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: Enterprise Facility Management Software System (EFMSS)
Bureau/Office: NPS/Park Facility Management Division (PFMD)
Date: August 10, 2021
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: *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?

Enterprise Facility Management Software System (EFMSS) is an asset and work identification, planning, and management system that supports the DOI and NPS enterprise asset management programs, mission requirements, and applicable Executive Orders and Director Orders. The EFMSS is managed by Park Facility Management Division (PFMD), a division within the National Park Service/ Park Planning, Facilities, and Lands directorate. EFMSS is used to record labor, manage work orders, track the condition of assets, and support the NPS PFMD in efficient work planning and execution. EFMSS is a combination of the Facility Management

Software System (FMSS) as its core system, over a dozen interfacing component applications/subsystems and additional interfaces with external systems. FMSS is an NPS customized version of IBM Maximo® COTS software. The component applications/subsystems are primarily Cold Fusion based, and were custom built to perform specialized functions not included in FMSS. Additional external interfaces with the Federal Personnel and Payroll System (FPPS)/QuickTime and the Financial and Business Management System (FBMS) exist. The FPPS/QuickTime interface supports the bi-weekly transfer of actual hours entered on FMSS Work Orders to QuickTime, thereby streamlining data entry and reducing the need for duplicative entries in two systems. The FBMS interfaces transfer data between FBMS and FMSS and support accounting, financial and Federal Real Property reporting. This PIA covers all of the systems, components and interfaces of EFMSS described above.

EFMSS assists NPS facility managers in developing a plan for and managing inventory assets, determining the condition of the asset, planning work to bring the asset into a better operating condition, and identifying obsolete assets in the inventory. The asset information includes, but is not limited to, documenting 1) specific data such as quantities, locations, etc. and 2) the entire life-cycle of each asset throughout the NPS including acquisition, maintenance, operations, component renewal, rehabilitations/repairs, capital improvements, sustainment and demolition. Typical program information includes but is not limited to asset management, environmental, accessibility, transportation, concession, housing, fleet, roads, projects, dams, lands, natural, cultural, heritage, planning, interpretive, structural fire, contracting, budget and funding information.

Currently, the EFMSS subsystems include maintenance management software, cost estimating software, multiple interfaces, multiple databases, and multiple web applications in place for developing and storing data related to specific asset data, the life-cycle of each asset and specific program information. The software and applications that comprise the subsystems are supported by platform, hardware, computers, servers, etc. and are listed below in the table found in section 1F.

EMSS systems include information about two types of individuals: Facility Labor Staff and NPS Users. Facility Labor staff are DOI authorized employees, contractors, and volunteers (collectively, Facility Labor Staff) who perform work on NPS facilities and include individuals such as carpenters, electricians, engineers, trail workers, etc. NPS Users are NPS authorized employees, contractors, and volunteers (collectively, NPS Users) who have one or more EFMSS system account, (collectively, NPS Users) who use the system(s) for its specified purpose according to their roles(s) such as regular system users, system administrators and managers, etc. A Facility Labor Staff may or may not also be a NPS User. More information about these two groups is provided below.

EFMSS systems include information about Facility Labor Staff so that their hours worked on NPS facilities can be planned, managed and tracked on Work Orders. Unique identifiers called “Labor Code” and “Person Code” are created when Facility Labor Staff are entered in EFMSS for the first time. Additional attributes such as assigned park and work orders are added and updated as applicable. It is common for Facility Labor Staff to transfer to other parks or be assigned to work orders at parks other than their designated parks.

EFMSS systems include information about NPS Users so that their access to those systems can be enabled. NPS Users provide the information through voluntary self-registration via the FMSS User Management Process (FUMP) using DOI Active Directory username. FUMP allows NPS users to select systems, roles and levels of access in FUMP, which are later approved/rejected by Park Account Managers (PAMs), or approvers at regional or NPS-wide levels, as appropriate. Access to EFMSS systems is through the use of the Personal Identity Verification (PIV) Credentials and DOI Active Directory using User Principal Name (UPN) or UserID attributes for authentication and role/permission management, or two factor authentications in most cases. DOI users must complete a background check, are required to sign the DOI's Rules of Behavior, and must complete security and privacy training prior to accessing a DOI computer system or network.

