Privacy Impact Assessment

for

Electronic Management of NEPA (eMNEPA)

Policy, E-Government and Fair Information Practices

Version: 3.0.0

Date: May 11, 2020

Prepared for: USDA OCIO TPA&E

Contact Point

Amy C Baker

System Owner

USDA Forest Service, NSG Branch Chief

(801) 975-3358

Reviewing Official

Cynthia Towers

Privacy Officer

USDA NRE Forest Service

(816) 844-4000

Abstract

The eMNEPA program is a U.S. Department of Agriculture (USDA) Forest Service (FS) e-Government (e-Gov) initiative. It is an incremental process modernization program, not a single tool or application. The eMNEPA program began in 2004 as an effort to “reduce the workload associated with National Environmental Policy Act (NEPA) compliance” using electronic communication, digital tools and improved process management. The mission is to improve the field’s effectiveness and reduce its administrative burden at completing NEPA activities by supporting compliance, efficiency, and sustaining knowledge. The purpose is to improve the effectiveness and efficiency of NEPA compliance activities within FS projects.

Overview

The reason that eMNEPA exists is because the USDA Forest Service is mandated to follow all legal requirements of the National Environmental Policy Act of 1963 (NEPA) and associated Clean Water Act and other environmental policies. The NEPA Services Group (NSG) located in Salt Lake City, UT, manages the Electronic Management of National Environmental Policy Act (eMNEPA) program with the Washington Office. The eMNEPA program enables the agency to comply with NEPA, National Forest Management Act (NFMA), and regulations and directives, which define required agency business.

Every forest tracks their NEPA projects in eMNEPA to create the mandated Schedule of Proposed Actions (SOPA). Agency NEPA regulations require the responsible official to ensure the SOPA is updated and to notify the public of its availability (36 CFR 220.4d). The ability of district and forest employees to produce complete administrative records improves the agency’s ability to respond quickly and accurately to litigation requirements.

eMNEPA has six components. The central eMNEPA component is called PALS (Project management, Administrative review and Litigation System); PALS is the main eMNEPA workspace for tracking and reporting NEPA projects, decisions and records, including project-related objections, administrative review and litigation. PALS is hosted within the FS ACE environment and will not be addressed further in this document.

Four eMNEPA components reside within Amazon Web Services (AWS) GovCloud. These applications are accessed via logging in to PALS.

CARA (Comment Analysis and Response Application) is the Agency's web-based solution for receiving, analyzing and responding to public comments; CARA standardizes and facilitates sharing information with the public. CARA

collects personally identifiable information (PII) from the public as part of the comment process.

DMD (Document Management and Distribution) is a back-end document storage and management service for eMNEPA applications. It streamlines creation, management and distribution of complete NEPA project files, and enables publishing NEPA information to the public web.

PRM (Project Record Management) is a project documentation storage and publishing application. PRM enables users to e-file project documentation with the EPA (a legal requirement).

MLM (Mailing List Management) assists NEPA staff with managing postal mailing lists.

These components will be addressed below for privacy impacts. The components may be stated as eMNEPA generically or individually when necessary but will still only represent the components which contain PII.

Section 1.0 Characterization of the Information

The following questions are intended to define the scope of the information requested and/or collected as well as reasons for its collection as part of the program, system, rule, or technology being developed.

1.1 Identification

What information is collected, used, disseminated, or maintained in the system?

NEPA requires public agencies to make diligent efforts to invite and solicit comments from the interested and affected public when planning significant actions that could affect federal lands. This information is voluntarily provided by the public when submitting comments on proposed projects and is stored in CARA.

PII collected by eMNEPA may include: Name, Street or mailing address, Email address, and Phone number.

1.2 Source

What is the source(s) of the information in the system?

Sources of the PII come from: information provided by the public when submitting comments on projects, information provided by the public when they request to be added to a mailing list to receive information about NEPA projects, and court records of appellants and litigants from the PALS application that are stored in DMD.

1.3 Justification

Why is the information being collected, used, disseminated, or maintained?

