Privacy Impact Assessment

National Soils Information System (NASIS)

Revision: 1.0

Natural Resources Conservation Service

Date: June 2007

Template Release 070606

USDA PRIVACY IMPACT ASSESSMENT FORM

Agency: Natural Resource Conservation Service

System Name: National Soils Information System (NASIS)

System Type:
- ☒ **Major Application**
- ☐ **General Support System**
- ☐ **Non-major Application**

System Categorization (per FIPS 199):
- ☐ **High**
- ☒ **Moderate**
- ☐ **Low**

Description of the System:

The National Soil Information System (NASIS) is designed to manage and maintain soil data from collection to dissemination. NASIS provides for data collection at project soil survey offices, management and interpretation of soil information at the soil survey area, state, Major Land Resource Area (MLRA), and national levels. The primary purpose of NASIS is to provide quality soil information to NRCS field offices and conservation partners for conservation planning, conservation effects, conservation practice design, water quality tools, and for dissemination of National Cooperative Soil Survey (NCSS) information to the general public. NASIS also includes the system in which NRCS maintains goals and progress reporting items associated with the national soil survey program. The NASIS application can be accessed at URL http://nasis.usda.gov/.

Who owns this system? (Name, agency, contact information)
Wendell Oaks, Director ITC, USDA-NRCS, Wendell.Oaks@ftc.usda.gov, 970-295-5479

Who is the security contact for this system? (Name, agency, contact information)
Chuck Hart, Information System Security Manager, USDA-NRCS,
Chuck.Hart@ftc.usda.gov, (970) 295-5550.

Who completed this document? (Name, agency, contact information)
Ray Coleman, Systems Security Analyst, USDA NRCS Contractor,
ray.coleman@ftc.usda.gov, 970-2955-5570.

DOES THE SYSTEM CONTAIN INFORMATION ABOUT INDIVIDUALS IN AN IDENTIFIABLE FORM?

Indicate whether the following types of personal data are present in the system

QUESTION 1 Does the system contain any of the following type of data as it relates to individual:	Citizens	Employees
Name	**YES**	**YES**
Social Security Number	**NO**	**NO**
Telephone Number	**YES**	**YES**
Email address	**YES**	**YES**
Street address	**NO**	**NO**
Financial data	**NO**	**NO**
Health data	**NO**	**NO**
Biometric data	**NO**	**NO**
QUESTION 2 Can individuals be uniquely identified using personal information such as a combination of gender, race, birth date, geographic indicator, biometric data, etc.? NOTE: 87% of the US population can be uniquely identified with a combination of gender, birth date and five digit zip code[1]	**NO**	**NO**
Are social security numbers embedded in any field?	**NO**	**NO**
Is any portion of a social security numbers used?	**NO**	**NO**
Are social security numbers extracted from any other source (i.e. system, paper, etc.)?	**NO**	**NO**

If all of the answers in Questions 1 and 2 are NO,

You do not need to complete a Privacy Impact Assessment for this system and the answer to OMB A-11, Planning, Budgeting, Acquisition and Management of Capital Assets, Part 7, Section E, Question 8c is:

3. No, because the system does not contain, process, or transmit personal identifying information.

If any answer in Questions 1 and 2 is YES, provide complete answers to all questions below.

[1] Comments of Latanya Sweeney, Ph.D., Director, Laboratory for International Data Privacy Assistant Professor of Computer Science and of Public Policy Carnegie Mellon University To the Department of Health and Human Services On "Standards of Privacy of Individually Identifiable Health Information". 26 April 2002.

DATA COLLECTION

3. Generally describe the data to be used in the system.

Personal user information including name, telephone, e-mail address and office City and State are maintained within the database. This information is needed to set up the user with access to the NASIS database. The user information is only viewable by the NASIS application users.

4. Is the use of the data both relevant and necessary to the purpose for which the system is being designed? In other words, the data is absolutely needed and has significant and demonstrable bearing on the system's purpose as required by statute or by Executive order of the President.

