Privacy Impact Assessment
ePermits

Version: 1.0

Date: October 11, 2017

Prepared for: USDA OCIO-Policy, E-Government and Fair Information Practices (PE&F)

USDA

United States Department of Agriculture

Privacy Impact Assessment for the ePermits

October 11, 2017

<u>Contact Point</u>

Orion Dix
Forest Service, ePermits ISSO
(541) 750-7137

<u>Reviewing Official</u>

Darrin Maxwell
Privacy Officer
USDA Forest Service
(202) 239-4186

Abstract

ePermits is an permit application solution that will create an online option along with the current manual process of issuing natural resource and special use permits. It includes the following steps in the application of a permit; application, assessment, disposition (approval, rejection, or pending status), issue, and analysis capabilities.

A PIA is required for ePermits due to the outcome of the results of ePermits Privacy Threshold Analysis (PTA).

Overview

This PIA applies to the following Forest Service division(s):

    USDA Forest Service

    Washington Office

    National Forest System

    Natural Resource Manager (NRM)

    System Name: ePermits

    UII Code: 005-000002223 00-96-01-11-01-00

Description

This ePermit system is part of the U.S. Forest Service effort to modernize and simplify their permitting processes. One facet of this effort is an online permitting application, or making the applications for many Forest Service permits available online. The system will present permit application instructions, and allow members of the public to submit application information online as well as receive permits directly from the system.

The system is primarily a JavaScript web application server that facilitates a client user-interface in browser. Another module exists to connect the server to the Special Uses Data System Application protocol interface.

Transactions

Within the system, applicants will submit the information required by OMB approved forms for special use and forest products applications. For special use applications, these applications are then given an initial review by Forest Service employees. Upon their acceptance they will accept the information into the USDA Forest Service Special Use Data System within the FS Natural Resource Manager. Where payment is required for the permit fee, applicants will be directed to pay.gov.

The system is primarily a JavaScript web application server that facilitates a client user-interface in browser. Another module exists to connect the server to the Special Uses Data System Application protocol interface.

Information Sharing

The following is a list of other systems that ePermits shares data with:

● Cloud.gov (cloud hosting only)

● Natural Resource Manager (NRM)

● Pay.gov

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

Permit applicant contact information, business information pertaining to certain types of permit including guide documentation, operating plans, certificates of insurance, evidence of good standing, and an acknowledgement of risk form. Certain applications will require detailed route data of planned trips. This information is collected within ePermits and then transferred to other Forest Service systems, which serve as the systems of record for the permit process.

1.2 What are the sources of the information in the system?

Permit application information is derived from existing Forest Service resources. Permit applicants supply applicant information including their personally identifiable information and business addresses. For certain types of permits they also submit guide documentation, operating plans, certificates of insurance, evidence of good standing, and an acknowledgement of risk form. These materials are currently being collected via email.

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

The information being collected is used to make a determination as to whether the Forest Service should issue a permit for special use or special forest product collection on the National Forest.

Trip route data and information may be used to generate maps and relevant spatial representations of the data.

1.4 How is the information collected?

The information is collected in a web application interface after the member of the public is authenticated. In some cases, a Forest Service employee may enter in the permit application information on behalf of the applicant either by phone or in person.

1.5 How will the information be checked for accuracy?

The system interface will conduct the first round of validation, by ensuring that the applications are complete, do not contain any special injections, and/or meet the requirements of the particular field information (i.e. is a valid phone number). Following submission by the applicant, a Forest Service Special Use Administrator will provide an initial review and notify the applicant if the information needs updating or review.

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

1. Organic Administration Act of June 4, 1897 (16 U.S.C. 477-482, 551). Permits and temporary permits.

2. Preservation of American Antiquities Act of June 8, 1906 (16 U.S.C. 431 et seq.). Permits and temporary permits.

3. Act of March 4, 1915, as amended July 28, 1956, (16 U.S.C. 497). Term permits.

4. Mineral Leasing Act of 1920, as amended on November 16, 1973, (30 U.S.C. 185). Easements, permits, and temporary permits.

5. Bankhead-Jones Farm Tenant Act of July 22, 1937, as amended (7 U.S.C. 1010-1012). Easements, permits, and temporary permits.

