorization process verifies that the payment card is current and not past its expiration date. The payment card and check information are provided directly by the individual who is responsible for ensuring the data they provide is current.

For Government Users, Fee Program Managers and contractor program managers are responsible for identifying employees or other government users whose duties or positions change or are terminated and (a) require a corresponding change in their system role or permission or (b) no longer have a need to access the system. Fee Program Managers are responsible for notifying system administration to affect the appropriate change/s using the established RBMS Access Management Procedures posted to the internal RBMS Collaboration SharePoint portal. Terminations are required to be escalated for immediate action within 24 hours of the effective date of termination, at minimum. Accounts are also periodically audited to ensure data is current.

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

All RBMS records are retained in accordance with the National Park Service Records Schedule, Management and Accountability (Item 10), which has been approved by the National Archives and Records Administration (Job No. Nl-79-08-9). The disposition for routine fiscal, contracting, and purchasing records is temporary and records are destroy/delete 7 years after closure. The disposition for routine housekeeping and supporting records is temporary and records are destroyed/deleted 3 years after closure.

No payment card information, check information, or PII on members of the public is retained in the system.

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

The approved disposition methods include shredding or pulping for paper records, and degaussing or erasing for electronic records, in accordance with National Archives and Records Administration Guidelines and 384 Departmental Manual 1. Detailed disposition procedures will be defined and published on the RBMS Collaboration Portal on SharePoint.

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

There are privacy risks related to hosting, processing and sharing of data, unauthorized access to records, or any inappropriate use and dissemination of information. These risks are mitigated through a combination of physical, administrative, and technical controls, many of which will be referenced in the System Security and Privacy Plan. Risk is also mitigated through system configuration controls that limit or prevent access to privacy information.

There is a risk that unauthorized persons could potentially gain access to the PII on the system or misuse the data. To mitigate this risk, access to data is restricted to authorized personnel who require access to perform their official duties. Access to administrative functions is strictly controlled. System administrators periodically review audit logs to prevent unauthorized monitoring. Government Users are required to accept rules of behavior when using the system. All users must have an account in the system and user authentication protocols are enforced based on the user's role and permissions, i.e. personal identity verification (PIV) cards, two factor authentication, two step verification. Government employees, contractors, and partners (collectively, Government Users) will be required to use two-factor authentication. Government Users will be authorized for their role and permissions using a formal process for ensuring least privilege access is maintained before their accounts are created in RBMS. Government Users will authenticate to RBMS using the applicable agency identity provider (e.g. Active Directory Federated Services for DOI) and their GSAccess issued PIV card.

The RBMS employs Transport Layer Security (TLS) technology to protect information in transit using both server authentication and data encryption. Platform and device level encryption have been deployed to encrypt data at rest. Other system security mechanisms have also been deployed to ensure data security, including but not limited to, firewalls, virtual private network, and intrusion detection.

There is a risk of unauthorized access to payment card information. To avoid this risk, payment card numbers and data used to process visitor payment transactions are encrypted automatically by the payment card PIN pads, and the encrypted information is sent to the payment card processor for authorization. Neither the RBMS nor NPS staff possess the decryption keys, and the information can only be decrypted by the payment card processor. Only an authorization token which does not provide any identifying information is stored in the RBMS. The NPS and RBMS comply with PCI control standards for handling of payment card information.

There is a risk that unauthorized persons could gain access to PII on paper checks. To mitigate this risk, checks are maintained under lock and key from when the visitor provides the check in payment to when the checks are deposited in the bank. Dual controls are used throughout the process of counting and depositing the checks, and physical controls may include the use of armored car services or law enforcement escort. No copies or images are made of the checks, and no PII is entered in the RBMS.

There is a risk that user PII may be inappropriately used or disseminated by personnel authorized to access the system or view records. The system uses audit logs to protect against unauthorized access, changes or use of data. Government Users are required to take annual mandated security, privacy and records management as well as role-based training where applicable and sign the NPS Rules of Behavior prior to accessing the system, conducting fee collection, or handling paper checks. Failure to protect PII or mishandling or misuse of PII may result in disciplinary actions and potential termination of employment, criminal, civil, and administrative penalties.

