Privacy Impact Assessment
Integrated Data for Enterprise Analysis (IDEA)

Technology, Planning, Architecture, & E-Government

- Version: 2.02
- Date: July 26, 2013
- Prepared for: USDA OCIO TPA&E

USDA
United States Department of Agriculture

Privacy Impact Assessment for the

Integrated Data for Enterprise Analysis (IDEA)

26 July 2013

Contact Point
TC Patterson
Natural Resources Conservation Service
970-295-5450

Reviewing Official
Lian Jin
Acting Chief Information Security Officer
United States Department of Agriculture
202-720-8493

Abstract

The abstract should be a minimum of three sentences and a maximum of four, if necessary, and conform to the following format:

- First sentence should be the name of the component and system.
- Second sentence should be a brief description of the system and its function.
- Third sentence should explain why the PIA is being conducted.

The Integrated Data for Enterprise Analysis (IDEA) is a system of the Natural Resources Conservation Service (NRCS).

Integrated Data for Enterprise Analysis (IDEA) application provides a one stop location to find integrated agency reports and analysis tools for Natural Resources Conservation Service (NRCS) employees and partners. The IDEA application and supporting technology provides integration of multiple databases, thereby allowing users to compare various types of related information side-by-side that is not currently available in one application. IDEA provides users with real time NRCS data via reports that will be updated and customized as needed.

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 Management Act of 2002 (FISMA) and the E-Government Act of 2002 (Public Law. 107-347, 116 Stat. 2899, 44 U.S.C. § 101, H.R. 2458/S. 803) Federal Law.

Overview

The overview is the most important section of the PIA. A thorough and clear overview gives the reader the appropriate context to understand the responses in the PIA. The overview should contain the following elements:

- The system name and the name of the Department component(s) who own(s) the system;
- The purpose of the program, system, or technology and how it relates to the component's and Department's mission;
- A general description of the information in the system;
- A description of a typical transaction conducted on the system;
- Any information sharing conducted by the program or system;
- A general description of the modules and subsystems, where relevant, and their functions; and
- A citation to the legal authority to operate the program or system.

The NRCS Integrated Data for Enterprise Analysis (IDEA) application provides integrated agency reports and analysis tools for NRCS employees.

The purpose of IDEA is to provide access to comprehensive, integrated business intelligence (BI) to provide for the access, analysis and reporting of NRCS data. IDEA produces financial reports for the costing and budgeting of conservation practices.

Some of these financial reports contain vendor PII that is obtained from the Service Center Information Management System (SCIMS) system via read-only web service calls.

- The PII obtained from SCIMS consists of names and contact information.
- Some of this SCIMS PII is maintained in the IDEA DataMart to ensure efficient performance during the generation of IDEA reports. This PII is refreshed periodically from the SCIMS source system to ensure that it remains current.
- Some of these IDEA reports rely upon transitory read-only vendor PII that is obtained from SCIMS via web service calls, noting that this transitory PII is not maintained in the application database.

Important notes:

- IDEA does not collect any Personally Identifiable Information (PII) from any person.
- While IDEA does not process any transactions, the application allows the user to produce reports using selectable criteria from drop-down menus.
- IDEA does not provide any functionality to retrieve records about individuals by reference to any type of personal identifier.
- NRCS does not, in fact, retrieve records about any individuals from the IDEA database by any reference to any personal identifier.
- IDEA does not process any financial transactions.
- IDEA does not transmit any information to FMMI or any other application.
- Authority to operate IDEA was previously provided via the ATO granted in 2010.

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 IDEA application uses (but does not maintain) a minimal amount of transitory PII that is obtained via SCIMS ID (e.g., vendor information).
- The PII obtained from SCIMS consists of names and contact information.

IDEA Does NOT contain any account number per 7/30/13 0150 PM discussion. BS

- The IDEA application also uses and maintains a minimal amount of SCIMS PII in the IDEA DataMart to ensure efficient performance during the generation of IDEA reports.
- IDEA does not collect any PII within the accreditation boundary.
- IDEA does not disseminate any PII information to any other system.

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

- SCIMS is the source of the PII used in IDEA.

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

- The IDEA application needs to use and maintain the minimal amount of PII that is obtained via SCIMS ID (e.g., vendor information) in order to produce reports for the costing and budgeting of conservation practices.
- IDEA does not collect any PII from any individual.
- IDEA does not disseminate any PII information to any other system.

1.4 How is the information collected?

- N/A – IDEA does not collect any PII from any individual.

1.5 How will the information be checked for accuracy?

- N/A – IDEA does not collect any PII from any individual.
- Note that PII is refreshed periodically from the SCIMS source system to ensure that it remains current.

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

- N/A – IDEA does not collect any PII from any individual.

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

- Note that IDEA does not collect any PII from any individual.
- The only PII data in the application that poses privacy risks is the minimal amount of PII that is obtained via SCIMS ID (e.g., vendor information) to produce reports for the costing and budgeting of conservation practices. This is discussed in the PIA Overview and Section 1.1.