The information is collected, used, disseminated and maintained to:

Meet legal or policy requirements including NEPA

Meet FS obligations under the electronic Freedom of Information Act to publish final agency opinions on the Web (determined in a 1996 lawsuit by the Wyoming Outdoor Council against the FS)

Register and track any project objections and litigation plaintiffs or appellants

Contact members of the public who ask to participate in the NEPA process

Keep the public informed of proposed actions and changes to those actions Law 40 CFR 1506.6

1.4 Collection

How is the information collected?

eMNEPA Web Form - Comment Collection, Request to be added to the projects mailing list

Email - Comment Collection, Request to be added to the projects mailing list

Letter - Comment Collection, Request to be added to the projects mailing list

Public Meetings - Request to be added to the projects mailing list

PALS application - Appeals and Litigation information obtained from Court Records related to the project.

1.5 Validation

How will the information be checked for accuracy?

Names and contact information from public comments are entered directly by the general public. The eMNEPA system allows the public to provide accurate, inaccurate or no personal information at all with their comments. All comments are accepted per the NEPA process regardless of the quality or existence of contact information. The contact information is collected to fulfill legal requirements and to contact individuals if they request to be contacted. The NEPA program does not validate publicly provided contact information. The onus is on the information provider to ensure that the information is correct.

1.6 Authority

What specific legal authorities, arrangements, and/or agreements defined the collection of information?

Code of Federal Regulations – Title 7: Agriculture – 7 CFR 1.27

Code of Federal Regulations – Title 40: Public Involvement – 40 CFR 1506.6

Freedom of Information Act (Public Law 89-554, 80 Stat. 383; Amended 1996, 2002, 2007, 2016)

Wyoming Outdoor Council vs. Forest Service, 1996

1.7 Risk Mitigation

Given the amount and type of data collected, discuss the privacy risks identified and how they were mitigated.

Unauthorized access is gained to the system or to the database content that stores PII data. Existing access controls prevent unauthorized modification of data. Roles are tested and updated to ensure that users can only access data that they are intended to have.

PII data can be downloaded in reports/queries and stored on other systems not listed. PII from eMNEPA applications is downloaded into permanent project record folders; this is explained to the public in announcements that solicit participation. These records are stored in a FS repository (currently Box/Pinyon). Access to the project record folders is assigned on a need-to-know basis by Forest Environmental Coordinators and NEPA project managers to FS management and forest personnel working on NEPA activities. NEPA records stored in Pinyon are protected by the authorizations assigned to the folder in accordance with the FS PIA for Box/Pinyon.

When PII is printed from eMNEPA systems, are there user procedures in place for handling the information sent to the printers.PII is not printed from eMNEPA. Emails are not printed. They are maintained in Outlook and/or saved in pst files for storage in electronic project records.

Paper copies that contain PII information may be accessible to persons at the sight collected. Hardcopy letters are addressed and delivered directly to project personnel.

Members of the public may provide email addresses at a public meeting if FS personnel request it. A record of meeting attendees is created by FS personnel and retained in the project record; it serves as a record of persons who could have viewed individual email addresses. This process functions similarly to FOIA when contact information is released to interested persons who identify themselves.

All attendees may refrain from providing any personally identifiable information at public meetings; all persons are always provided the opportunity to provide their contact information via the public comment web form.

Section 2.0 Uses of the Information

The following questions are intended to delineate clearly the use of information and the accuracy of the data being used.

2.1 Usage

Describe all the uses of information.

Routine uses include:

FS District and Supervisor Office personnel conducting NEPA planning

FS Regional Offices conducting end-of-year reporting on appeals and litigation

FS Washington Office conducting evaluation of Regional planning projects

Public opportunity to download documents related to a particular project

CEQ - the Council on Environmental Quality for coordinating Federal environmental efforts, working with agencies and other White House offices in the development of environmental policies and initiatives

A component of the permanent project record

2.2 Analysis and Production

What types of tools are used to analyze data and what type of data may be produced?