☒ Yes
☐ No

5. Sources of the data in the system.

5.1. What data is being collected from the customer?

Personal user information including name, telephone, e-mail address and office City and State are maintained within the database. This information is needed to set up the user with access to the NASIS database. The user information is only viewable by the NASIS application users.

5.2. What USDA agencies are providing data for use in the system?

There are several agencies providing data for NASIS including NRCS, USDA Forest Service, Bureau of Land Management (BLM), and other Federal Government agencies.

5.3. What state and local agencies are providing data for use in the system?

Many state units of government (i.e., Department of Natural Resources, etc.) are National Cooperative Soil Survey (NCSS) partners, and contribute soil survey data under the standards established by NRCS as lead for the NCSS.

5.4. From what other third party sources is data being collected?

State Universities and local soil consultants contributing soil survey information to the NCSS.

6. Will data be collected from sources outside your agency? For example, customers, USDA sources (i.e. NFC, RD, etc.) or Non-USDA sources.

☒ Yes
☐ No. If NO, go to question 7

6.1. How will the data collected from customers be verified for accuracy, relevance, timeliness, and completeness?

Data is checked for accuracy and completeness by a combination of automated tools in NASIS and Soil Survey QA processes.

6.2. How will the data collected from USDA sources be verified for accuracy, relevance, timeliness, and completeness?

NRCS, as the lead agency for the NCSS, establishes data quality and completeness standards. Some of the checks are built into the NASIS software and some of the checks are the responsibility of the MLRA Soil Survey Leaders. Data entered into the NASIS system is the responsibility of the user; therefore it is the user's responsibility to ensure data is accurate.

6.3. How will the data collected from non-USDA sources be verified for accuracy, relevance, timeliness, and completeness?

NRCS, as the lead agency for the NCSS, establishes data quality and completeness standards. Some of the checks are built into the NASIS software and some of the checks are the responsibility of the MLRA Soil Survey Leaders. Data entered into the NASIS system is the responsibility of the user; therefore it is the user's responsibility to ensure data is accurate.

DATA USE

7. Individuals must be informed in writing of the principal purpose of the information being collected from them. What is the principal purpose of the data being collected?

To provide quality soil information to NRCS field offices and conservation partners for conservation planning, conservation effects, conservation practice design, water quality tools, and for dissemination of National Cooperative Soil Survey (NCSS) information to the general public.

8. Will the data be used for any other purpose?

☐ Yes
☒ No. If NO, go to question 9

8.1. What are the other purposes?

9. Is the use of the data both relevant and necessary to the purpose for which the system is being designed? In other words, the data is absolutely needed and has significant and demonstrable bearing on the system's purpose as required by statute or by Executive order of the President

☒ Yes
☐ No

10. Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected (i.e. aggregating farm loans by zip codes in which only one farm exists.)?

☐ Yes
☒ No. If NO, go to question 11

10.1. Will the new data be placed in the individual's record (customer or employee)?

☐ Yes
☒ No

10.2. Can the system make determinations about customers or employees that would not be possible without the new data?

☐ Yes
☒ No

10.3. How will the new data be verified for relevance and accuracy?

Not applicable.

11. Individuals must be informed in writing of the routine uses of the information being collected from them. What are the intended routine uses of the data being collected?

To provide quality soil information to NRCS field offices and conservation partners for conservation planning, conservation effects, conservation practice design, water quality tools, and for dissemination of National Cooperative Soil Survey (NCSS) information to the general public.

12. Will the data be used for any other uses (routine or otherwise)?

☐ Yes
☒ No. If NO, go to question 13

12.1. What are the other uses?

13. Automation of systems can lead to the consolidation of data – bringing data from multiple sources into one central location/system – and consolidation of administrative controls. When administrative controls are consolidated, they should be evaluated so that all necessary privacy controls remain in place to the degree necessary to continue to control access to and use of the data. Is data being consolidated?

