Privacy Impact Assessment
NRCS Micropact
(NRCS Micropact)

- Version: 4.0
- Date: January 3, 2020
- Prepared for: USDA OCIO-Policy, E-Government and Fair Information Practices (PE&F)

USDA

United States Department of Agriculture

Privacy Impact Assessment for the

NRCS Micropact (NRCS Micropact)

January 3, 2020

Contact Point

Laura Neal

FPAC-BC IT Project Manager

970-295-5701

Reviewing Official

James Flickinger

FPAC Chief Information Security Officer

United States Department of Agriculture

(816) 926-6010

Abstract

The Natural Resources Conservation Service (NRCS) Micropact (NRCS MP) is a combination of the following applications: National Easement Staging Tool (NEST); Audit Tracking Tool (ATT); and Appeals and Equitable Relief Database (AERD) System. These applications track, monitor, and audit easement applications, appeals actions, programmatic data, resolution case information, and audit information.

A Privacy Threshold Analysis (PTA) was performed, indicating that a PIA must be completed. This PIA is being conducted to comply with the Federal Information Security Modernization Act of 2014 (FISMA) (44 U.S.C. §3551 to §3559) and the E-Government Act of 2002 (Pub. Law. 107-347, 44 U.S.C. §101).

Overview

NRCS provides private landowners with advice, guidance and technical services to carry out conservation practices. The NRCS is an agency within the USDA that has provided over 75 years of leadership in a partnership effort to help America's private land owners and managers. NRCS works with its partners to conserve their soil, water, and other natural resources by providing financial and technical assistance based on sound science and technology suited to a customer's specific needs.

The NRCS MP is a frontend application that uses the Cloud Service Provider (CSP) MicroPact, Inc. software-as a service (SaaS) solution. NRCS MP will consist of the following applications that are all hosted on the entellitrak platform at MicroPact, Inc.: NEST, AERDS and ATT:

- **National Easements Staging Tool (NEST)**: NEST is hosted at MicroPact, Inc., using the entellitrak platform. The application allows State and National Program Managers to manage new and existing easement applications and contracts for these programs: Agricultural Conservation Easement Program- Wetland Reserve Easement (ACEP-WRE), Agricultural Conservation Easement Program- Agricultural Land Easement (ACEP-ALE), Regional Conservation Partnership Program- Agricultural Conservation Easement Program- Wetland Reserve Easement (ACEP-WRE) (RCPP-ACEP-WRE), Regional Conservation Partnership Program- Agricultural Conservation Easement Program-Agricutrual Land Easement (RCPP-ACEP-ALE), Regional Conservation Partnership Program- Healthy Forest Reserve Program (RCPP-HFRP), Emergency Watershed Protection Program- Flood Plain Easement (EWPP-FPE), Healthy Forest Reserve Program (HFRP),Water Bank Program (WBP), Other Stewardship Lands (OSL), through a variety of steps, inputs and workflows.
- **The Appeals and Equitable Relief Database System (AERDS)**: AERDS was developed using the entellitrak middleware product (a part of the NRCS NEST system) and is hosted at the MicroPact, Inc. facility. This is a web-based application containing existing and new appeal case data, enabling NRCS employees in NHQ and the State Offices to strategically track and monitor NRCS appeals actions and resolution case information.

- **The Audit Tracking Tool (ATT)**: ATT was developed using the entellitrak platform and is hosted at the MicroPact, Inc. facility. This web-based application contains existing and new audit data, allowing NRCS staff to manage their audit programmatic data, as well as enabling NRCA employees in NHQ and the State Offices to strategically track and monitor audit information.

Legal Authority: This system is regulated by privacy laws, regulations and government requirements, including the Privacy Act (5 U.S.C. §552a); the E-Government Act of 2002 (Pub. Law. 107-347, 44 U.S.C. §101); the Paperwork Reduction Act of 1995 (44 U.S.C. §3501); the Federal Information Security Modernization Act of 2014 (FISMA) (44 U.S.C. §3551 to §3559); OMB Memos M-03-22, M-10-23, M-16-24, and M-17-12; and OMB Circular A-130, Appendix I.

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?

- The system does not directly "collect" any PII from any individual.

- AERDS – contact information (names, mailing addresses and phone numbers of individuals related to appeals cases) related to members of the public who are involved in appeals and equitable relief actions.

- NEST – land locations of clients who have existing/active WRP, GRP, EWPP, WBP, OSL, MBHI, and FRPP easement agreements, as well as for members of the public who submit new easement applications.

