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: Planning, Environment and Public Comment (PEPC) System
Bureau/Office: National Park Service, Natural Resource Stewardship and Science Directorate, Environmental Quality Division, Environmental Information Management Branch
Date: March 12, 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, 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 National Park Service, Natural Resource Stewardship and Science (NRSS) Directorate's Planning, Environment and Public Comment (PEPC) system is a collaborative online tool designed to: 1) facilitate the project management process in conservation planning and environmental impact analysis, 2) assist NPS employees in making informed decisions regarding

pertinent compliance issues throughout the planning, design, and construction process; 3) provide consistency in applying applicable policies, laws and regulations, and 4) provide a platform for public comment opportunities for environmental impact analysis and other documents that require public input.

PEPC is one system, but is accessed through two websites:

PEPC Secure Site - https://pepc.nps.gov - a secure site for DOI Active Directory (DOI AD) users and Non-DOI PEPC Users to conduct project planning and compliance activities; and

ParkPlanning - https://parkplanning.nps.gov - a public site where the public can find information on park projects/documents posted for public review and provide comment on those projects.

PEPC assists with national park planning activities by improving the overall tracking and management of project cost, schedule and scope; helping interdisciplinary team members collaborate on projects; tracking key milestones of projects; and increasing communication among project participants, both inside and outside the NPS.

PEPC assists with protecting the environment of national parks by increasing the efficiency of the compliance process; helping NPS employees prepare compliance documentation; simplifying communication, tracking, and scheduling of team members and activities; identifying and tracking mitigations; tracking environmental consultations; and helping everyone involved in the process to make better decisions.

The National Environmental Policy Act (NEPA), as implemented through NPS Director's Order 12: Conservation Planning, Environmental Impact Analysis, and Decision Making, requires NPS to involve the public in decision making. PEPC helps to meet these requirements by helping the NPS to communicate plans, meetings, and the status of projects via a public website; collect, analyze, and respond to public comment; and make project information available to the public in a single, easily accessible online location. The system facilitates continuity of information maintained and disseminated by the NPS and provided to the Department and other groups, such as the President's Council on Environmental Quality. It also provides a unified portal for public consultation and comment analysis.

Additionally, the public comment capabilities found in PEPC can be used by DOI, other DOI bureaus, and other federal agencies to meet public comment needs or mandates, such as for environmental planning, policy planning, rule-making, and natural resource damage assessment planning and restoration. PEPC has been used extensively for providing opportunity for public comment for the Deepwater Horizon Oil Spill restoration projects and Restore the Gulf documents.

PEPC enables access for DOI authorized employees, contractors, and volunteers (collectively, DOI AD Users) through the use of Personal Identity Verification (PIV) Credentials and DOI

Active Directory using User Principal Name (UPN) for authentication. 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.

Users from other federal agencies, local governments, tribal organizations, and other authorized project participants (collectively, Non-DOI PEPC Users) may request user account from PEPC administrators. PEPC provides multifactor authentication using a valid e-mail account and a temporary encrypted account confirmation code to allow the user to specify a unique username. Non-DOI PEPC Users authenticate by means of username/email address and password. Non-DOI PEPC Users must complete annual security and privacy training, including signing DOI's Rules of Behavior, to maintain account access.

Unregistered members of the public (Anonymous User/s) access is only enabled for the ParkPlanning site. Users can access data and documents that have been approved for sharing with the general public and excludes PII without the need for a user account or signing in. PII may be entered by Anonymous Users in the process of commenting on a proposed action.

The NPS Project Management Information System (PMIS) can pull PEPC project information for linked PEPC projects that includes: PEPC project number, project title, compliance information, and NPS project leader contact information. This is done by using a datalink to the secure PEPC database that was created by PEPC development staff.

C. What is the legal authority?

42 U.S.C. 4321, The National Environmental Policy Act of 1969, as amended; and 43 CFR Part 46, Implementation of the National Environmental Policy Act of 1969.