Analysis tools are not part of nor provided by eMNEPA. eMNEPA reports can be used to obtain data for user analysis. Specific data can be downloaded via these reports and the data extracted for analysis by any external tool available to the user.

2.3 Commercial/Public Use

If the system uses commercial or publicly available data, please explain why and how it is used

eMNEPA contains commercial and publicly available research and geospatial data that is uploaded to PRM and analyzed by specialists as part of the NEPA analysis process to determine environmental impacts of proposed actions. This data does not contain any PII.

2.4 Risk Mitigation

Describe any types of controls that may be in place to ensure that information is handled in accordance with the above described uses.

All Forest Service employees have read-only access via e-Authentication to view eMNEPA data for work-related purposes. Designated Forest Service employees and contractors have role-based Administrator or Contributor access to eMNEPA PII data to upload, download and edit data, and grant access to additional users on a project-by-project basis. Direct access to the database is limited by Security Group, VPC, Subnet, and F5 settings in AWS by the Systems Administrator, who serves requests for account modification for developers to access eMNEPA.

When public comments are entered into eMNEPA, comments entered into the letter text box are published to the web. No PII entered into contact information form fields is published to the web. eMNEPA uses HTTPS to encrypt data before it is sent to the server. PII is unencrypted inside of eMNEPA because data inside the network utilizes the AWS network and security configuration to secure data.

eMNEPA has several audit tables that monitor user activity. HTTP requests are logged through AWS CloudWatch, IIS http logs, and on the CARA application server logs.

Paper documents submitted to units by the public are secured in locked filing cabinets at the unit when appropriate. This is not part of the eMNEPA system.

Section 3.0 Retention

The following questions are intended to outline how long information will be retained after the initial collection.

3.1 Time Period

How long is information retained?

All data entered remains in the system archive permanently or until disposed of per the appropriate NARA schedule for the type of project.

3.2 Approval

Has the retention period been approved by the component records officer and the National Archives and Records Administration (NARA)?

The retention period was approved in NARA schedule DAA-0095-2017-0001.

3.3 Risk Mitigation

Please discuss the risks associated with the length of time data is retained and how those risks are mitigated.

The risk of accidentally publishing PII entered into web form contact fields is mitigated by the system automatically masking the fields from publication.

There is no risk associated with the length of time the data is retained.

Section 4.0 Internal Sharing and Disclosure

The following questions are intended to define the scope of sharing within the United States Department of Agriculture.

4.1 Identification and Purpose

With which organization(s) outside of the Forest Service, but still within the Department of Agriculture is the information shared? What information is shared and for what purpose?

USDA OGC: Name, address, email, phone number, for litigation records

4.2 Delivery and Disclosure

How is the information transmitted or disclosed?

The information is sent to OGC staff in email attachments as part of legal briefs.

4.3 Risk Mitigation

Considering the extent of internal information sharing, discuss the privacy risks associated with the sharing and how they were mitigated.

Unauthorized access is gained during the sharing of data with internal organizations. Users ensure that records containing PII are sent only to those authorized to receive the information and are not widely distributed.

Section 5.0 External Sharing and Disclosure

The following questions are intended to define the content, scope, and authority for information sharing external to USDA which includes Federal, state and local government, and the private sector.

5.1 Identification and Purpose

With which external organization(s), outside of both the Forest Service and the Department of Agriculture, is the information shared? What information is shared, and for what purpose?

Congress: Name, address, email, phone number, to respond to congressional inquiry

DOJ: Name, address, email, phone number, for litigation records

Courts: Name, address, email, phone number, for litigation records

Tribunals: Name, address, email, phone number, for litigation records

BLM: Name, address, email, phone number, for litigation records

5.2 Compatibility

Is the sharing of personally identifiable information outside the Department compatible with the original collection? If so, is it covered by an appropriate routine use in a SORN? If so, please describe. If not, please describe under what legal mechanism the program or system is allowed to share the personally identifiable information outside of USDA.

eMNEPA collects and shares information about litigants/appellants with the general public and publishes this information on the relevant FS websites. All of the data collected falls under USDA/OCIO-03, Freedom of Information Act (FOIA) and Privacy Act (PA) Requests and Administrative Appeals Files.

