Privacy Impact Assessment

NRCS Mission Support

Policy, E-Government and Fair Information Practices

- Version: 3.1
- Date: November 4, 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 Mission Support (NRCS MS)

November 4, 2020

Contact Point

Lanita Thomas
NRCS MS Program Manager
202-260-8593

Reviewing Official

James Flickinger
Chief Information Security Officer, FPAC
United States Department of Agriculture
(816) 926-6010

Abstract

NRCS Mission Support contains the NRCS IT Security tools including: The NRCS Enterprise Vulnerability Assessment (EVA), NRCS Enterprise Data Masking (NED) and Web Application Firewall (WAF).

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

The Natural Resources Conservation Service (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 landowners 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.

In order to encourage efficiency, the decision was made to integrate the following NRCS complementing systems into one mission support entity, to support the overall NRCS security posture. NRCS MS program will combine the above described five NRCS systems/applications under one program.

Authority to operate EVA was previously provided via the ATO granted on 12/22/2017. EVA has been re-named as NRCS Mission Support.

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-10-22, 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?

Information is collected, used or maintained in NRCS MS by the use of the various applications:

- EVA conducts security testing of NRCS systems as an important means of detecting weaknesses and determining the threat posed by them.
- NED is a software that monitors the NRCS databases to discover and mask or encrypt PII data for NRCS applications. In this process it has the ability to read all NRCS application PII and Controlled Unclassified Information (CUI) data.
- WAF analyzes network traffic, then monitors and analyzes each request/ response from the applications and filters any malicious requests.

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

Information is collected, used or maintained in NRCS MS by the use of the various applications:

- EVA – from NRCS applications.
- NED will monitor all NRCS databases, which may include data obtained from the Service Center Information Management System (SCIMS) database. The *Service Center Information Management System* (SCIMS), maintained by FSA, Service Center Information Management System (SCIMS), CSAM ID # 1672, is the database of customer information that is shared by the three Service Center Agencies, FSA, NRCS, and Rural Development. SCIMS is a repository for USDA business entity and conservation compliance information.
- WAF analyzes NRCS application traffic from NITC HA service provider.

NRCS has access to a copy of the SCIMS database 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 and general public applicants may provide information to SCIMS, which is the source of the PII. All information is obtained through a database copy.

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

- EVA will provide a robust, secure and stable security testing and vulnerability assessment platform for NRCS IT Security to serve NRCS and other USDA agency enterprise applications.
- NED will be utilized to: detect where Sensitive and Personally Identifiable Information (PII) is held; provide audit capabilities to understand what Sensitive and PII data is connected to and mingling with, and who is accessing it; protect Sensitive and PII data with data masking and encryption strategies; and monitor or track how and where Sensitive and PII data is moving through a 360-degree dashboard. NED will collect the PII information obtained from the SCIMS database copy to assist NRCS with the data masking and encryption strategies.
- WAF analyzes network traffic, then monitors and analyzes each request/ response from the applications and filters any malicious requests.

1.4 How is the information collected?

- EVA – from NRCS applications.
- NED will monitor all NRCS databases, which may include data obtained from the SCIMS database.
- WAF analyzes NRCS application traffic from NITC HA service provider.

1.5 How will the information be checked for accuracy?

- Information is reviewed for accuracy and verified through manual review, as well as by comparison with existing agency data throughout the planning process. This is done by employees at local offices who have the requisite knowledge and responsibility for the data.
- The accuracy of PII obtained from SCIMS or other applications not maintained by NRCS is not within the scope of NRCS MS. NRCS MS does not have the ability to update any information in SCIMS, nor does it have the ability to update the information in any other application databases not maintained by NRCS.

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

- The system collects or uses various types of PII.

- Privacy risks are mitigated because access to the information is limited to appropriate NRCS personnel and partners who must be authenticated via the USDA e-AUTH system and authorized via USDA's role based authorization for end-user access to the application.
- 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.