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 Code: 010-000000569

SSP Name: Planning Environment & Public Comment 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

None. PEPC is a single database system with two interfacing websites: a secure site for DOI AD Users and Non-DOI PEPC Users and a public site for Anonymous User public information access review and comment submission (see Section 1(B)).

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)*

NPS-23, Planning, Environment and Public Comment (PEPC) System, 79 FR 30641 (May 28, 2014) (SORN is under revision.)

DOI-21, eRulemaking Program, 85 FR 33701 (June 2, 2020)

DOI-05, Interior Volunteer Services File System, 66 FR 28536 (May 23, 2001)

DOI Active Directory credentials are covered under: DOI-47, HSPD-12: Logical Security Files (Enterprise Access Control Service/EACS) 72 FR 11040 (March 12, 2007)

☐ 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

☒ Personal Email Address
☒ Group Affiliation
☒ Mailing/Home Address
☒ Other: *Specify the PII collected.*

PII is stored in PEPC primarily for (1) creation and management of user accounts and to allow DOI AD Users and Non-DOI PEPC Users to interact with NPS; (2) listing the members involved in a project and their area of responsibility; and (3) allowing correspondence with members of the public who comment on a project.

For the purpose of creating a user account, DOI AD Users must provide business email address and the PEPC Secure Site will pull first and last name, UPN, and business phone number from DOI AD into PEPC.

Non-DOI PEPC Users must provide first and last name, business email address, and a self-selected username when creating an account in the PEPC Secure Site. They may optionally provide a business phone number.

Both DOI AD User and Non-DOI PEPC User information may be used to associate individuals with PEPC project roles, responsibilities, and tasks as Interdisciplinary Team (IDT) members.

Each correspondence received from an Anonymous User (the public) is assigned a unique identifier number that links a comment to a project and document in the system. The correspondent's unique identification number can be used to recall the correspondent's submitted comment and provided personal information (already noted in checkboxes above). A correspondent may enter first name, last name, organization, email, and address when submitting a comment. Only city, state, and postal code of the address are required in order to submit a comment.

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:

PEPC may electronically import public comments and associated information, including PII, from the Regulations.gov federal public comment site (privacy and security notice | SORN | PIA), when federal agencies involved in projects are mandated to utilize this system.

PII may be present in metadata (author, reviewer, editor, or project participant as part of a citation) in electronic documents or records submitted to the PEPC site by DOI AD Users and Non-DOI PEPC Users in the process of conducting compliance. These documents may originate from other agencies and may contain PII.

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*

PEPC Secure Site user details are collected by authorized system representatives (park administrators, regional administrators, or PEPC support staff (superusers)) via email, face-to-face contact, or telephone to create a user access profile.

For DOI users, user profile name, email, and username are synchronized with DOI Active Directory (AD) upon creation.

PII from the public may be submitted via web form on ParkPlanning or by scans of emails, faxes or hard copy letters received. Scanned documents may be entered into PEPC and become a part of the project record for the responsible agency conducting the project and follow agency-defined records management procedures.

PEPC may electronically import public comments and associated information, including PII, from the Regulations.gov federal public comment site (privacy and security notice | SORN | PIA), when federal agencies involved in projects are mandated to utilize this system.

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

PII in the PEPC Secure Site is used to authenticate DOI AD Users and Non-DOI PEPC Users to the system, manage user roles and permissions, and enable change and audit logging. It is also used by the project team to facilitate communication and collaboration.

PII from Anonymous Users is used to provide copies or summaries of comments received on a project, to provide information to the public as a report or verification of all correspondence received for a project, as part of the process of reporting the public's concerns on a project and the NPS's response to those concerns, and may be used to facilitate subsequent communication to the individual about the project on which they commented.

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.*

DOI AD Users may share the public comment data (including PII) with NPS project team members and NPS management to meet needs or mandates, such as compliance with NEPA, the National Historic Preservation Act (NHPA), policy planning, rule-making, and natural resource damage assessment planning and restoration, or other activities, as necessary pursuant to the routine uses listed in the PEPC SORN.