- Privacy risks are mitigated because access to the information will be limited to appropriate NRCS personnel by the use of the USDA-OCIO-eAuthentication application, which provides user authentication for NRCS. Role-Based Access Control (RBAC) provides access enforcement.
- 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.

- The IDEA application uses a minimal amount of PII that is obtained via SCIMS ID (e.g., vendor information) to produce reports for the costing and budgeting of conservation practices. This minimal PII is vendor name and address per PTA Q 4. -BPS

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

- N/A – IDEA does not use any type of tools to analyze PII. No PII data is "produced." PII data is not manipulated or reformatted.

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

- N/A – IDEA does not use commercial or publicly available data.

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.

This application is in compliance with the Federal Information Security Management Act of 2002 (FISMA) as reflected in CSAM, USDA Office of the Chief Information Officer (OCIO) Directives, and National Institute of Standards and Technology (NIST) guidance, including applicable controls provided in these NIST Special Publication 800-53 control families:

- Access Control (AC)
- Security Awareness and Training (AT)
- Identification and Authentication (IA)
- Media Protection (MP)
- Physical and Environmental Protection (PE)

- Personnel Security (PS)
- Risk Assessment (RA)
- System and Communication Protection (SC)
- System and Information Integrity (SI)

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?

- Application-specific information is retained while the application remains in production. Per NARA General Records Schedule 20, application-specific information has been authorized by the NRCS Records Manager for erasure or deletion when the agency determines that this information is no longer needed for administrative, legal, audit, or other operational purposes.
- Note that IDEA does not collect any PII on any individual.

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.

- 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 in Section 1.7 and Section 2.4 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?

- N/A – IDEA does not transmit or share any PII with any other internal USDA organizations.
- While IDEA obtains read-only information related to vendors from SCIMS, IDEA does not share or transmit any information to SCIMS, nor does IDEA update any information in SCIMS.
  - SCIMS vendors (FSA) may include those who assist food product producers with conservation practices. -BPS

4.2 How is the information transmitted or disclosed?

- N/A – IDEA does not transmit or disclose any PII with any other internal USDA organizations.

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.

- IDEA does not "share" PII with any other internal USDA organization.
- Privacy risks are mitigated by virtue of NOT sharing information with other internal USDA organizations.
- 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 information is not transmitted or disclosed externally.

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 information is not transmitted or disclosed externally.

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

- N/A – PII information is not transmitted or disclosed externally.

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

- PII information is not transmitted or disclosed externally. Privacy risks are mitigated by virtue of NOT sharing PII with organizations external to 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 Was notice provided to the individual prior to collection of information?

- N/A – no notice is provided, because no PII is collected from any individual by this application.

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

- N/A – IDEA does not collect any PII from any individual.

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

- N/A – IDEA does not collect any PII from any individual.

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

- Notice does not need to be provided to individuals. There is no risk that an individual would be unaware of "collection," because no PII is collected from any individual by this application.

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?

- N/A – No procedures are required. IDEA does not collect any PII from any individual. The vendors associated with IDEA reports are not allowed access to IDEA.

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

- N/A – IDEA does not collect any PII from any individual. PII is obtained via SCIMS per PIA Q2.1. -BJS

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

- N/A – IDEA does not collect any PII from any individual.

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

- N/A – See 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.

- There are no privacy risks specifically associated with the redress process for this application. No PII is collected from any individual by this application.

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 IDEA application 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. The application 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 IDEA as part of their regular assigned technical support 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, per General Manual, Title 270, Part 409 - Logical Access Control and Account Management.
- Annual Security Awareness and Specialized Training are also required, per FISMA and USDA policy, and this training is tracked by USDA.

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

- Yes. Authority to operate IDEA was granted in 2010.
- An A&A is currently in progress, to be completed by 9/2013.

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

- NRCS complies with the "Federal Information Security Management Act of 2002" (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. Additionally, NRCS complies with the specific security requirements for "auditing measures and technical safeguards" provided in OMB M-07-16. 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).

- 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 Privacy Impact Analysis: 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?

- IDEA does not directly collect any PII from any person, but does utilize PII within the system which is obtained from other sources (see Section 1.0 above). 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 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?

- IDEA is an NRCS custom-developed application that has received an Authorization to Operate (ATO), as discussed in Section 8.4.

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 – 3rd 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 – 3rd 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 – 3rd 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 – 3rd 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 – 3rd 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 – 3rd 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 – 3rd 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 – 3rd 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 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.

- Privacy risks are nominal. IDEA does not provide access or link to 3rd Party Applications. In addition, the system does not use web measurement and customization technology.

Responsible Officials

tc.patterson@usda.gov Digitally signed by tc.patterson@usda.gov
DN: cn=tc.patterson@usda.gov
Date: 2013.07.26 13:25:24 -06'00'

TC Patterson — Date
NRCS
United States Department of Agriculture
This signature certifies that the above PIA responses are provided to the best of my knowledge and understanding.

Approval Signature

7/30/13

Mr. Lian Jin — Date
Acting Chief Information Security Officer
United States Department of Agriculture
This signature certifies that the PTA analysis and PIA determination due diligence has been conducted pursuant to Department guidance and NIST regulations.