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

- AERDS – NRCS obtains information from USDA National Appeals Division (NAD), which provides summaries of the appeals and equitable relief cases. NRCS enters this summary information (including case number) into AERDS. AERDS receives this PII contact information from public records that contain case, participant and agency information. AERDS makes use of case-related data (no audio files are used) and determinations as well as participant and agency contact information.
- NEST – NRCS SCIMS database. NRCS has access to a copy of the SCIMS database (maintained by FSA) via replication and access to the data from SCIMS for NRCS users is via NPAD and through eAuthentication (eAuth). NRCS users do not have direct access to SCIMS. The landowners may provide information to SCIMS, which is the source of the PII. All information is obtained through a database copy.
- NRCS MP does not modify or update any information in SCIMS.

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

- AERDS - The information is used to track appeals and case resolution activities, which may include physically mailing materials to the relevant individuals, or contacting them by phone or email as necessary.
- NEST – Information is used and maintained in order to manage new and existing easement applications.

1.4 How is the information collected?

- AERDS - PII information is not submitted directly to the system by members of the public. USDA personnel enter information into the system that is manually collected from various sources, including members of the public.
- NEST – NEST collects landowner information, including the names, addresses and SCIMS IDs from the SCIMS database copy. NRCS users do not have a direct access to SCIMS. All information is obtained through a database copy. NRCS State and National Program Managers also provide non-PII information that is used within NEST, uploaded from easement forms.

1.5 How will the information be checked for accuracy?

- AERDS – The accuracy of the PII is dependent upon the members of the public submitting the information. AERDS users are responsible for validating the accuracy of PII within AERDS through interaction with members of the public who submit PII.
- NEST - The accuracy of PII obtained from SCIMS is not within the scope of NEST or NRCS MP. NRCS users do not have the ability to update any information in SCIMS, nor do they have the ability to update the information in any other application databases not maintained by NRCS. Non-PII information in NEST is reviewed for accuracy and is verified through manual review and comparison with existing agency data (e.g. specific land boundaries). This is done by knowledgeable State and National Program Managers.

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

These regulations are applicable:
- Privacy Act (5 U.S.C. §552a);
- E-Government Act of 2002 (Pub. Law. 107-347, 44 U.S.C. §101);
- Paperwork Reduction Act of 1995 (44 U.S.C. §3501)

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 primary privacy risk is that a data breach could result in the release of information on members of the public.
- Privacy risks are mitigated because access to the information will be limited to appropriately trained NRCS employees only by the use of the USDA eAuthentication (eAuth) system, which provides user authentication for NRCS and role based access control (RBAC) provides access enforcement. Other access requirements include the need for users to be on the USDA network backbone, using a CCE computer.
- Please see Section 2.4 and Section 8.6 for a further discussion of security controls that are in place to mitigate privacy risks.

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.

- AERDS - PII data collected is only used to contact individuals regarding appeals cases, and sometimes physically mail materials related to an appeals case.
- NEST - This information is used to identify landholders for purposes of managing existing active agreements and to provide a uniform means for recording editing and/or deleting new applications.

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

The applications do not use any tools to analyze the PII.

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

The applications do not use commercial or publicly available data.

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.

- This application is in compliance with the FISMA and the security and privacy controls provided in the U.S. National Institute of Standards and Technology (NIST) Special Publication 800-53, Revision 4.
- If any residual risks are identified, they will be managed and reported via the FISMA mandated risk assessment processes.

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?

- All information contained will be retained in compliance with NARA Guidelines, which vary on average in years from less than one year to more than ten years according to the NARA General Records Schedules Transmittal 29, issued December 2017, unless specified otherwise.
- Per the NRCS-1 System of Record Notice (SORN), "Records are maintained as long as the owner, operator, producer, or participant qualifies for conservation programs".

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

- Yes

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.

- The primary privacy risk is that a data breach could result in the release of information on members of the public. This is mitigated by limited access to the data, the non-portability of the data and controlled storage of the data in controlled facilities.
- Retention of application-specific data is required to meet business and organizational requirements for this particular information system. The risks associated with retaining application-specific information are mitigated by the controls discussed above.

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?

- NEST obtains information related to landowners from the SCIMS database copy maintained by NRCS. NEST does not share or transmit any information to SCIMS, nor does it update any information in SCIMS.

4.2 How is the information transmitted or disclosed?

- NRCS has access to a copy of the SCIMS database via replication. Access to the data is through established security rules via eAuth.

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.

- Privacy risks are mitigated by ensuring that access to the data is through established security rules via eAuth. Any residual risks are mitigated by the controls discussed in Section 2.4 above.