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

PEPC DOI AD Users from other DOI bureaus, programs, or offices collaborating on or jointly managing NPS projects in the PEPC Secure Site, or who entered projects into the PEPC Secure Site in order to utilize its functionality, can access information entered or received for their project, including document reviews and public comment containing any voluntarily provided PII. They may share the public comment data (including PII) with project team members and management within their bureau, either within the PEPC Secure Site, or through comment analysis reports to meet needs or mandates, such as compliance with NEPA, NHPA, or other activities, policy planning, rule-making, and natural resource damage assessment planning and restoration, as necessary pursuant to the routine uses listed in the PEPC SORN.

DOI AD user and PEPC account user account information would only be shared with DOI in the event of a security incident.

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

Non-DOI PEPC Users may be from other Federal agencies and will have access to shared project information available through PEPC. These Federal agencies may be participants in NEPA documents as cooperating agencies when requested by the lead agency by virtue of jurisdiction or special expertise under 40 CFR 1501.8 NEPA Cooperating agencies. They may also be participating agencies or Federally mandated organizations, such as the Gulf Coast Ecosystem Restoration Council that was established by the Restore Act. Federal agencies who are joint or cooperating agencies on a project, or who entered projects into the PEPC system in order to utilize its functionality, can access information entered or received for their specific project including reviewing document and public comments containing

voluntarily provided PII. Non-DOI PEPC Users from other federal agencies are granted appropriate access to project information on a project-by-project basis, according to their role in the project. They could use voluntarily provided PII pursuant to the routine uses listed in the PEPC SORN for managing the project.

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

Tribal, State, or Local Agency staff can be granted specific project access to the PEPC system as Non-DOI PEPC Users to review only those specific projects, according to their role in the project. They use voluntarily provided PII only to collaborate and communicate on projects pursuant to the routine uses listed in the PEPC SORN.

☒ Contractor: *Describe the contractor and how the data will be used.*

Contractors are granted appropriate access to the PEPC Secure Site on a project-by-project basis, according to their role on the project, as either DOI AD Users or as Non-DOI PEPC Users. They may have access to PII for the project-specific work they were hired for, which could include project management, consultation, collaboration, communication, and comment analysis pursuant to the routine uses listed in the PEPC SORN.

NPS also contracts with commercial information technology (IT) organizations to provide application development, configuration and operations, and maintenance of the PEPC Secure Site and ParkPlanning. Contractor staff are required to undergo background checks as defined by NPS policy and procedures. Contractor staff have full access to the system, including public comments and any provided PII in order to assist NPS employees, other federal agencies, and contractors in performing comment analysis within the system, to manage user access, and to perform development, operations, and maintenance tasks. This maintenance is critical to protecting the system and the PII contained within the system.

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

Partner organizations executing a Cooperating Association Agreement with NPS may serve in a consultative role or be a party to a compliance effort and be granted access to the PEPC Secure Site as Non-DOI PEPC Users. The NPS may also share public comment data (including PII) directly with the organization in order for NPS to meet needs or mandates, such as compliance with NEPA, NHPA, or other activities, policy planning, rule-making, and natural resource damage assessment planning and restoration, as necessary pursuant to the routine uses listed in the PEPC SORN.

Private companies who have applied to NPS for permits on projects may access documents on the PEPC Secure Site to review and comment on those documents for accuracy and consistency with project objectives. NPS may share the public comment data (including PII) with these sources within the PEPC Secure Site in order for NPS to meet needs or mandates,

such as compliance with NEPA, NHPA, or other activities pursuant to the routine uses listed in the PEPC SORN.

NPS may share public comment PII with members of the public in order to provide copies or summaries of comments received on a project, and to provide information to the public as a report or verification of all correspondence received for a project, or as part of the process of reporting the public's concerns on a project and the NPS's response to those concerns pursuant to the routine uses listed in the PEPC SORN.