C. What is the legal authority?

54 U.S. Code § 101301 - Maintenance management system; Section 4(a) of Public Law 98-540, October 24, 1984 Amendment to the Volunteers in Parks Act of 1969.

EO 13327, February 4, 2004 Federal Real Property Asset Management.

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: 010-000000578, SSP Name: Enterprise Facility Management Software System (EFMSS) 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.*
Facility Management Software System (FMSS)	FMSS is the core system collecting information on planning and managing work and associated costs of facilities assets including information about work performed on NPS facilities by Facility Labor Staff.	Yes	Name, work address, work phone, NPS email, title, park, work group, supervisor, regular and premium hours worked, craft code, termination date of Facility Labor Staff. Stores UPN, first name, last name, NPS email, work phone of NPS Users.
Asset Management Reporting System (AMRS)	The reporting subsystem for asset management decisions and NPS mandatory reporting requirements. It does not collect PII, but reports PII from the FMSS core system including information about work performed on NPS facilities by Facility Labor Staff.	Yes	Name, work address, work phone, NPS email, title, park, work group, supervisor, regular and premium hours worked, craft code, termination date of Facility Labor Staff. Stores UPN, first name, last name, NPS email, work phone of NPS Users.
Work Order Reporting Kiosk (WORK)	The Work Order Reporting Kiosk is a subsystem that allows NPS staff to submit labor hours, tools, materials, and other costs to the Facility Management Software System without requiring users to access FMSS directly.	Yes	Name, work address, work phone, NPS email, title, park, work group, supervisor, regular and premium hours worked, craft code, termination date of Facility Labor Staff. Stores UPN, first name, last name, NPS email, work phone of NPS Users.
FMSS User Management Process (FUMP)	FUMP facilitates the user access request PAM approval process for EFMSS applications.	Yes	Stores UPN, first name, last name, NPS email, region,

			park, work phone of NPS Users.
Cost Estimating Software System (CESS)	Sage Timberline cost estimating tool for work orders and projects.	Yes	Stores UPN, first name, last name, NPS email, work phone of NPS Users.
• 35B Rate Tool • Audit Tracking • Asset Priority Index Web Site (API) • Exceptions List • FASAB Reporting • Housing Information Portal • Lead and Green Ammunition Survey • Optimizer Tool Portal • Roads Portal • Web Current Replacement Value Calculator (Web CRV)	Specialized function web application extensions to the FMSS enterprise system to address specific non-PII data collection and manipulation or re-assembly to enable specialized reports and improved reporting performance.	Yes	Stores UPN, first name, last name, NPS email, work phone of NPS Users.

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)*

Volunteer records are covered under DOI-05, Interior Volunteer Services File System, (May 23, 2001, 66 FR 28536).

Time and attendance records in Quicktime are covered under DOI-85, Payroll, Attendance, Retirement, and Leave Records (July 19, 2018, 83 FR 34156).

DOI Active Directory credentials are covered under DOI-47, HSPD-12: Logical Security Files (Enterprise Access Control Service/EACS) (March 12, 2007, 72 FR 11040). Please see these SORNs on the DOI SORN website at https://www.doi.gov/privacy/sorn.

☐ 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.

☒ Name
☒ Employment Information
☒ Other: *Specify the PII collected.*

For Facility Labor Staff, information collected includes Person/Labor Code, Work Location and Site (alpha code), Alpha Code Description, Status, Quicktime User ID, and Volunteer (checked if a nonpaid employee). The employee's Craft Code and Pay Rate are provided prior to posting any work order hours against the labor code. Additional information that may be collected includes; Bill to Park Location Address (this is a NPS address, not a personal address), City, Default Work Order Priority, Department, Drop Point, Employee Type, Hire Date, Ship to Address, State/Province, Supervisor, Supervisor Name, Termination Date, Time Zone, Time Zone Description, Title, Very Important Person, Work Address, Work E-mail, Work Phone, Zip/ Postal Code, Work Type, Crew, Seasonal Employee, Skill Level, Regular Hours, Premium Hours, Overtime Refused, and Vendor.