6. Alaska Term Permit Act of March 30, 1948 (48 U.S.C. 341). Term permits (Alaska only).

7. Section 7 of the Granger-Thye Act of April 24, 1950 (16 U.S.C. 580d). Term permits and permits. WO AMENDMENT 2700-2014-1 EFFECTIVE DATE: 04/17/2014 DURATION: This amendment is effective until superseded or removed. 2710 Page 6 of 109 FSM 2700 – SPECIAL USES MANAGEMENT CHAPTER 2710 – SPECIAL USE AUTHORIZATIONS

8. Act of September 3, 1954, (43 U.S.C. 931c-931d). Easements, permits, and term permits.

9. Wilderness Act of September 3, 1964, (16 U.S.C. 1121, 1131-1136). Permits and temporary permits.

10. Land and Water Conservation Fund Act of September 3, 1964, (16 U.S.C. 4601). Permits.

11. National Forest Roads and Trails Act of October 13, 1964, (16 U.S.C. 532-538). Easements.

12. Title V, Federal Lands Policy and Management Act of October 21, 1976, (43 U.S.C. 1761-1771). Easements, leases, and permits.

13. American Indian Religious Freedom Act of 1978, (42 U.S.C. 1996). Permits.

14. Archeological Resources Protection Act of 1979, (16 U.S.C. 470). Permits.

15. Alaska National Interest Lands Conservation Act of 1980, (16 U.S.C. 3210). Easements and permits.

16. National Forest Ski Area Permit Act of 1986, (16 U.S.C. 497b). Permits.

17. Federal Lands Recreation Enhancement Act of December 8, 2004, (16 U.S.C. 6808(h)). Permits.

1.7 <u>Privacy Impact Analysis</u>: Given the amount and type of data collected, discuss the privacy risks identified and how they were mitigated.

The system will be housed in a FedRAMP Moderate authorized hosting environment. The data storage will be encrypted at Rest. Only authenticated users will be allowed to submit or edit information.

Risk	Mitigation
Unauthorized access is gained to the system or to the database content that stores ePermit PII data.	Existing access controls prevent unauthorized modification of data, and in some instances, data is no longer available for modification based on process (it is locked). Roles are tested to ensure that they can only get to the data that they are intended to give access to.
PII data is inadvertently viewed on a user's screen	The data is encrypted in the database and the system uses least privilege principles to only allow authenticated applicants and privileged Forest Service Administrators to view the information.
When PII data is electronically transferred to non-ePermit systems such as eAuth might be accessible.	Data is encrypted using both client certificate exchange, token based authentication, and TLS.
When PII is printed from ePermit, are there user procedures in place for handling the information sent to the printers.	Data is required to be retrieved immediately for safe storage.

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 Describe all the uses of information.

Specific Use

The system will be used to collect permit application information, make determinations of whether to issue a permit, in some cases issue permits, and maintain a record of who has permits on the Forest. It will be used to facilitate discussions about the permitting process. It will be also used to generate statistics of usage of special uses and forest products on the Forest.

Routine Use

Routine use refers to disclosures generally permitted under 5 U.S.C. 552a (b) of the Privacy Act. Routine use disclosures are not mandatory. They are optional disclosures made at the discretion of the appropriate Privacy Act System Manager or designee. Nevertheless, FS must keep an accounting of all disclosures made pursuant to a routine use on a disclosure accounting record such as this PIA. Routine Uses are agreements for sharing personal information with:

- The Department of Treasury or another Federal agency conducting financial assessment, collection and payments (such as Treasury offset for debt collection for TSRM permits)

- The Department of Justice (including United States Attorney Offices) or another Federal agency conducting litigation or in proceedings.

- To a congressional office in response to an individual's request.

- To the National Archives and Records Administration or an authority of 44 U.S.C. §§ 2904 and 2906.

- To contractors and their agents, grantees, experts, consultants, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for FS, when necessary to accomplish an agency function related to this system of records. Individuals provided information under this routine use are subject to the same Privacy Act requirements and limitations on disclosure as are applicable to FS officers and employees.

- To the news media and the public, in consultation with counsel, when there exists a legitimate public interest in the disclosure of the information or when disclosure is necessary to preserve confidence in the integrity of FS or is necessary to demonstrate the accountability of FS's officers, employees, or individuals covered by the system, except to the extent it is determined that release of the specific information in the

context of a particular case would constitute an unwarranted invasion of personal privacy.

