Privacy Impact Assessment
Technical Service Provider Registry (TechReg)

Technology, Planning, Architecture, & E-Government

- Version: 2.01
- Date: July 26, 2013
- Prepared for: USDA OCIO TPA&E

USDA

United States Department of Agriculture

Privacy Impact Assessment for the

Technical Service Provider Registry (TechReg)

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 Technical Service Provider Registry (TechReg) is a system of the Natural Resources Conservation Service (NRCS).

TechReg is an application that provides a means, via the Internet, for qualified individuals, businesses, or public agencies to register to become USDA certified Technical Service Providers (TSPs). TSPs provide technical services to farmers and ranchers on behalf of the USDA. TechReg also includes the Technical Service Payment Rates (TSPR) module.

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 Technical Service Provider Registry (TechReg) application provides the public with a search capability on the TechReg web page to obtain the contact information for Technical Service Providers (TSPs), by location or by the services that they provide.

TSPs provide technical services to farmers and ranchers on behalf of the USDA. The Farm Bill requires that private landowners benefit from a portfolio of voluntary assistance, including cost-share, land rental, incentive payments, and technical assistance.

TechReg collects and uses a minimal amount of PII, consisting of the name and contact information for TSPs. In addition, TechReg assigns and retains a unique TSP ID to each certified technical service provider, and TechReg collects and retains State TSP Service License numbers.

The Technical Service Provider Rates (TSPR) module is an integrated component of the TechReg system and TSPR depends upon the Technical Service Provider Registry (TechReg) application for role management. Likewise, the TechReg application depends upon the TSPR module for TSP rates. TSPR functionality provides a means to view and manage rates that can be charged by Technical Service Providers (TSPs). The TSPR module does not collect, use, disseminate, or maintain any type of PII.

TechReg provide the ability for a TSP to update their profile, including contact information. Other non-PII transactions available in the TechReg web application allow users to find a TSP, become a TSP, track TSP training, complete TSP renewal, register a business, and add categories to TSP Profile.

NOTE: TechReg does not process any financial transactions. TechReg does not transmit any information to FMMI.

Users of this application include qualified individuals, businesses, or public agencies who are (or who seek to become) USDA certified TSPs. The application manages data that can identify TSPs and provide means for contacting the TSP, as well as basic demographic information for monitoring completeness of coverage in the delivery of agency conservation programs. The application also manages data about skills, education, experience and training that qualify persons seeking to become a TSP.

Authority to operate TechReg 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 TechReg application collects, uses and maintains the minimum amount of PII (e.g., name, contact information **(business address- home office may exist)**, license numbers, SCIMS ID) for TSPs.
- TechReg does not disseminate PII information to any other system.

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

- SCIMS is the primary source of the PII used in TechReg.
- TechReg also collects information directly from the TSPs.

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

- The information is collected, used and maintained in order to provide technical services to farmers and ranchers on behalf of the USDA.

1.4 How is the information collected?

- TechReg collects information directly from the TSPs. TechReg also obtains some information from SCIMS via web service calls.

1.5 How will the information be checked for accuracy?

- The accuracy of the PII in the TSP profile (collected directly from the TSP) is checked by the TSP during data entry. This PII is also validated by the National TSP Team during the TSP approval process.
- The accuracy of PII obtained from SCIMS is not within the scope of TechReg. TechReg does not have the ability to update any information in SCIMS.

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

- Federal Register /Vol. 75, No. 27 /Wednesday, February 10, 2010/Rules and Regulations
- Paperwork Reduction Act of 1995 (44 U.S.C. 3501 et seq.)

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

- The only PII data in the application that poses privacy risks is the minimal amount of PII that is used to identify qualified TSPs in order to provide

technical services to farmers and ranchers on behalf of the USDA. 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 and partners 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.

- This information is used to identify qualified TSPs in order to provide technical services to farmers and ranchers on behalf of the USDA.

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

- N/A – TechReg 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 – TechReg 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. **For TechReg, the retention period may vary depending on the business purpose, but typically it is no longer than 10 years.** Per NARA General Records Schedule 20, CPD 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.

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 TSPs. This is mitigated by limited access to the data, non-portability of the data and controlled storage of the data 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?

- N/A – TechReg information is not shared with (or transmitted to) any other internal USDA organizations. While TechReg obtains transitory information related to TSPs from SCIMS, TechReg does not maintain this transitory SCIMS information in the application database. Furthermore, TechReg does not share or transmit any information with SCIMS nor does it update any information in SCIMS.

4.2 How is the information transmitted or disclosed?

- N/A – TechReg information is shared with no 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.

- TechReg does not "share" PII with any 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?

- Yes, notice is provided during the process of registering to become a TSP.

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

- Yes, individuals have the opportunity to decline to provide their PII during the process of registering to become a TSP; however this choice will prevent that user from becoming a TSP.

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

- Yes, individuals have the opportunity to consent to the use of their PII during the process of registering to become a TSP, via the Technical Service Provider Certification Agreement. Failure to consent will prevent that user from becoming a TSP.

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.

- There is no risk that any TSP would be unaware of "collection," because notice is provided during the process of registering to become a TSP.

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?

- Procedures that allow TSPs to gain access to the information in their profile are documented on the TechReg website.
- The TSP is responsible to keep their SCIMS data current. The TechReg website instructs the TSP to correct any errors by contacting their local USDA Service Center to make changes to their SCIMS record. Applicable SCIMS procedures that allow individuals to gain access to their SCIMS information are maintained outside of the accreditation boundary of this application 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?

- Procedures that allow TSPs to correct the information in their profile are documented on the TechReg website.
- The TSP is responsible to keep their SCIMS data current. The TechReg website instructs the TSP to correct any errors by contacting their local USDA Service Center to make changes to their SCIMS record. Applicable SCIMS procedures that allow individuals to gain access to their SCIMS information are maintained outside of the accreditation boundary of this application by SCIMS (owned by the Farm Service Agency), which is the source of the PII used by this application.

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

- Procedures that allow TSPs to correct the information in their profile are documented on the TechReg website.
- 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 (owned by the Farm Service Agency), which is the source of the PII used by this application.

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, because TechReg allows TSPs to gain access to (and correct) the information in their profile on the TechReg website.
- 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 TechReg 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 TechReg 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 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 TechReg 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?

- TechReg does collect information from TSPs. TechReg also utilizes 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. Remediation of privacy risks associated with notice and redress are addressed in PIA Sections 6 and 7 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?

- TechReg 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. TechReg 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 13:17:30 -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.