NPS Users use their government issued PIV authenticated through the Enterprise Active Directory (AD). The system collects the user's name, official email address, username, date of last login, and role or access levels 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 *Describe*
☐ Other: *Describe*

For Facility Labor Staff, PII related to labor hour transactions are transferred to the DOI Quicktime system. Data sent includes the Quicktime Userid, date worked, hours worked, FBMS funding information and standing parent work order number for each labor transaction.

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. The NPS User request access through FUMP which routes an approval request within the system to the appropriate PAM for acceptance and approval. Upon the user's account accessing the subsystem, EFMSS services communicate with Active Directory to authenticate and collect PII stored in Active Directory about the DOI user.

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

The PII is intended to be used to track availability and crew status of a person/labor for assignment on work orders. Once assigned to Work Orders, the PII is used to track a person/labor's work hours and costs on work orders for each labor transaction. The purpose of the system is to allow National Park Service employees to manage park facility inventory assets and provide a work management process for scheduling work, performing preventive maintenance and tracking the work performed on an asset. QuickTime IDs are collected for the purposes of sharing labor hours with the QuickTime application.

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 used.* EFMSS data is shared with PFMD park, region and Washington Area Support Office (WASO) level offices. The data is used to inform park management, work management and resources decisions throughout the NPS.

Other Region and WASO programs and offices may also use EFMSS information to inform program efforts as follows:

- Cultural Resources Office and Programs where cultural resources may be associated with or impacted by facilities maintenance and management activities.
- Structural Fire Offices and Programs when information about fire-related asset components is needed.
- Accessibility Offices and Programs when information about work on accessibility features of NPS facilities is needed.
- Housing Offices and Programs when information about work on NPS housing facilities and buildings where people sleep is needed.

- Transportation Offices and Programs when information about work on transportation related assets such as roads and bridges is needed.

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

For Facility Labor Staff, EFMSS sends labor hour transactions to the DOI Quicktime system, which is managed by the Interior Business Center, when the optional Import feature of Quicktime is used and actual hours have been entered on one or more work orders in FMSS or WORK prior to the end of the pay period. Data sent includes the Quicktime Userid, date worked, hours worked, FBMS funding information and standing parent work order number for each labor transaction. The purpose of data transfer is to minimize duplication of effort for the Quicktime user by leveraging the time entries made in FMSS or WORK to record hours worked.

Account creation and management data of NPS Users will be shared with DOI and its Bureaus and Offices through Active Directory. PII found in EFMSS may be shared with the DOI Office of the Inspector General (OIG) for official auditing purposes as required.

☐ 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.*

NPS may contract with other commercial organizations to provide application development, configuration and operations, and maintenance of EFMSS. Contractor staff will be 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 the System Security Plan and Privacy Plan. This maintenance is critical to protecting the system and the PII contained within the system. EFMSS performs tests on the annual mandatory Security and Privacy controls as well as a subset of controls selected by the NPS Information Technology Security Office (ITSO) as part of an annual Security control review. In addition, EFMSS completes an annual Security Assessment Plan (SAP) and Security Assessment Review (SAR) as part of the required control review. This maintenance, in addition to controls enforced as defined in the Privacy Plan, is critical to protecting the system and the PII contained within the system. Accounting of disclosures are maintained for the life of the record following the prevailing records retention schedule or for five years after the disclosure is made, whichever is longer, in accordance with the Privacy Act and DOI policy.

☐ 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.*

For Facility Labor Staff, 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. Additional PII such as hours worked and work site is collected from Facility Labor Staff during performance of work associated to work orders as part of the work tracking function of EFMSS.

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. PII is collected from NPS Users who must use the system to perform the duties of their employee, contract or volunteer position. NPS Users also provide the information through voluntary self-registration via the FMSS User Management Process (FUMP) using DOI Active Directory username.

Facility Labor Staff and NPS 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, with that determination made at the park or other level where the user will be performing his or her duties.

☐ 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.*

Notice is provided through publication of this PIA and the applicable published SORNs.

☐ 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.).

Information is retrieved by key word searches. Identifiers used to retrieve data include Labor/People code (system assigned unique identifier), First Name, Last Name, Display Name, Work Location/Site (alpha code), Alpha Code Description, Crew (work or person group) and/or Craft.