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.*

DOI AD Users must provide a business email address to a PEPC Park Administrator, Regional Administrator, or Superuser who enters the business email address into the PEPC Secure Site on their behalf to create a user profile. DOI AD Users whose business email address has a match in DOI Active Directory (AD) automatically have their first name, last name, phone number, and username queried from DOI AD Federated Services and entered into their user profile by the PEPC Secure Site.

For DOI AD Users this information from DOI AD is collected from the individual during onboarding or generated as DOI records (e.g., business phone, UPN) during operational activities. PII is collected from DOI AD users who must use the system to perform the duties of their employee, contract or volunteer position. DOI AD 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.

Non-DOI PEPC Users voluntarily provide information to a PEPC Park Administrator, Regional Administrator, or Superuser to establish an account. Anyone requesting access who declines to provide his or her name and business email address will not be granted access to PEPC.

Anonymous Users may voluntarily provide PII when they submit comments on ParkPlanning. The only required fields for an Anonymous User to provide a comment are City, State/Territory and Postal Code. Anonymous Users are cautioned before submitting comments or PII accompanying their comment that their information may be made publicly available (see Section 2G).

For data imported from Regulations.gov that site's PIA states "Yes, individuals do not need to submit any information they do not want to provide. Comments submitted are provided on a completely voluntary basis and it is up to the commenter as to what information is provided. The system informs users through a disclaimer notice that any contact information they provide is voluntary and will be published with their comments."

☐ 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.*

A Privacy Act Statement is posted on the ParkPlanning "Submit Comments" page and is available to all Anonymous Users who are providing comments through the system.

A Privacy Act Statement will be displayed on the PEPC "Create User" screen for the PEPC Park Administrator, Regional Administrator, or Superuser to send to the individual who is requesting the account.

☒ Privacy Notice: *Describe each applicable format.*

Notice is provided through the publication of this PIA and published system of records notice Planning, Environment and Public Comment (PEPC) System — NPS-23, which may be viewed at https://www.doi.gov/privacy/sorn.

☐ 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.).

Datasets are retrieved from both pre-generated and dynamic search results.

User profile information may be retrieved by first name, last name, email address, PEPC status (i.e. active or inactive), training status, park, or region for DOI AD Users and Non-DOI PEPC Users in a Search User Profiles feature in the PEPC Secure Site. User profile information may also be retrieved by region, park, role, and PEPC status in the Active User Details by Role report and by park, region, and PEPC status in the Inactive Users report.

IDT member name may be retrieved by region, park, project status, IDT member name, responsibility, project type, and project start date in the Projects by IDT Member report. IDT member name may also be retrieved by region, park, project ID, ID member name, responsibility, project status, task completion status, project type, NEPA type, division, task due

date, or task completion date in the Tasks by IDT Member report. IDT member name may also be retrieved by these identifiers and more in the Ad Hoc report.

Public comment data may be retrieved by park, project ID, document ID, correspondence ID, organization type, affiliation, or receipt date in the Demographics report.

I. Will reports be produced on individuals?

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

The PEPC Secure Site contains the following reports that are produced on individuals:

- Reports may be produced on government DOI AD Users and Non-DOI PEPC Users for purposes of account and incident management. All reports are access-controlled, and only DOI AD Users with the appropriate need-to-know will be given access to the reports.
- PEPC can produce reports on projects and tasks by IDT member to understand responsibilities, progress, and breadth of involvement.

☐ No

Section 3. Attributes of System Data

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

For DOI AD Users, information is collected from the individual during onboarding or generated by NPS or DOI as DOI records (e.g., email address, UPN, first name, and last name) during operational activities.

For Non-DOI PEPC Users, PII is collected from the individual during their voluntary account creation process and they are responsible for ensuring the accuracy of that information.

The only PII received from the public is voluntarily provided when submitting comments on a document posted on the public PEPC website. Comments received by email, fax or hard copy may contain voluntarily provided PII and are individually entered and uploaded into PEPC. The data is a point in time reference and is not checked for accuracy or updated. Public commenters are responsible for ensuring the accuracy of the data they submit.