5.3 Delivery and Security Measures

How is the information shared outside the Department and what security measures safeguard its transmission?

Legal records that contain PII are emailed in .zip file attachments to other agency legal staff personnel. Emails are sent only to agency personnel who need the information to perform their duties

5.4 Risk Mitigation

Given the external sharing, explain the privacy risks identified and describe how they were mitigated.

Unauthorized access is gained during the sharing of data with internal organizations. Litigation and Administrative Review staff ensure that records containing PII are sent only to those authorized to receive the information and are not widely distributed.

Section 6.0 System of Records Notice (SORN)

The following questions are directed at notice to the individual of the scope of information collected, the right to consent to uses of said information, and the right to decline to provide information.

6.1 Requirement and Identification

Does this system require a SORN and if so, please provide SORN name and URL?

(Note: If a SORN is not required, answer "No" to this question, and "N/A" for questions 6.2 through 6.5.)

Yes. USDA/OCIO-03, Freedom of Information Act (FOIA) and Privacy Act (PA) Requests and Administrative Appeals Files

6.2 Individual Notification

Was notice provided to the individual prior to collection of information?

Public project notices inform the general public of the opportunity to comment and contain a warning that information provided by the public is retained by the Forest Service in the project record.

The public comment web form contains a warning that contact information provided in the contact form fields not publicly visible but is retained as part of the project record, and information entered into the comment text box is publicly available.

Information to individuals is provided via:

The Federal Register for SORNs and legal authorities

Newspaper of record for regional, forest and district-level projects

The public comment web form Warning statement

6.3 Right to Decline

Do individuals have the opportunity and/or right to decline to provide information?

Yes. Public project announcements in the newspaper of record for regional, forest and district-level projects state that contact information is not required to comment; contact information is required only to retain legal standing to object

to the project. Individuals routinely provide anonymous comments for consideration without supplying any PII.

All contact information text fields in the comment web form are optional and do not need to be completed to submit comments. This is indicated by not having asterisks next to contact information fields and by the warning above the letter text entry box which states, “Do not enter any personally identifiable information (PII) such as address or email in the text editor below. Your name and all information entered into the text box below may be published on this website. Enter contact information in the form fields above.”

6.4 Right of Consent

Do individuals have the right to consent to particular uses of the information? If so, how does the individual exercise the right?

Public project announcements and the public comment web form state that information provided by the public will become part of the permanent project record. Individuals who do not consent to this use may submit anonymous comments. When persons submit a request to be contacted with further information about the project, their contact information may be added to a project mailing list in GovDelivery or eMNEPA specific to that project.

There are no other uses of personal information collected in eMNEPA.

6.5 Risk Mitigation

Describe how notice is provided to individuals, and how the risks associated with individuals being unaware of the collection are mitigated.

The following is a standard FS public comment solicitation.

Commenting on This Project:

Comments, including anonymous comments, will be accepted at any time. However, comments posted after the close of a designated comment period may not be able to be given full consideration. Anonymous comments and comments submitted after the close of the final designated comment period will not provide the commenter standing for administrative review.

The Forest Service values public participation. Communications from the public regarding this project, including commenters’ names and contact information, will become part of the public record.

Comments along with respondent's contact information submitted during the comment period may be necessary to establish a respondent's eligibility to participate in an administrative review for this proposed action. Interested members of the public should review the proposal's information to determine the applicable administrative review process and the eligibility requirements for that process. The date of the legal notice of opportunity to comment on this proposed action is the exclusive means for calculating the comment period. For proposals to be documented with an Environmental Assessment, the legal notice announcing the comment period appears in the Newspaper of Record. For Draft Environmental Impact Statements, the Notice of Availability announcing the comment period appears in the Federal Register.

Section 7.0 Access, Redress and Correction

The following questions are directed at an individual's ability to ensure the accuracy of the information collected about them.

7.1 Access

What are the procedures that allow individuals to gain access to their information?