- To appropriate agencies, entities, and persons when: FS suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; The Department has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the Department or another agency or entity) or harm to the individual that rely upon the compromised information; and the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Department's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

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

The data will be reviewed manually by individuals. Aggregated data will be primarily about the quantity of permits for a particular forests and not about the individual applicants. Forest Service employees produce maps from the route information provided by the applicants.

Trip route data and information may be used to generate maps and relevant spatial representations of the data.

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

The permit fee information will be used to generate fee estimates.

2.4   <u>Privacy Impact Analysis</u>: Describe any types of controls that may be in place to ensure that information is handled in accordance with the above described uses.

Only specifically designated Forest Service employees and contract staff will have access to review the information in the system.

The following are used to protect PII data stored and transmitted by ePermits:

- Use of encryption at rest for the Amazon Web Services Relational Database (accessed through cloud.gov).
- The ePermit system is audited for access cloud.gov USDA Forest Service organization to the application level to ensure only approved users have access.
- 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.
- FS personnel who have access to ePermits applications are authenticated (proof that the person is who they say they are) using the USDA eAuthentication system (Level 2) prior to access to the application. There is a secondary authentication of the user when they log into their FS corporate computer.
- Members of the public must be authenticated using login.gov Level of Assurance 1 to view applications which they have submitted.

Section 3.0 Retention

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

3.1 How long is information retained?

ePermits retains records for a minimum of 30 days online and a minimum of three (3) years offline not to conflict with NARA policy to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.

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

Yes, the retention period noted above is the NARA requirement for retention of records.

3.3 <u>**Privacy Impact Analysis**</u>**: Please discuss the risks associated with the length of time data is retained and how those risks are mitigated.**

Risk	Mitigation
Unauthorized access is gained to the system or to the database content that stores ePermit PII data.	Existing access controls prevent unauthorized modification of data, and in some instances, data is no longer available for modification based on process (it is locked). Roles are tested to ensure that they can only get to the data that they are intended to give access to.
PII data is inadvertently viewed on a user's screen	The data is encrypted in the database and the system uses least privilege principles to only allow authenticated applicants and privileged Forest Service Administrators to view the information.
When PII data is electronically transferred to non-ePermit systems such as eAuth might be accessible.	Data is encrypted using both client certificate exchange, token based authentication, and TLS.
When PII is printed from ePermit, are there user procedures in place for handling the information sent to the printers.	Data is required to be retrieved immediately for safe storage.

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 **With which internal organization(s) is the information shared, what information is shared and for what purpose?**

Name, address and phone number, SSN, or TIN information is shared with the Forest Service district and forest offices. In some cases, it will be shared with the regional offices. This information will also be shared with the NRM Special Uses organization and business owners. This information is shared to make determinations about whether to issue a permit and reporting on the number of permits issued.

The information is transmitted via an encrypted and authenticated application protocol interface connection to the NRM SUDS system. The connection is limited only to registered IP addresses.

4.2   How is the information transmitted or disclosed?

All transactions are only provided electronically and transmitted an encrypted connection using an authenticated and encrypted TLS connection.

4.3   <u>Privacy Impact Analysis</u>: Considering the extent of internal information sharing, discuss the privacy risks associated with the sharing and how they were mitigated.

Risk	Mitigation
Unauthorized access is gained to the system or to the database content that stores ePermit PII data.	Existing access controls prevent unauthorized modification of data, and in some instances, data is no longer available for modification based on process (it is locked). Roles are tested to ensure that they can only get to the data that they are intended to give access to.
PII data is inadvertently viewed on a user's screen	The data is encrypted in the database and the system uses least privilege principles to only allow authenticated applicants and privileged Forest Service Administrators to view the information.
When PII data is electronically transferred to non-ePermit systems such as eAuth might be accessible.	Data is encrypted using both client certificate exchange, token based authentication, and TLS.
When PII is printed from ePermit, are there user procedures in place for handling the information sent to the printers.	Data is required to be retrieved immediately for safe storage.

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   With which external organization(s) is the information shared, what information is shared, and for what purpose?

Name, address and phone number PII will be shared with the US Treasury's Pay.gov system. This will facilitate financial payments to permits generated by the system, while allowing the system to not have to handle Personal Credit Card information directly.

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

The information is shared via an API that is encrypted via TLS. The connection is limited to the cloud.gov egress IP addresses.