B. How will data be checked for completeness?

For PEPC Secure Site users who are in the DOI Active Directory (AD), a work email address is entered on account creation and the remaining details are pulled from AD. DOI 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 and update account information.

For non-DOI PEPC Secure Site users, PEPC administrators are required to enter First Name, Last Name, Work Email, and Username in order to create an account based on the non-DOI user's input.

PII received from the public is voluntarily provided when submitting comments on a document posted on the PEPC website. Public correspondence can be submitted anonymously, as the name, address, and email address fields are not required. The only required fields are City, State/Territory and Postal Code. Comments received by email, fax or hard copy may contain voluntarily provided PII and are individually entered and uploaded into PEPC. The data is a point in time reference (i.e. comments are provided on a single document within a specific time window) and only validated for email address format and not checked for completeness or updated. Public commenters are responsible for ensuring the completeness of the data they submit.

The system performs security and validation checks to ensure the data provided is what is expected prior to accepting and storing the information. Users are warned of errors and given an opportunity to correct any issues found by the system.

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

PEPC Secure Site users on DOI AD may update their AD profile and changes will be reflected in PEPC during synchronization with DOI AD. Non-DOI users of the PEPC Secure Site may update their PII (except for Username) by editing their PEPC User Profile.

Data within project files in PEPC is owned by individual parks or regions. Information in the system is considered a "working file" and remains in the system as long as needed by the park to carry out official business. PEPC Secure Site users who are members of a project team are responsible for ensuring the data are current.

The PII received from the public is voluntarily provided when submitting comments on a document posted on the PEPC website. Public comments received by email, fax or hard copy are individually entered and uploaded into PEPC. The data is a point in time reference (i.e. comments are provided on a single document within a specific time window), applying only to the document on which the individual commented, and is not checked for completeness nor updated. Public commenters are responsible for the currency of the data they submit.

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

Records are retained in accordance with the National Park Service Records Schedule, Resource Management and Lands (Item 1C), which has been approved by the National Archives and Records Administration (Job No. N1-79-0801). The disposition of 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 destroyed/deleted 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?

Approved disposition methods for records include shredding or pulping paper records and erasing or degaussing electronic records in accordance with 384 Departmental Manual 1. Detailed disposition procedures and processes will be defined, implemented and published to internal system administration staff within the PEPC technical reference manuals.

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

The privacy risks to individuals are considered moderate due to the PII collected, and PEPC is rated as a FISMA Moderate system; however, multiple controls have been implemented to mitigate and substantially lower privacy risks. Information acquisition and collection may be done through means listed in 2.C., but data are entered into the PEPC system by electronic web forms over encrypted communication channels that comply with the required federal standards to minimize risk of data breaches while in transit. Information access and retrieval is done through electronic web forms over encrypted channels following 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. A formal Assessment and Authorization for issuance of an authority to operate is being conducted in accordance with the Federal Information Security Modernization Act (FISMA), and the system is 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 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.

There is a risk of unauthorized access to the system or public comment information, inappropriate use, or disclosure of information to unauthorized recipients. To mitigate this risk, access to files is strictly limited to authorized personnel whose official duties require such access. Paper records are secured in file cabinets in areas which are locked during non-duty hours. Electronic records conform to OMB and Departmental guidelines reflecting the implementation of the E-Government Act of 2002, National Institute of Standards and Technology Special Publication standards for Computer Security and the DOI regulations on safeguarding of Privacy Act information (43 CFR 2.226). Database tables are kept on separate file servers away from general file storage and other local area network usage. The data itself is stored in a password protected, client-server database. Electronic transmissions of records are encrypted and password protected. Security measures establish access levels for different types of users. Security controls have been implemented in the application to prevent unauthorized intrusion into the system, such as prevention of cross-site scripting and SQL injection attacks.

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.