There is a risk that erroneous information may be collected. This risk is mitigated by validating information against DOI Access, authentication results, and activity report and audit log content.

There may be a risk associated with hosting the system with a cloud service provider. RBMS is hosted in the FedRAMP-authorized Microsoft Azure Commercial Cloud. The Azure Commercial Cloud is a partitioned instance of the software as a service (SaaS). Microsoft maintains FedRAMP authorization, and Azure undergoes an annual security assessment by a third-party assessment organization as well as providing periodic reporting on security vulnerabilities and related plans of action and milestones.

Microsoft Azure support personnel require access to the platform to provide support and maintenance but will not have access to the data and PII. This maintenance is critical to protecting the system and any PII contained in the system. A formal Assessment and Authorization for issuance of an authority to operate has been conducted in accordance with the Federal Information Security Modernization Act (FISMA), and the system has been rated as moderate, requiring management, operational, and technical controls in accordance with the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53. As part of continuous monitoring, continual auditing will occur to identify and respond to potential impacts to PII information.

There is a risk that information in the system will be maintained longer than necessary to achieve the agency’s mission or may be improperly disposed or destroyed. 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. Detailed procedures and automated scripts for data disposal/destruction will be developed and secured under change management. Contingency plans and procedures will be defined to ensure the ability to recover in the event of improper data disposal.

There is a risk that individuals providing information do not have adequate notice on how their PII will be collected or used. This risk is mitigated by the publication of this PIA.

Section 4. PIA Risk Review

A. Is the use of the data both relevant and necessary to the purpose for which the system is being designed?

☒ Yes: *Explanation*

The data are relevant and necessary for the collection of, accounting for, and reporting on user recreation fees from visitors at all NPS fee collection sites in order to increase the capacity for recreation fee management, increase the efficiency of the operation, and decrease the total cost of ownership of systems and equipment.

NPS offers members of the public the option to pay user fees in the form of cash, checks, or payment cards. Payment card and check information is relevant and necessary for executing secure fee payment transactions and for the convenience of the fee-paying members of the public.

Data on Government Users is relevant and necessary for enabling secure authentication to the system, tracking system configuration and data changes, managing system account permissions, and conducting activity reporting and auditing of fee-collection and system usage.

☐ 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?

Not applicable. The system does not derive new data about individuals.

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.*

This system entails the consolidation of transactional data that would normally only be collected in multiple separate systems (both electronic and paper-based) at a park level. Controls that are in place include:

- **Restriction of network access**: although cloud-based, the system will only be available from government-owned equipment on the DOI network with users who have authenticated to their devices via PIV.
- **Access control**: reports will only be available to users who have authenticated via PIV through Active Directory and been granted access to the reports based on the requirements of their job. All access is documented.
- **Cloud hosting**: System and data will be hosted in a FedRAMP-authorized High Impact public cloud environment.

No data on members of the public is consolidated by the system. Payment card and check information is not retained or consolidated in the system.

☐ 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:

For payments made by check, the information printed on the check will not be entered into the system; however, the check will remain in the custody of authorized NPS officials under lock and key until it is deposited in the bank. Checks are manually collected and secured following the program-defined process for ensuring chain of custody and appropriate safeguards of paper financial instruments until the physical check is submitted to an appropriate financial institution or an electronic check is submitted to the Department of Treasury via the OTC.net. The NPS does not retain any version of the check either physical or electronic after deposit.

For payment card transactions, only the Visitor Use Assistant (cashier) who processes the visitor's payment card transaction will have access to the visitor's payment card until the transaction is complete and the payment card is handed back to the visitor. The payment card number is immediately encrypted by the PIN pad device and transmitted to Card Acquiring Services for processing.

Payment card information used to process visitor payment transactions is encrypted automatically by the payment card PIN pad devices, and the encrypted information is sent to the payment card processor for authorization in accordance with Payment Card Industry (PCI) standards. The encrypted information is not accessible to NPS.