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?

- NRCS MP's three applications utilize the entellitrak platform that is hosted at the MicroPact, Inc. facility.

5.2 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.

- NRCS MP is subject to the NRCS-1 SORN. URL: https://www.ocio.usda.gov/sites/default/files/docs/2012/NRCS-1.txt

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

- NEST, ATT and AERDS applications are applications that reside on the MicroPact FedRAMP SaaS solution using the Entellitrak middleware product (a part of the NRCS NEST system) at the MicroPact, Inc. facility.
- NRCS MP allows access to the system through a browser to users who have Level 2 eAuthentication and have been granted access by a supervisor, as well as STC permission Within the parameters of the NRCS MP system, the web server performs queries to view and/or update data in the NEST, ATT and AERDS databases.

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

- Privacy risks are mitigated by ensuring that access to the data is through established security rules via eAuth and authorized through role based access. Any residual risks are mitigated by the controls discussed in Section 2.4 above.

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.

- NRCS MP is subject to the NRCS-1 SORN. URL: https://www.ocio.usda.gov/sites/default/files/docs/2012/NRCS-1.txt

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

- AERDS – Members of the public are advised of the uses of the PII when they contact a USDA, State or local appeals case manager.
- NRCS Privacy Policy published on USDA website.

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

- AERDS – Disclosure of PII is voluntary when members of the public contact USDA regarding an appeals case. Members of the public retain the right to decline to provide any PII at any time.
- Any PII information is obtained from the SCIMS system is maintained by FSA. Members of the Public do not have access to this application.

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

- No. Any PII information is obtained from the SCIMS system, which is maintained by FSA. Members of the Public do not have access to this application.

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.

- Any PII information that is obtained from the SCIMS system, is maintained by FSA, with a copy of the SCIMS database provided to NRCS. NRCS MP is not responsible

for eliciting consent for the use, or collection, of PII, as any PII that is obtained from SCIMS is maintained by FSA.
- No notice is provided to any affected individuals because no PII is solicited or collected from any individual by NRCS MP.

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?

- AERDS - Individuals can access their PII through their assigned case manager, or by contacting the USDA. As published in SORN USDA/NRCS-1: "Any individual may request information regarding this system of records, or information as to whether the system contains records pertaining to him/her by contacting the respective district conservationist or other designee. If the specific location of the record is not known, the individual should address his/her request to the Director, Management Services Division, USDA-Natural Resources Conservation Service, P. O. Box 2890, Washington, DC 20013, who will refer it to the appropriate field office. A request for information pertaining to an individual should contain: Name, address, and other relevant information (e.g., name or nature of program, name of cooperating body, etc.)."

- NEST – Does not collect information directly from individuals. NEST users can enter publicly available information from a land transfer, which typically contains the new landowner's name and address, that has been recorded at the county courthouse in the county that the easement is recorded.

- Any PII information obtained from the SCIMS system would be subject to the applicable procedures to allow individuals to gain access to their SCIMS information, as maintained by the FSA. Note that the applicable procedures to allow individuals to gain access to their SCIMS information are maintained outside of the accreditation boundary of this application by SCIMS

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

- As published in SORN USDA/NRCS-1: "Any individual may obtain information as to the procedures for contesting a record in the system which pertains to him/her by submitting a written request to the district conservationist or his/her designated representative or to the Director, Management Services Division, USDA-Natural Resources Conservation Service, P.O. Box 2890, Washington, DC 20013."

- Any PII information obtained from the SCIMS system would be subject to the applicable procedures to allow individuals to gain access to their SCIMS information, as maintained by the FSA. Note that the applicable procedures to allow individuals to gain access to correct their SCIMS information are maintained outside of the accreditation boundary of this application by SCIMS.

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

- The SORN USDA/NRCS-1 is published on the USDA.gov website.

- Any PII information obtained from the SCIMS system would be subject to the applicable procedures to allow individuals to gain access to their SCIMS information, as maintained by the FSA. Note that the applicable procedures to allow individuals to gain access to correct their SCIMS information are maintained outside of the accreditation boundary of this application by SCIMS.

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

- *N/A*- See section 7.3.

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.

- The risk associated with redress is considered low, as the public does not have access to the system or the data. Any PII information obtained from the SCIMS system would be subject to the applicable procedures governing their SCIMS information as maintained by the FSA.
- Residual privacy risks associated with the redress process for individuals are mitigated since individuals can use the relevant procedures discussed above to update their original public records.

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?

- Access to the NRCS MP application/system is determined via USDA eAuthentication system (eAuth ID) (level II) and authorized via USDA's Role Based Access Control (RBAC) using zRoles.