Specific roles are assigned to PEPC Secure Site users. These roles create a separation of duties that ensure that each user can access only the pieces of data necessary for the users role. Users are granted roles using the “least privilege” access rule and can only access certain information via the tools in PEPC. Access to the complete database is restricted to PEPC support staff only. These measures apply to all secure site users.

User passwords are required to follow the security guidelines set up by DOI Office of the Chief Information Officer. These security guidelines include complex passwords, account lockout after three unsuccessful attempts, password expire after 90 days, no guest or generic usernames, etc. Audit logs are maintained of user creation, modification and deletion. For the secure site, the NPS General Support system regulations require all federal employees and users of NPS information systems to complete Federal Information System Security Awareness (FISSA) training, Privacy Awareness Training, Records Management and Section 508 Compliance training, and Controlled Unclassified Information (CUI) training before being granted access to the DOI network or any DOI system, and annually thereafter.as well as acknowledge the DOI/NPS Rules of Behavior. PEPC Secure Site users are also required to complete annual Role-Based Privacy Training (RBPT).

There is a risk of data interception in transit between PMIS and PEPC. This risk is mitigated through data encryption.

NPS may voluntarily release public comments, either in summary form, or full and complete public comments, including PII, to further the NPS mission. Release of individual information may occur under a FOIA request that includes the release of full and complete public comments. Under FOIA laws, regulations and guidance, the personal information of commenters responding to government solicitations for formal comments will be released absent exceptional, documentable circumstances.

For non-NPS documents in the system, comments are accessed by non-NPS users of the system. The comments on these documents are owned and controlled outside of the system by the responsible organization, and PEPC only acts as a tool to collect comments from the public. Therefore, release of public information by other Federal agencies follow their own Privacy Act policies and procedures. Non-NPS users of the PEPC System users are required to take DOI Privacy Act training, Role-Based Privacy Training, and other standard training. PEPC Park and Regional Administrators and PEPC support staff work with these parties to assure they are cognizant of the PEPC SORN NPS-23.

There is a risk that PII that is not relevant to the work of conducting compliance or collecting comments may be collected. Under the Privacy Act, NPS is required to minimize the use of PII, and to identify the minimum PII elements that are relevant and necessary to protect individual privacy and for the legally authorized purpose of collection. The PEPC Security Assessment Plan requires the PEPC System Administrator to conduct periodic evaluations to ensure the collection and maintenance of the PII is necessary and appropriate, as well as accurate, timely, and complete. The PEPC Administrator reviews the information in this PIA periodically and updates this PIA and the SORN as needed to meet this requirement.

There is a risk that user PII may be inappropriately used or disseminated by personnel authorized to access the system or view records. 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 users to access and update only their records in the system. For DOI user accounts, this risk is further mitigated by validating information against DOI Active Directory, authentication results, and activity report and audit log content. No sensitive PII is collected or managed by the system.

There is a risk that information including PII may be output from PEPC 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.

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.

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.

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 PEPC System is an integral part of meeting the NPS mission. The information in the PEPC Secure Site is critical for project communication and collaboration. PEPC utilizes the email functionality in the system as required by Director's Order 12, which requires an "Interdisciplinary approaches to problem-solving and decision-making [in park planning efforts]." Director's Order 12 also requires NPS employees to follow the legal requirements of NEPA and "be diligent in involving any interested or affected members of the public in the decision-making process [in park planning efforts]". The PEPC System also meets public comment requirements for projects undertaken under other laws and regulations, such as the Oil Pollution Act, Natural Resource Damage Assessment, and the Comprehensive Environmental Response, Compensation and Liability Act.

☐ 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?

N/A. There is no new data being created.

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?

Access is restricted for all users based on the assignment of roles. PEPC Secure Site roles are assigned by the Park or Region Administrators, or Superusers to grant specific roles and access to data in the system based on the "least privilege" access rule and an official "need to know." These administrators (park, regional, and PEPC staff) have the responsibility to change roles and

access for individual users when creating user profiles and as needs change (such as creation on new projects). Users cannot change their own roles and access.