There are no procedures that allow the public to gain access to eMNEPA data.

7.2 Correction

What are the procedures for correcting inaccurate or erroneous information?

Members of the public cannot view data contained inside of eMNEPA. Public comment letters stored in eMNEPA may be published to the web; these letters are viewable by the public. The public can contact the FS at any time during the NEPA process and afterwards to inquire about their information contained in eMNEPA and provide updated contact information using the project contact information provided on the web.

This is not stated on announcements. The public supplies information in order to participate in the process. Since the public can supply real, fake or no information, they can supply any contact information they choose at any time, and provide updated information at any time.

7.3 Notification

How are individuals notified of the procedures for correcting their information?

Instructions for submitting information are provided when comments are solicited. The public can follow the instructions to submit updates to their information.

7.4 Redress Alternatives

If no formal redress is provided, what alternatives are available to the individual?

There is no formal communication procedure regarding information correction, nor is a formal process needed. The public can follow the instructions to submit updates to their information. FS personnel who are assigned a role on

the specific project concerned can edit outdated information in eMNEPA applications.

7.5 Risk Mitigation

Please discuss the privacy risks associated with the redress available to individuals and how those risks are mitigated.

Another person attempts to change an individual's contact information. If an individual requests to have their contact information updated, the project staff can contact the individual at the old and new addresses to confirm the change.

Individual does not update, or know how to update, their information. There is no risk associated to not updating information. Everyone has an opportunity to submit new information when a new project begins.

Section 8.0 Technical Access and Security

The following questions are intended to describe technical safeguards and security measures.

8.1 Procedures

What procedures are in place to determine which users may access the system and are they documented?

Privileged administrative users authenticate to AWS GovCloud through the AWS IAM service which includes multi-factor authentication. Authorization is enforced by AWS IAM groups. Administration of Linux servers requires SSH and a certificate. Administration of Windows servers requires RDP along with username/password.

End users authenticate for applications by first authenticating to PALS hosted at FS ACE, which implements USDA eAuthentication. The single-sign-on capabilities between PALS and security eMNEPA are custom built.

For PALS and security eMNEPA, users login through PALS. User access is enforced through role-based permissions for individual projects. There are four role levels:

Administrator

Approver

Contributor

Read-only

Administrator permissions are granted by existing system administrators; Approver role is granted by administrators based on the user's position as a project manager; Contributor role is granted by administrators, or by approvers only for the projects they manage. All Forest Service personnel are eligible to be assigned to participate in the NEPA process and be assigned to projects; therefore all Forest Service personnel have Read access to eMNEPA applications. These roles are documented in PALS system documentation.

8.2 Contractor Access

Will Department contractors have access to the system?

Yes. Contractor access is based on Least Privilege necessary to perform job roles, and Separation of Duties. Administrator permissions are granted by existing system administrators. Authentication to AWS GovCloud includes multi-factor authentication and authorization is enforced by AWS IAM groups. Administration of Linux servers requires SSH and a certificate. Administration of Windows servers requires RDP along with username/password.

There are three contractor roles:

Technical Lead

Developer

Systems Administrator

8.3 Privacy Training

Describe what privacy training is provided to users either generally or specifically relevant to the program or system?

FS users are required to take the Annual Information Security Awareness Training Course, and FS Personally Identifiable Information course provided by the USDA via AgLearn computer-based training (CBT). Instructions for handling PII are included in the CARA 101 training course provided by NEPA Services Group.

8.4 System Authority to Operate

Has Assessment & Authorization been completed for the system(s) supporting the program? If so, answer “Yes” and provide ATO expiration date(s).

eMNEPA has an Authority To Operate dated 10/26/2018

8.5 Audit and Technical Safeguards

What auditing measures and technical safeguards are in place to prevent misuse of data?

Unauthorized individuals gaining access to the system. The eMNEPA system, is audited for access from the Amazon Web Services (AWS) cloud environment to the application level to ensure only approved administrators have access.

Unauthorized individuals gaining access to the application Administrative access to the system and data are determined by business need and individual roles. Access to the application's PII is recertified and audited on a quarterly basis.