5.4 Privacy Impact Analysis: Given the external sharing, explain the privacy risks identified and describe how they were mitigated.

Risk	Mitigation
Unauthorized access is gained to the system or to the database content that stores ePermit PII data.	Existing access controls prevent unauthorized modification of data, and in some instances, data is no longer available for modification based on process (it is locked). Roles are tested to ensure that they can only get to the data that they are intended to give access to.
PII data is inadvertently viewed on a user's screen	The data is encrypted in the database and the system uses least privilege principles to only allow authenticated applicants and privileged Forest Service Administrators to view the information.
When PII data is electronically transferred to non-ePermit systems such as eAuth might be accessible.	Data is encrypted using both client certificate exchange, token based authentication, and TLS.
When PII is printed from ePermit, are there user procedures in place for handling the information sent to the printers.	Data is required to be retrieved immediately for safe storage.

Section 6.0 Notice

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

No. Information is not able to be retrieved or queried via PII.

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

Prior to PII collection, applicants will be required to verify that they have reviewed the notice provided to them PII collection prior to submission of their application. This notice will include an itemized list of PII that will be collected.

Information to individuals is provided via:

- ePermits Privacy Impact Analysis (PIA) on the USDA PIA website.
- Forms are approved through OMB for the Paperwork Reduction Act (also cited in the Federal Register) and they cite the privacy information act.

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

Yes, however if they do decline, they will not receive the product/services requested.

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

Yes, individuals have the right to consent to particular uses of information. ePermits itemizes consent using the minimal necessary PII required to complete transactions requested by individuals. Individuals can either accept the uses required to complete their particular transaction or not accept the particular uses. If consent is not given then transactions do not have sufficient information to occur.

6.5   <u>Privacy Impact Analysis</u>: Describe how notice is provided to individuals, and how the risks associated with individuals being unaware of the collection are mitigated.

Prior to supplying information, applicants are provided notice will that includes an itemized list of PII to be be collected.

- Customers are advised that they do not have to furnish the information but failure to do so in special circumstances may prevent their request from being processed. The information that customers furnish is never used for any purpose other than to process and respond to their request.
- However, US FS may disclose information to a Congressional office in response to an inquiry made on behalf of the requestor, to the Department of Justice, a court, other

- tribunal when the information is relevant and necessary to litigation, or to a contractor or another Federal agency to help accomplish a function related to this process.
- If shared within USFS and the Department of Agriculture, all information is still used in accordance with the system's stated authority and purpose. Risks to privacy are mitigated by granting access only to authorized persons. All employees of the Department of Agriculture have undergone a thorough background investigation.
- Access to computer facilities is typically controlled by security guards and admission is limited to those individuals possessing a valid identification card or individuals under proper escort. All records containing personal information are maintained in secured-file cabinets or in restricted areas, access to which is limited to authorized personnel. Access to computerized files is password-protected and under the direct supervision of the system manager. The system manager has the capability of printing audit trails of access from the computer media, thereby permitting regular ad hoc monitoring of computer usage.
- When a transaction must contain a signature in writing in order to be legally enforceable, due care is taken to ensure that documentation provides a record that is not subject to imperfect memory or competing claims as to what parties to the transactions intended.
- The methods used to obtain, send, disclose and store information complies with applicable laws, such as those governing privacy, confidentiality, recordkeeping, and accessibility to persons with disabilities.

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

An individual would be able to access their previously submitted application by authenticating into the system. They may also phone, visit, or email a special use administrator to obtain the information included in the NRM SUDS system.

7.2 What are the procedures for correcting inaccurate or erroneous information?

For applications the applicant has submitted they will be able to authenticate into the system and update it as well as phone, visit, or email with their designated Special Use Administrator to update it.

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

Notification occurs at time of information collection. Users are notified that they can phone, visit, or email the Forest Service Special Use Administrator to fix erroneous information.

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

They can phone, visit or email the Forest Service Special Use Administrator.

7.5 <u>Privacy Impact Analysis</u>: Please discuss the privacy risks associated with the redress available to individuals and how those risks are mitigated.

Risk	Mitigation
Someone claiming to be user can change PII without being required to prove that they are, indeed, the user The guidance for the content of requests for correction of information is not intended to constitute a set of legally binding requirements. Requestors bear the 'burden of proof' with respect to the necessity for correction as well as with respect to the type of correction they seek. However, the USFS may be unable to process, in a timely fashion or at all, requests that omit one or more of the requested elements	Persons contacting the special use administrator are required to provide identification in order to make any changes to PII.