- User account requests will be sent via email to the designated Application Administrator appointed by the System Owner, who will grant access after verifying that the requestor's official duties necessitate access to the application.
- The application/system has documented Access Control Procedures, in compliance with FISMA and USDA directives. See Section 2.4.

8.2 Will Department contractors have access to the system?

- AERDS – Access is limited to contractors supporting the AERDS project, USDA, State and local case managers, and other NRCS and USDA contractors, as needed.
- Department contractors with a need to know will have access to NRCS MP as part of their regular assigned duties. Contractors are required to undergo mandatory background investigations commensurate with the sensitivity of their responsibilities, in compliance with Federal requirements.

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

- NRCS requires that every employee and contractor receives information security awareness training before being granted network and account access, which contains the requisite privacy training, and Annual Security Awareness and Specialized Training, as required by FISMA (NIST SP 800-53 rev 4) and USDA policies (USDA OCIO DR 3545-001 – Information Security Awareness and Training Policy and USDA OCIO DR 3505-003 - Access Control Policy).

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

- Yes. NRCS Micropact's most recent authorization to operate (ATO) dated on 5-9-2017.

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

- NRCS complies with the "Federal Information Security Modernization Act of 2014" (FISMA). Assessment and Accreditation, as well as annual key control self-assessments, and continuous monitoring procedures are implemented for this application per the requirements given in National Institute of Standards and Technology (NIST) Special Publication 800-53, Rev. 4. Additionally, the system provides technical safeguards to prevent misuse of data including:
- Confidentiality: Encryption is implemented to secure data at rest and in transit for this application (e.g., by FIPS 140-2 compliant HTTPS and end-user hard disk encryption).

- Integrity: Masking of applicable information is performed for this application (e.g., passwords are masked by eAuth).
- Access Control: The systems implements least privileges and need to know to control access to PII (e.g., by RBAC). Administrative and management operational controls in place to ensure proper access termination.
- Authentication: Access to the system and session timeout is implemented for this application (e.g. by eAuth and via multi-factor authentication for remote access).
- Audit: Logging is implemented for this application (e.g. by logging infrastructure).
- Attack Mitigation: The system implements security mechanisms such as input validation.
- Notice: For the privacy notice control, please see Section 6 which addresses notice. For the privacy redress control, please see Section 7 which addresses redress.

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?

- NRCS MP does not directly collect any PII from any individual landowner (i.e., member of the public). NEST users can enter publicly available information from a land transfer, which typically contains the new landowner's name and address, that has been recorded at the county courthouse in the county that the easement is recorded
- NRCS MP does utilize PII within the system obtained from the SCIMS database, copied from the SCIMS system, which is maintained by FSA. Data extracts containing PII are not regularly obtained from the system, therefore, privacy risk from this area is limited and addressed through IT Data Extract processes controls. Any PII information is obtained from the SCIMS database, copied from the SCIMS system, which is maintained by FSA.
- Any privacy risks identified in this system are mitigated by the security and privacy safeguards provided in Section 8.5, and by the security controls discussed in Section 2.4 above. Remediation of privacy risks associated with internal/external sharing are addressed in PIA Sections 4 and 5 respectively.

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?

- NRCS MP is a frontend application that uses the Cloud Service Provider (CSP) MicroPact, Inc. software-as a service (SaaS) solution. NRCS MP's three applications are all hosted on the entellitrak platform at MicroPact, Inc.

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

- No, the project utilizes Agency approved technologies, and these technology choices do not raise privacy concerns.

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

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

- *N/A* - Third party websites / applications are not used

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

- *N/A* - Third party websites / applications are not used

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* - Third party websites / applications are not used

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* - Third party websites / applications are not used

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

- *N/A* - Third party websites / applications are not used

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 - Third party websites / applications are not used*

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 - Third party websites / applications are not used*

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 - Third party websites / applications are not used*

10.10 Does the system use web measurement and customization technology?

- No, the system does not use web measurement and customization technology.

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?

- *N/A - See section 10.10.*

10.12 Privacy Impact Analysis: 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.

- NRCS MP does not provide access or link to Third Party websites or applications. In addition, the system does not use web measurement or customization technology.

Agency Responsible Officials

Jake Zebell
NRCS MP Information System Owner
United States Department of Agriculture

Agency Approval Signature

Lanita Thomas
FPAC Information Systems Security Program Manager
United States Department of Agriculture

Agency Privacy Approval Signature

Amber Ross
FPAC Privacy Officer
United States Department of Agriculture