Following the principle of least privilege, individual project access may be granted to those who only need to contribute to particular projects and may be limited to read-only access if the user is not expected to edit project information. Park-by-park access may be granted to all projects for a park, with roles for document reviewer, general user, public information user, and park administrator. Region roles may be granted that align with the park roles but cover all parks in a region. The Superuser role is assigned only to PEPC central office staff for the purpose of troubleshooting and system maintenance.

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 interfacing with the system and/or related data or providing services, administration or management are required to sign nondisclosure agreements as a contingent part of their employment. Contractor employees are also 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; however, no sensitive PII is collected or managed by the PEPC 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. *Explanation*

The PEPC Secure Site has rules in place to deactivate user accounts after periods of non-use or noncompliance with security practices/training and therefore records the date of last login for each PEPC user. Audit tables monitor changes to data in key tables, including the username of the editor; however, this information is only accessible by the PEPC Developer and the PEPC System Administrator.

The web server records login history, UPN, and other information to support user access controls, troubleshooting, and incident response support.

Auditing policies are for the purposes of data integrity and security per NIST SP 800-53.

☐ No

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

PEPC is not intended for monitoring users, however, the system does identify and monitor user activities within the system through audit logs. PEPC conforms to the DOI Security Controls standards with audit tables which collect secure system username, last successful login date, password reset date, password locked date, and an encrypted password that has been hashed and uniquely salted. PEPC completed an independent assessment in 2017 to assure that the system meets DOI security requirements, and security controls are periodically reviewed and updated. Audit tables are intended to manage changes to data made by a user for data integrity purposes and to record login attempts for security purposes. System interaction that results in system errors may also audit the details of the request/response involved in the error in order to correct system failures. Audit data is only recorded in these cases.

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

PEPC Secure Site users do not have access to monitoring; that function is only available to authorized PEPC support staff with approved elevated system access.

The PEPC System Administrator and contractors who develop and test the system are required to take annual Role-Based Security Training (RBST), Role-Based Privacy Training (RBPT), and FISSA Training.

Separation of duties, permission restrictions, and audit controls are implemented to prevent unauthorized monitoring.

N. How will the PII be secured?

(1) Physical Controls. Indicate all that apply.

☒ Security Guards
☒ Key Guards
☒ Locked File Cabinets
☒ Secured Facility
☒ Closed Circuit Television
☐ Cipher Locks
☒ Identification Badges
☐ Safes
☐ Combination Locks
☒ Locked Offices
☐ Other. *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, NRSS EQD, is the PEPC Information System Owner and the official responsible for oversight and management of the PEPC security and privacy controls and the protection of bureau information processed and stored in the PEPC system. Operation of PEPC is managed by the Chief, NRSS, EQD, Environmental Information Management Branch who is the System Manager for the system of records

The Information System Owner, Privacy Act System Manager, and the NPS Associate Privacy Officer, in collaboration with the NPS Associate Director for Information Resources, are responsible for ensuring adequate safeguards are implemented to protect individual privacy in compliance with Federal laws and policies for the data managed, used, and stored in the PEPC system. These officials, along with the System Owner and Privacy Act System Manager, and authorized personnel are responsible for protecting individual privacy for the information collected, maintained, and used in the system, and for meeting the requirements of the Privacy Act, including providing adequate notice, making decisions on Privacy Act requests for notification, access, and amendments, as well as processing complaints, in consultation with the NPS Associate Privacy Officer.

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 Chief, NRSS EQD, is the PEPC Information System Owner and the official responsible for oversight and management of the PEPC security and privacy controls and for ensuring to the greatest possible extent that agency data is properly managed and that all access to agency data has been granted in a secure and auditable manner. Operation of PEPC is managed by the Chief, NRSS, EQD, Environmental Information Management Branch and the System Administrator.

The Information System Owner and Information System Security Officer are also responsible for ensuring that any loss, compromise, unauthorized access or disclosure of agency PII is reported to DOI-CIRC, the DOI incident reporting portal 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.