I. Will reports be produced on individuals?

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

Reports are produced on Facility Labor Staff to verify labor assignments, summarize utilization and labor reporting primarily at the park level, by park staff including supervisors. Reports containing information on individuals may include labor code, person code, name, work location (alpha code), estimated pay rate, supervisor, and hours posted to work orders. Reports are used for data auditing and resource tracking. Reports are available to all users of the AMRS, as well as users with appropriate access in WORK and FMSS based on approved permissions.

Reports are produced on NPS Users and are reviewed and analyzed weekly for inappropriate or unusual privileged and non-privileged user activity. Reports in the form of audit logs may include name, action such as "Access Requested", action details, application, role, access level, requestor, approver and approver role. Reports are used for auditing and system access tracking. Reports are available to FUMP users with appropriate access or may be provided to PAMS or other NPS staff or the DOI OIG on a need-to-know basis.

☐ No

Section 3. Attributes of System Data

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

For Facility Labor Staff, identity, job series, and work team information is collected from the individual during onboarding or generated by NPS or DOI as DOI records during operational activities. Facility Labor Staff may provide labor related information through email or direct communication with the appropriate NPS User. NPS Users are responsible for the accuracy of the information for Facility Labor Staff entered into the system.

For NPS users, information is collected from the individual during onboarding, generated by NPS or DOI as DOI records during operational activities, and/or self-provided during the systems access request process. NPS Users are responsible for the accuracy of the information entered into the system.

B. How will data be checked for completeness?

Completeness of labor information is at the discretion of the park unit and is not enforced by the system. Business practice is to collect the minimum information necessary to record labor transactions or for system access.

NPS 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. Incomplete data may result in an error preventing account creation or data entry. Incorrect data may also may be identified by supervisors when reviewing activity reports. Users may contact the help desk for assistance to validate account information and follow FMSS User Management Process 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).

Contact information and hours worked are obtained from employees and volunteers and are assumed to be accurate and current. PAMs are responsible to ensure that data collected for their park unit is current. PAMs responsibilities are documented in the EFMSS PAM Responsibilities Checklist.

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

EFMSS is used to record labor, manage work orders, track the condition of assets, and support the NPS work planning and execution. Due to the broad scope of these functions, there may be project work orders, labor related or other records that contain information on employees, contractors and volunteers that are covered by several records retention schedules. EFMSS records are retained in accordance with the National Park Service Records Schedule, Resource Management and Lands (Item 1) and Park Facility and Maintenance (Item 4), which have been approved by the National Archives and Records Administration (Job Nos. N1-79-08-1 and N1-79-08-3, respectively). The disposition of Park Facilities and Maintenance Program and Policy Records/Significant Design and Construction Projects, including records that document the design, construction, repair, restoration, or rehabilitation of buildings, roads, and other long-term structures on NPS land, is permanent. The disposition of Cultural and Natural Resource Management Program and Planning records, including records / data documenting construction, restoration, or rehabilitation performed on a historic structure maintained as a cultural or natural resource, is permanent.

The disposition of Non-Permanent Park Facilities and Maintenance Program Records documenting the design, construction, restoration, repair, or rehabilitation of non-permanent and non-historic structures and Supporting Design and Construction Contract Documentation, excluding specifications, is temporary and are destroy/delete 15 years after closure.

The disposition of Non-Permanent Long –Term Resource Management and Land Records that document ongoing management, maintenance, preservation, modification, and rehabilitation of land and natural and cultural resources, including everyday construction and maintenance records for historic structures, is temporary. These records are destroy when no longer needed, but never before they are 10 years old.

The disposition of Routine Maintenance and Service Records for activities that do not materially changes permanent structures is temporary, and the records are destroy/delete 7 years after closure.

The disposition of records Short-Term Resource Management and Land records with short-term operational value and not considered essential for ongoing management of land, cultural and natural resources is temporary, including account management records, These operational records are destroy/delete 15 years after closure.

The disposition for routine housekeeping and supporting documentation is temporary and records are destroyed/deleted 3 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?

