Privacy Impact Assessment

Windows Pesticide Screening Tool (WIN-PST)

Revision: 1.0

Natural Resources Conservation Service

Date: June 28, 2007

Template Release 070606

USDA PRIVACY IMPACT ASSESSMENT FORM

Agency: **USDA NRCS**

System Name: **Windows Pesticide Screening Tool (WIN-PST)**

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

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

Description of the System:

WIN-PST is a pesticide environmental risk screening tool that NRCS field office conservationists, extension agents, crop consultants, pesticide dealers and producers can use to evaluate the potential for pesticides to move with water and eroded soil/organic matter and affect non-target organisms.

Who owns this system? Wendall R. Oaks, IT Application Development Branch Chief, USDA-NRCS, wendall.oaks@ftc.usda.gov, 970-492-5479.

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

Who completed this document? Sandy Williams, Sr. Systems Security Analyst/CISSM, sandy.williams@ftc.usda.gov, 970-295-5558.

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**	**NO**
Social Security Number	**NO**	**NO**
Telephone Number	**YES**	**NO**
Email address	**YES**	**NO**
Street address	**YES**	**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]	**YES**	**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.

The Cooperator field is the only field where customer data is entered. The depth and extent of the information provided is dependent upon the Local NRCS representative and the customer's input. This data could be as simple as a single name, or as detailed as full name, address, telephone numbers etc. This information is used to identify a specific cooperator's (not necessarily individual) involvement in the project. Other category information described and used within the system application can also be soil and pesticide information. Individual users described for WINPST system application are TSP personnel, NRCS field personnel and the public.

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?

The data could be as simple as a single name, or as detailed as full name, address, telephone numbers etc. This information is used to identify a specific cooperator's (not necessarily individual) involvement in the project.

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

NRCS

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

None

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

EPA (for pesticide information, not an active link)

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?

Customer data is provided to the system through screen data entry by the local NRCS planner. Soil data is provided by the program, no customer data is used other than to identify location of the cooperator if so entered.

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

Data is reviewed by the water quantity and quality team in Portland, OR for accuracy and completeness before incorporating the data into the application. As new data is released, soil and pesticide data is updated.

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

N/A. Only pesticide information collected from EPA. Not an active link

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?

WIN-PST is a pesticide environmental risk screening tool that NRCS field office conservationists, extension agents, crop consultants, pesticide dealers and producers can use to evaluate the potential for pesticides to move with water and eroded soil/organic matter and affect non-target organisms.

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?

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?

WIN-PST is a pesticide environmental risk screening tool that NRCS field office conservationists, extension agents, crop consultants, pesticide dealers and producers can use to evaluate the potential for pesticides to move with water and eroded soil/organic matter and affect non-target organisms.

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

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

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?

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

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?

Contracts entered in the system can have a life up to 30 years. Other files (including Owner, Operator and Producer (Volunteer/Employee) range from 10 years retention to the 30 for contracts. The longevity of the system is not known, but data regularly outlives a particular processing system. Legal requirements for data retention are adhered to, as applicable. There is no set retention period for data within WINPST. It is the users responsibility to modify/delete data when data has expired. Current system data has not reached the retention period specified. When this happens, the usefulness of the data will be evaluated on a case-by-case basis by the user to determine if it should be retained or not.

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

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

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

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

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

The WINPST system is operated at multiple sites. Procedures and processes are in place to ensure continuance of operations and to assure the integrity of the system. Again, this is a client based application and is version controlled through NRCS.

DATA ACCESS

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

Data is only accessible through business applications. Customers have no direct access to the data. No personal identifier required to retrieve data. This is a client based application. All data is stored within the application itself and only the user of the application has access to the data.

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

Any local NRCS representative has access to the data depending on where the data is saved on the system/systems. Criteria, procedures, controls and responsibilities are all identified and defined through NRCS policies and procedures. The WINPST application itself is of public access. However individual data input is solely controlled by users through the client based application.

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

☒ Yes
☐ No

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

Data is only accessible through business applications. Customers have no direct access to the data. No personal identifier required to retrieve data. This is a client based application. All data is stored within the application itself and only the user of the application has access to the data.

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

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.)?

USDA NRCS

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

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

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?

The system is not being modified.

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

Windows Pesticide Screening Tool (WIN-PST)

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.

Wendall R. Oaks
System Owner

5-16-08
Date

Mary Alston
NRCS FOIA/PA Officer

4-29-08
Date

Jack Carlson
NRCS CIO

5-16-08
Date