Information is collected, used or maintained in NRCS MS by the use of the various applications:

- The EVA system provides a robust, secure and stable security testing; and vulnerability assessment platform for NRCS IT Security to serve NRCS and other USDA agency enterprise applications.
- NED will be utilized to: detect where Sensitive and Personally Identifiable Information (PII) is held; provide audit capabilities to understand what Sensitive and PII data is connected to and mingling with, and who is accessing it; protect Sensitive and PII data with data masking and encryption strategies; and monitor or track how and where Sensitive and PII data is moving through a 360-degree dashboard.
- WAF analyzes network traffic, then monitors and analyzes each request/ response from the applications and filters any malicious requests.

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

The NED software will monitor the NRCS databases to discover and mask or encrypt PII data for NRCS applications.

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

Yes, NED and EVA gather cyber threat intelligence data from the vendor to update application signatures. This data is used to identify known attackers and is updated daily. Signatures do not contain PII and are downloaded directly from the vendor. This is one-way communication and NRCS does not transfer data back to the vendor.

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

- NRCS MS 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 from less than one year to more than ten years according to the NARA General Records Schedules Transmittal 29, issued December 2017.
- 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 Privacy Impact Analysis: 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 and controlled storage of the data located 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?

NED monitors NRCS systems on which PII information is stored, collected or used. Some NRCS systems obtain PII information from the SCIMS database. NED does not share/transmit any information to SCIMS not does it update any information in SCIMS. NED monitors the NRCS databases to discover and mask or encrypt PII data for NRCS applications. In this process it has the ability to read all NRCS application PII and Controlled Unclassified Information (CUI) data.

4.2 How is the information transmitted or disclosed?

NED data is transmitted via secure and encrypted transmission from the various systems' databases to the server specifically assigned to NED in NITC. For the NRCS systems that use SCIMS data, 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 Privacy Impact Analysis: 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?

N/A- PII is not shared or disclosed with organizations that are external to the USDA.

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.

N/A- PII is not shared or disclosed with organizations that are external to the USDA.

NRCS MS, however, 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?

N/A- PII is not shared or disclosed with organizations that are external to the USDA.

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

Privacy risks are mitigated by virtue of NOT sharing information external to the USDA. 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 MS 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?

Yes. NRCS Privacy Policy published on USDA website.

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

For the systems that obtain information from SCIMS, individuals do not have the opportunity to decline to provide information, as this 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?

For the systems that obtain information from SCIMS, individuals do not have the opportunity to decline to provide information, as this system is maintained by FSA. Members of the public do not have access to this application.

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

For the systems that obtain information from SCIMS, any PII information that is obtained from the SCIMS system, is maintained by FSA.

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?

- 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.)."

- 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 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.)."

- 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.

7.3 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 Privacy Impact Analysis: 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 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.
- 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 MS program is determined via a valid eAuthentication ID and password (level II) on a valid "need to know" basis, determined by requirements to perform applicable official duties and authorized via USDA's Role Based Access Control (RBAC) model for end-user 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?

Yes. Department contractors with a need to know will have access to this application 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 includes 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?

EVA granted an authorization to operate (ATO) on 12/22/2017. EVA was later re-named as NRCS Mission Support.

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. Finally, 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 MS does not directly collect any PII from any individual landowner (i.e., member of the public), but various NRCS systems do utilize PII within their own systems that was obtained from SCIMS, 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 MS is a consolidation of applications into one system.

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 MS 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

Digitally signed by JAKE ZEBELL
Date: 2020.12.17 12:58:46 -07'00'

Jake Zebell
NRCS Mission Support Information System Owner
United States Department of Agriculture

Agency Approval Signature

BRIAN DAVIES

Digitally signed by BRIAN DAVIES
DN: c=US, o=U.S. Government, ou=Department of Agriculture, cn=BRIAN DAVIES, 0.9.2342.19200300.100.1.1=12001000000604
Date: 2020.12.15 18:15:37 -05'00'

Brian Davies
Information Systems Security Program Manager
United States Department of Agriculture

Agency Privacy Approval Signature

Digitally signed by AMBER ROSS
Date: 2020.12.14 08:45:02 -06'00'

Amber Ross
FPAC Privacy Officer
United States Department of Agriculture