☒ Yes
☐ No. If NO, go to question 14

Access to personal information is viewable by the system administrators and each NASIS user can view other users' email and phone numbers. The administrators are federal employees or contractors for USDA NRCS. Each administrator has a background investigation, has received Security Awareness Training and completed an Information System Security Computer User Security Agreement. The Privacy Act clause is included in the contractors' contract.

13.1. What controls are in place to protect the data and prevent unauthorized access?

Only authorized NASIS users (authorized through Level 2 eAuthentication ID and NASIS login) have access to the personal data.

14. Are processes being consolidated?

☐ Yes
☒ No. If NO, go to question 15

14.1. What controls are in place to protect the data and prevent unauthorized access?

DATA RETENTION

15. Is the data periodically purged from the system?

☒ Yes
☐ No. If NO, go to question 16

15.1. How long is the data retained whether it is on paper, electronically, in the system or in a backup?

Two days of transaction logs and two days of archives of all databases are kept locally and dumped to tape for off-site storage cycled every other month. Nightly dumps of the database are used for incremental restores and kept 31 days on high speed disks, and 11 months on slower disks. Weekly backups are kept forever (stored by year) on tape off-site.

15.2. What are the procedures for purging the data at the end of the retention period?

Two days of transaction logs and two days of archives of all databases are kept locally and dumped to tape for off-site storage cycled every other month. Nightly dumps of the database are used for incremental restores and kept 31 days on high speed disks, and 11 months on slower disks. Weekly backups are kept forever (stored by year) on tape off-site.

The soil data within NASIS is updated with the most current soil survey information as needed and determined by the authorized soil scientists using the system.

15.3. Where are these procedures documented?

16. While the data is retained in the system, what are the requirements for determining if the data is still sufficiently accurate, relevant, timely, and complete to ensure fairness in making determinations?

NRCS has developed a number of procedures and criteria to determine when a soil survey is in need of an update. The criteria includes land use changes, new uses of soil survey information, and feedback from users of the soil survey information. Transactions logs are maintained to identify updates to the data.

17. Is the data retained in the system the minimum necessary for the proper performance of a documented agency function?

☒ Yes
☐ No

DATA SHARING

18. Will other agencies share data or have access to data in this system (i.e. international, federal, state, local, other, etc.)?

☒ Yes
☐ No. If NO, go to question 19

The soil data within NASIS can be used by other agencies including Federal, State, Local and the public users with access to NASIS data.

18.1. How will the data be used by the other agency?

Only the soil data information can be used.

18.2. Who is responsible for assuring the other agency properly uses of the data?

System Owner

19. Is the data transmitted to another agency or an independent site?

☐ Yes
☒ No. If NO, go to question 20

19.1. Is there the appropriate agreement in place to document the interconnection and that the PII and/or Privacy Act data is appropriately protected?

20. Is the system operated in more than one site?

☒ Yes
☐ No. If NO, go to question 21

The NASIS database provides read only information for the Soil Data Warehouse/Mart which is then used by Web Soil Survey (WSS), the Geospatial Data Warehouse/Mart, the Plant Data Warehouse/Mart and the Natural Resource Data Marts Web Service Access.

20.1. How will consistent use of the system and data be maintained in all sites?

DATA ACCESS

21. Who will have access to the data in the system (i.e. users, managers, system administrators, developers, etc.)?

Administrative personnel have access to personal data for the users. Users have access to the soil data and read only access to the name, phone number and email address of other users. A user can update their own data.

22. How will user access to the data be determined?

The soil data is accessed by the users for their assigned area of responsibility. The user is granted access by the NASIS Coordinator in their region. The access is restricted by roles within NASIS.

22.1. Are criteria, procedures, controls, and responsibilities regarding user access documented?

☒ Yes
☐ No

23. How will user access to the data be restricted?

The user's access is restricted by their location and area of responsibility for soil survey information. The user's access is set up as read only or update depending on their job responsibilities and functions.