8.6 Risk Mitigation

Given the sensitivity and scope of the information collected, as well as any information sharing conducted on the system, what privacy risks were identified and how do the security controls mitigate them?

Unauthorized individuals gaining access to the data. FS personnel who want to access eMNEPA applications are authenticated using USDA eAuthentication system (Level 2) prior to accessing the application. There is a preliminary authentication of the user when they log into their FS corporate computer.

FS personnel are also given access to enter and edit data via individual role-based permissions.

Section 9.0 Technology

The following questions are directed at critically analyzing the selection process for any technologies utilized by the system, including system hardware and other technology.

9.1 Description

What type of project is the program or system?

eMNEPA, is a Federal Information Security Management Act (FISMA) Moderate system

9.2 Privacy Concerns

Does the project employ technology which may raise privacy concerns? If so, please discuss their implementation.

No

Section 10.0 Third Party Websites/Applications

The following questions are directed at critically analyzing the privacy impact of using third party websites and/or applications.

10.1 Review

Has the System Owner (SO) and/or Information Systems Security Program Manager (ISSPM) reviewed Office of Management and Budget (OMB) memorandums M-10-22 “Guidance for Online Use of Web Measurement and Customization Technology” and M-10-23 “Guidance for Agency Use of Third-Party Websites and Applications”?

Yes. The System Owner has reviewed the above OMB memorandums

10.2 Purpose

What is the specific purpose of the agency’s use of 3rd party websites and/or applications?

N/A

10.3 PII Availability

What Personally Identifiable Information (PII) will become available through the agency’s use of 3rd party websites and/or applications?

N/A

10.4 PII Usage

How will the PII that becomes available through the agency’s use of 3rd party websites and/or applications be used?

N/A

10.5 PII Maintenance and Security

How will the PII that becomes available through the agency’s use of 3rd party websites and/or applications be maintained and secured?

N/A

10.6 PII Purging

Is the PII that becomes available through the agency's use of 3rd party websites and/or applications purged periodically? If so, is it done automatically? If so, is it done on a recurring basis?

N/A

10.7 PII Access

Who will have access to PII that becomes available through the agency's use of 3rd party websites and/or applications?

N/A

10.8 PII Sharing

With whom will the PII that becomes available through the agency's use of 3rd party websites and/or applications be shared—either internally or externally?

N/A

10.9 SORN Requirement

Will the activities involving the PII that becomes available through the agency's use of 3rd party websites and/or applications require either the creation or modification of a system of records notice (SORN)?

N/A

10.10 Web Measurement and Customization

Does the system use web measurement and customization technology? If so, is the system and procedures reviewed annually to demonstrate compliance to OMB M-10-23?

N/A

10.11 Web Measurement and Customization Opt-In/Opt-Out

Does the system allow users to either decline to opt-in or decide to opt-out of all uses of web measurement and customization technology? If so, does the agency provide the public with alternatives for acquiring comparable information and services?

N/A

10.12 Risk Mitigation

Given the amount and type of PII that becomes available through the agency's use of 3rd party websites and/or applications, discuss the privacy risks identified and how they were mitigated.

N/A

Responsible Official

AMY BARKER

Digitally signed by AMY BARKER
Date: 2020.05.18 12:58:00 -06'00'

Amy C Baker
System Owner (SO)
NSG Branch Chief, NEPA Services Group, Forest Service
United States Department of Agriculture

Approval Signature

CYNTHIA TOWERS

Digitally signed by CYNTHIA TOWERS
Date: 2020.05.18 14:37:29 -05'00'

Cynthia Towers
Privacy Officer (PO)
Natural Resources and Environment, Forest Service
United States Department of Agriculture

ROBERT CHADDERDON

Digitally signed by ROBERT CHADDERDON
Date: 2020.05.26 07:07:16 -06'00'

Robert Chadderdon, acting for:
Laura Hill
Assistant Chief Information Security Officer (ACISO)
Natural Resources and Environment, Forest Service
United States Department of Agriculture