Privacy Impact Assessment
Conservation Program Delivery System - Integrated Database for Enterprise

Policy, E-Government and Fair Information Practices

- Version: 1.5.1
- Date: February 18, 2020
- Prepared for: USDA OCIO-Policy, E-Government and Fair Information Practices (PE&F)

United States Department of Agriculture

Privacy Impact Assessment for the

Conservation Program Delivery System - Integrated Database for Enterprise (IDEA)

February 18, 2020

Contact Point

Ken Kinard
FPAC-BC IT Project Manager
970-295-5708

Reviewing Official

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

Abstract

The 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. IDEA is based on comprehensive and fully integrated enterprise business intelligence platforms whose architecture, integration, and simplicity are used by all levels of the organization. The design of IDEA addresses the need to provide for access, analysis and reporting of NRCS data.

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) 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 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 PH 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 PH 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.

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 processes (but does not maintain) a minimal amount of transitory PII that is obtained via SCIMS ID (e.g., vendor information).
- The PH obtained from SCIMS consists of names and contact information.
- IDEA does not contain any account numbers
- The IDEA application also uses and maintains a minimal amount of SCIMS PII in 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 (customer) 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?

- IDEA does **not** collect any PII from any individual

1.5 How will the information be checked for accuracy?

- 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?

- 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 individuals.
- 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-e-Authentication application, which provides access enforcement.
- Please see Section 2.4 and Section 8.6 for further discussion 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’s (customer) name and address per the PTA.

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

- 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.

- 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 2014 (FISMA), USDA Office of the Chief Information Officer (OCIO) Directives, and U.S. National Institute of Standards and Technology (NIST) Special Publication 800-53, Revision 4 guidance: • Access Control (AC)
  - Awareness and Training (AT)
  - Audit and Accountability (AU)
  - Security Assessment and Authorization (CA)
  - Configuration Management (CM)
  - Contingency Planning (CP)
  - Identification and Authentication (IA)
  - Incident Response (IR)
  - Maintenance (MA)
  - Media Protection (MP)
  - Physical and Environmental Protection (PE)
  - Planning (PL)
  - Personnel Security (PS)
  - Risk Assessment (RA)
  - System and Services Acquisition (SA)
  - System and Communication Protection (SC)
  - System and Information Integrity (SI)
- NIST 800-53, Appendix J, Revision 4 controls include: • Authority and Purpose (AP)
  - Accountability, Audit, and Risk management (AR)
  - Data Quality and Integrity (DI)
  - Data Minimization and Retention (DM)
  - Individual Participation and Redress (IP)
  - Security (SE)
  - Transparency (TR)
  - Use Limitation (UL)
- If any residual risks are identified, they will be managed and reported via the FISMA mandated risk assessment processes.
- The controls listed in this section shall be implemented in compliance with Federal and USDA standards regardless of deployment environment.

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 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 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 Sections 1.7 and 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?

- 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.

4.2 How is the information transmitted or disclosed?

- IDEA does **not** transmit or disclose any PII with any other internal USDA organization.

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?

- 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.

- 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?

- 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. Any residual risks are mitigated by the 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 Does this system require a SORN and if so, please provide SORN name and URL.

- This is covered by the NRCS-1 SORN. The NRCS System of Record Notice is accessible at: https://www.ocio.usda.gov/sites/default/files/docs/2012/NRCS1.txt

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

- Notices are not provided, as PII is not collected from any individual by this application.

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

- N/A - PII is **not** collected from any individual by 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?

- N/A - PII is **not** collected from any individual by 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.

- Notices are not provided to individuals. There is no collection of PII from individual, therefore there are no risks.

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?

- Applicable procedures to allow individuals to gain access to their information are maintained by SCIMS (owned by the Farm Service Agency), which is the source of the PII used by this application.

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

- Applicable notification is provided by SCIMS, which is the source of the PII used by this application.

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

- This is managed by the SCIMS Business Unit

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

- This is managed by the SCIMS Business Unit

7.5 Privacy Impact Analysis: Please discuss the privacy risks associated with the redress available to individuals and how those risks are mitigated.

- This is managed by the SCIMS Business Unit

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 e-Authentication 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 FSA Compliance 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, per General Manual, Title 270, Part 409 - Logical Access Control and Account Management
- Annual Security Awareness and Specialized Training and Privacy training, is also required, per FISMA and USDA policy, and is tracked by USDA.

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

- Yes. Most recent Authority To Operate for IDEA was granted in 2017.
- An A&A is currently in progress, to be completed by 12/2020

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 2014" (FISMA). Certification and Accreditation, Annual Key Control self-assessments, and Continuous Monitoring procedures are implemented per law following the U.S. National Institute of Standards and Technology (NIST) Special Publication 800-53, Revision 4 for applications. 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 e-Auth).
  - Access Control: The systems implements least privileges and need to know to control access to PIT (e.g., by RBAC).
  - Authentication: Access to the system and session timeout is implemented for this application (e.g. by e-Auth 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.

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?

- Third party websites and 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.

- Third party websites and 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?

- Third party websites and 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?

- Third party websites and 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?

- Third party websites and 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?

- Third party websites and 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?

- Third party websites and 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)?

- Third party websites and applications are not used

10.10 Does the system use web measurement and customization technology?

- No, IDEA 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?

- No, IDEA does not use web measurement and customization technology

10.12 <u>Privacy Impact Analysis</u>: 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 third party applications. In addition, the system does not use web measurement and customization technology.

Agency Responsible Officials

JAKE ZEBELL Digitally signed by JAKE ZEBELL Date: 2020.02.26 20:04:20 -07'00'

Jake Zebell
IDEA Information System Owner
United States Department of Agriculture

Agency Approval Signature

LANITA THOMAS Digitally signed by LANITA THOMAS Date: 2020.02.28 13:45:33 -05'00'

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

Agency Privacy Approval Signature

AMBER ROSS Digitally signed by AMBER ROSS Date: 2020.03.02 17:05:08 -06'00'

Amber Ross
FPAC Privacy Officer
United States Department of Agriculture