23.1. Are procedures in place to detect or deter browsing or unauthorized user access?

☒ Yes
☐ No

24. Does the system employ security controls to make information unusable to unauthorized individuals (i.e. encryption, strong authentication procedures, etc.)?

☒ Yes
☐ No

Access to NASIS is through eAuthentication Level 2, which requires for the user's identity to be verified through a Local Registration Authority (LRA). The user's information is verified during this LRA process. Once the user has eAuthentication Level 2, the NASIS Role can be added. This role allows the use of NASIS, but for read only access. The user is assigned update access by their respective NASIS Coordinator.

CUSTOMER PROTECTION

25. Who will be responsible for protecting the privacy rights of the customers and employees affected by the interface (i.e. office, person, departmental position, etc.)?

Only the NASIS administrators and authorized NASIS users have access to the private information about the NASIS users.

26. How can customers and employees contact the office or person responsible for protecting their privacy rights?

Customers and employees can contact the NRCS Security Response/Access Control Team via the NRCS 800 number and/or e-mail address. Additionally, each state has an Information System Security Point of Contact (ISSPOC) and a State Administrative Officer (SAO) that can be contacted at their Center or State Office.

27. A "breach" refers to a situation where data and/or information assets are unduly exposed. Is a breach notification policy in place for this system?

☒ Yes. If YES, go to question 28
☐ No

27.1. If NO, please enter the POAM number with the estimated completion date:

28. Consider the following:

- Consolidation and linkage of files and systems
- Derivation of data
- Accelerated information processing and decision making
- Use of new technologies

Is there a potential to deprive a customer of due process rights (fundamental rules of fairness)?

☐ Yes
☒ No. If NO, go to question 29

28.1. Explain how this will be mitigated?

29. How will the system and its use ensure equitable treatment of customers?

All NRCS systems/applications are versioned controlled through NRCS and will inherit the security controls of the hosting system/network infrastructure(s).

30. Is there any possibility of treating customers or employees differently based upon their individual or group characteristics?

☐ Yes
☒ No. If NO, go to question 31

30.1. Explain

SYSTEM OF RECORD

31. Can the data be retrieved by a personal identifier? In other words, does the system actually retrieve data by the name of an individual or by some other unique number, symbol, or identifying attribute of the individual?

☒ Yes
☐ No. If NO, go to question 32

The personal data is only used to authorize access for the individual.

31.1. How will the data be retrieved? In other words, what is the identifying attribute (i.e. employee number, social security number, etc.)?

The personal data is only used to authorize access for the individual.

31.2. Under which Systems of Record notice (SOR) does the system operate? Provide number, name and publication date. (SORs can be viewed at www.access.GPO.gov)

Notice of Privacy Act System of Records by Owner, Operator or Producer Files (or Volunteer / Employee Files) USDA/NRCS-1

31.3. If the system is being modified, will the SOR require amendment or revision? NO

TECHNOLOGY

32. Is the system using technologies in ways not previously employed by the agency (e.g. Caller-ID)?

☐ Yes
☒ No. If NO, the questionnaire is complete.

32.1. How does the use of this technology affect customer privacy?

Upon completion of this Privacy Impact Assessment for this system, the answer to OMB A-11, Planning, Budgeting, Acquisition and Management of Capital Assets, Part 7, Section E, Question 8c is:

1. Yes.

PLEASE SUBMIT A COPY TO
THE OFFICE OF THE ASSOCIATE CHIEF INFORMATION OFFICE/CYBER SECURITY

Privacy Impact Assessment Authorization Memorandum

I have carefully assessed the Privacy Impact Assessment for the

National Soil Information System (NASIS)

This document has been completed in accordance with the requirements of the EGovernment Act of 2002.

We fully accept the changes as needed improvements and authorize initiation of work to proceed. Based on our authority and judgment, the continued operation of this system is authorized.

5-16-08

Wendall R. Oaks
System Owner

Date

4-29-08

Mary Alston
NRCS/FOIA/PA Officer

Date

5-16-08

Jack Carlson
NRCS CIO

Date