Section 8.0 Technical Access and Security

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

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

Members of the public will be able to access the informational pages of the system as they will be on the open internet. To complete, review or cancel applications, they will have to be authenticated.

8.2 Will Department contractors have access to the system?

Yes. Access will be based on Least Privilege necessary to perform job role and Separation of Duties.

8.3 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 Security Awareness Training Course, and PII Lite course — currently provided by the USDA via AgLearn computer-based training (CBT). No PII training specifics to the program or system is offered.

8.4 Has Certification & Accreditation been completed for the system or systems supporting the program?

ePermits is in process of seeking its initial ATO

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

Risk	Audit Measure
Unauthorized individuals gaining access to the data via the system.	The ePermits system is audited for access from the cloud.gov USDA Forest Service organization to the application level to ensure only approved users have access.
Unauthorized individuals gaining access to the data via the application	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   <u>Privacy Impact Analysis</u>**: 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?**

Risk	Mitigation
Unauthorized individuals gaining access to the data.	FS personnel who want access to ePermits applications are authenticated (proof that the person is who they say they are) using the USDA eAuthentication system (Level 2) prior to access to the application. There is a secondary authentication of the user when they log into their FS corporate computer. FS personnel must also be given access to the system and data based on business need and the individual roles. Members of the public must be authenticated using login.gov Level of Assurance 1 to view applications which they have submitted.
Unauthorized access is gained during the sharing of data with internal and external organizations	Data is encrypted in in transit to the other systems using TLS and encrypted SAML partnerships.

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   What type of project is the program or system?

The system is a Node.JS JavaScript application, hosted on the FedRAMP Moderate Cloud.gov.

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

N/A - ePermits does not use any 3rd party websites and/or applications.

10.3   What personally identifiable information (PII) will become available through the agency's use of 3rd party websites and/or applications.

N/A - ePermits does not use any 3rd party websites and/or applications.

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

N/A - ePermits does not use any 3rd party websites and/or applications.

10.5 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 - ePermits does not use any 3ʳᵈ party websites and/or applications.

10.6 Is the PII that becomes available through the agency's use of 3ʳᵈ party websites and/or applications purged periodically?

N/A - ePermits does not use any 3ʳᵈ party websites and/or applications.

If so, is it done automatically?

N/A - ePermits does not use any 3ʳᵈ party websites and/or applications.

If so, is it done on a recurring basis?

N/A - ePermits does not use any 3ʳᵈ party websites and/or applications.

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

N/A - ePermits does not use any 3ʳᵈ party websites and/or applications.

10.8 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 - ePermits does not use any 3ʳᵈ party websites and/or applications.

10.9 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 - ePermits does not use any 3ʳᵈ party websites and/or applications.

10.10 Does the system use web measurement and customization technology?

In accordance with OMB Memo M-17-06, it will include measurement and analytics for the Digital Analytics Program.

If so, is the system and procedures reviewed annually to demonstrate compliance to OMB M-10-23?

Yes, Procedures will be reviewed annually as part of the PIA update and recertification.

10.11 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?

The System uses Google Analytics which does not have the option to opt-out of uses of the product. The following is information on how information collected is anonomized so as not to be traceable to an individual:

> *This data provides a window into how people are interacting with the government online. The data comes from a unified Google Analytics account for U.S. federal government agencies known as the Digital Analytics Program. This program helps government agencies understand how people find, access, and use government services online. The program does not track individuals, and anonymizes the IP addresses of visitors.*

If so, does the agency provide the public with alternatives for acquiring comparable information and services?

N/A

10.12 <u>Privacy Impact Analysis</u>: 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 – ePermits does not use any 3rd party websites and/or applications.

Responsible Officials

Name of System Owner: Brian Schwind

Phone for System Owner: 801-975-3751

Email for System Owner: bschwind@fs.fed.us

USDA Forest Service – National Forest System

Approval Signature

_____

Darrin Maxwell
Privacy Officer
USDA Forest Service

_____

Laura Hill
ISSPM
USDA Forest Service

_____

Brian Schwind
ePermits System Owner
USDA Forest Service -National Forest System