Data in the RBMS can only be accessed by authorized users, authenticated using a DOI PIV card and PIN. System administrators are authorized Government Users and have access for user account management purposes and technical support. Developers (contractors) will not have access to the production environment, therefore they will not have access to PII data in the system. Government Users may be assigned authorized user roles and must consent to and comply with the DOI and NPS access, training, and privacy requirements. NPS Fee Program Managers provide oversight and supervision of volunteers and contractors, and NPS personnel conduct periodic review of activity reports and audit logs.

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

Access will be restricted based on the principle of least privilege (that is, that each user will only have access to the reports and functions required to perform their duties). Specific standard operating procedures will be developed during system implementation; however, at minimum the following controls will be in place:

- Only Government Users will full background investigations, network access, PIV, and government-furnished equipment will have access to the RBMS.
- All reports will require specific authorization, with access levels and approval documented for each user and controlled by roles/permission authorization.
- All reports and access will be based on least-privilege and need-to-know.
- Shift and transaction-level reports (that include the cashier's name) will be restricted to the management chain of command for an individual park; summary-level data (that does not include individual transactions or cashier information) will be less restricted.

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?*

The design, development and maintenance contract/s included clauses for the following Privacy Act and regulatory measures:

- **Privacy Act:** "As prescribed in the Federal Acquisition Regulation (FAR) Part 24.104, if the system involves the design, development, or operation of a system of records on individuals, the contractor shall implement requirements in FAR clause 52.224-1, "Privacy Act Notification" and FAR clause 52.224-2, "Privacy Act.""
- **FedRAMP Security Compliance Requirements**:
  - Requirement for hosting in a moderate-level facility
  - Assessment and Authorization
  - Reporting and Continuous Monitoring
- **Payment Card Industry Data Security Standards (PCI DSS)**: "Point-to-Point Encryption (P2PE) credit card processing through Treasury Card Acquiring Services designated merchant processor (Vantiv) with a P2PE solution that will be accepted as out-of-scope for Payment Card Industry Data Security Standards (PCI DSS) by the NPS Qualified Security Assessor (QSA) and Vantiv."

☐ 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. *Explanation*

The system does not provide the capability to identify, locate or monitor members of the public. PII collected from members of the public is not retained in RBMS.

The system provides the capability to identify, locate and monitor Government Users only as follows:

a. For security purposes, login history is recorded for all users, and field history tracking is recorded for select data fields, including some PII data elements.
b. Fee-collection transactions and report activity identify the user executing the transaction and may indirectly identify the location of the user. This monitoring supports reconciliation and audit reporting of fee-collection revenue.
c. Privileged account (e.g. system administrators) activity is identified and routinely audited to ensure system and data privacy and security and to prevent unauthorized system and data use or monitoring.

□ No

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

The system does not monitor members of the public.

Limited monitoring of Government Users is conducted to ensure data and system integrity and security as detailed below:

a. Fee-collection transactions capture the cashier identifier (username), date, time, and register id of the Government User. The register ID could provide location information on the user when identified to a device in a physical location. No information is recorded on the visitor (fee paying) or the payment method (e.g. payment card).

b. Record and field level change tracking will be applied to sensitive data elements or elements that, if subject to unauthorized change, could present a risk to identity authentication or to the mission or business process.

c. Login history collects information for detecting unauthorized login attempts and/or 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, date, verification attempt ID, username, identity verification method, action attempted, status of the attempt, and location.

d. A minimum number of system administrators are 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. System configuration is under change management and monitoring to prevent unauthorized changes or monitoring of individuals. Any configuration change is stamped with the userid of the person making the change along with information about values that have been changed.

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. All access to the system, including the generation of reports, creates an audit log entry. Periodic review of report generation will be performed by the Information Systems Security Officer, along with other auditing bodies to verify that reports are being generated in accordance with policy.

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. *Describe*

(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*

(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*

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 Recreation Fee Program Manager serves as the RBMS 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 RBMS. 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 RBMS, in consultation with NPS and DOI Privacy Officials.

P. Who is responsible for assuring proper use of the data and for reporting the loss, compromise, unauthorized disclosure, or unauthorized access of privacy protected information?

The RBMS Information System Owner and RBMS Information System Owner 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 RBMS 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.