Workflows are in place to manage the disposition of permanent records in conformance with requisite retention schedules. Digital records, and their inherent machine-readable formats, will be transferred according to standards applicable at the time.

The approved disposition methods include degaussing or erasing for electronic records, in accordance with National Archives and Records Administration Guidelines and Departmental 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 is mitigated by limiting PII to official contact information, labor codes, and other project and labor related information. Sensitive PII is not collected or maintained in EFMSS. EFMSS is categorized as a moderate risk system; however, multiple controls have been implemented to mitigate and substantially lower privacy risks. Information acquisition and collection that is done through electronic means such as email, web applications, or shared between systems occurs on the NPS DOI network to minimize risk of data breaches while in transit and while stored. Information access and retrieval through electronic means such as information shared between systems or web applications 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 pertaining to natural resources and appropriate risk levels.

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 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 are referenced in the System Security and Privacy Plans. 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.

EFMSS enables access for NPS users through the use of the PIV Credentials and DOI Active Directory using User Principal Name (UPN) or UserID attributes for authentication and role/permission management. NPS users must complete a background check, are required to sign the DOI's Rules of Behavior, and must complete security and privacy training prior to accessing a DOI computer system or network.

Transport Layer Security (TLS) technology is employed to protect information in transit using server authentication. Device level encryption has been deployed to encrypt data at rest on laptop computers. Other 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 data interception in transit between EFMSS and Quicktime. This risk is mitigated by encryption of data in transit.

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. Federal employees and contractors 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. 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 allowing individuals to access and update only their records in the system. For NPS user accounts, this risk is further mitigated by validating information against DOI Active Directory, authentication results, and activity report and audit log content.

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 information including PII may be output from EFMSS to physical media and improperly secured or disposed. All PII information including reports is access-controlled, and only NPS staff with the appropriate need-to-know will be given access. DOI mandates that all

Federal employees and contractors complete initial and annual information security and privacy training. The resulting high awareness provides an enhanced level of assurance on the life cycle management of the PII data. Physical media including printed reports is manually collected and secured following the program-defined process for ensuring chain of custody and appropriate safeguards until the physical media is disposed of by shredding or pulping for paper media or erasing or degaussing for electronic physical media.

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, SORNs, and Privacy Act Statements within the application.

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 information is directly relevant and necessary to accomplish the purpose of managing park facility inventory assets and providing a work management process for scheduling work, performing preventive maintenance and tracking the work performed on an asset.

☐ 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. EFMSS 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. *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*

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

Determination of access to data by a user is made by the PAM when authorizing account permissions. Access will be restricted for all users. Each user will be assigned permissions, groups of permissions may be used to define a user's role. The permissions will determine what functions the user may execute in the system and define what records the user can create, read, edit or delete.

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. *Were Privacy Act contract clauses included in their contracts and other regulatory measures addressed?*

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, Public Law 93-579, December 31, 1974 (5 U.S.C. 552a) and applicable agency regulations.

Contractor employees are required to sign the DOI's Rules of Behavior and complete security and privacy training prior to accessing a DOI 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) with regard to 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. *Explanation*

☒ No

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

☐ Yes. *Explanation*

☒ No

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

For Facility Labor Staff, monitoring may include "Labor Utilization" reports. Pre-defined reports available in AMRS offer a variety of parameters to list (summary and detailed) labor associated with workorders and include hours, costs and locations for the labor. These reports are available to inform park management on recorded labor, manage work orders, track work completed affecting the condition of assets, and support the NPS in efficient work planning and execution.

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

EFMSS is not intended for monitoring users, however, the system does identify and monitor both Facility Labor Staff and NPS User activities within the system through reports and audit logs. Reports display laborcode, name, regular hours, premium hours, date, location and park. Audit logs automatically collect and store information about a user's login including UPN, identity verification method, action attempted and the status of the attempt, as well as create/update/delete activities performed by users to support user access controls, troubleshooting, and incident response support. Audit logs may also be used to identify unauthorized access or monitoring.

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.

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 Chief, Park Facility Management Division serves as the EFMMS 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 EFMMS. 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 EFMMS, 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 EFMSS Information System Owner and EFMSS 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 EFMSS 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.