Privacy Impact Assessment

Technical Service Provider Registry (TechReg) Application

Revision: 1.0

Natural Resource Conservation Service

Date: December, 2009

Document Information

Owner Details	
Name	Frank Geter
Contact Number	(970) 295-5540
E-mail Address	Frank.Geter@ftc.usda.gov

Revision History			
Revision	**Date**	**Author**	**Comments**
1.0	12/17/2009	Brad Gaylord	Initial Draft

Distribution List			
Name	**Title**	**Agency/Office**	**Contact Information**

Table of Contents

1 System Information

System Information	
Agency:	Natural Resources Conservation Service
System Name:	Technical Service Provider Registry (TechReg)
System Type:	☐ Major Application ☐ General Support System ☒ Non-major Application
System Categorization (per FIPS 199):	☐ High ☒ Moderate ☐ Low
Description of System:	TechReg is a major application that provides a means, via the Internet, for qualified individuals, businesses, or public agencies to register to become USDA certified Technical Service Providers (TSP's). TSP's provide technical services to farmers and ranchers on behalf of the USDA. TechReg helps to meet the Farm Bill requirements (and Paperwork Reduction Act) by providing professional and contact information for TSP's in order that interested parties may request their services. The Farm Bill requires that private landowners benefit from a portfolio of voluntary assistance, including cost-share, land rental, incentive payments, and technical assistance.
Who owns this system? (Name, agency, contact information)	Frank Geter, Branch Chief (Natural Resource Data), USDA–NRCS–ITC, Frank.Geter@ftc.usda.gov, (970) 295-5540.
Who is the Project Manager for this system? (Name, agency, contact information)	Ken Rojas, Application Project Manager, USDA–NRCS–ITC, Ken.Rojas@ftc.usda.gov, (970) 492-7326.
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)	Brad Gaylord, Systems Security Analyst, USDA NRCS Contractor, Bradley.Gaylord@ftc.usda.gov, 970-2955-5354.

2 Data Information

2.1 Data Collection

No.	Question	Response
1	Generally describe the data to be used in the system.	Customers of this application include qualified individuals, businesses, or public agencies who are (or who seek to become) USDA certified Technical Service Providers (TSP's). The application manages data that can identify customers and provide means for contacting the customer, 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 Technical Service Provider (TSP).
2	Does the system collect Social Security Numbers (SSNs) or Taxpayer Identification Numbers (TINs)?	☒ Yes ☐ No – If NO, go to question 3. The application uses the SSN or Employer Identification Number (EIN) to search for and extract a SCIMS ID from the Service Center Information Management System (SCIMS) for certain types of business entities. While this functionality is used to search for business entities (e.g., Sole Proprietorships) in SCIMS, it not used to search for individuals.
2.1	State the law or regulation that requires the collection of this information.	None. SSNs and EINs are not retained by the application after the SCIMS ID is extracted.
3	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
4	Sources of the data in the system.	Data is imported from a multi-agency Service Center Information Management System (SCIMS). NRCS is a co-owner of SCIMS. The application aggregates PII from SCIMS within the application's user interface. Note: SSNs and EINs are not stored within any field in the TechReg application database. Customer information can be entered into SCIMS by NRCS employees on an individual basis.
4.1	What data is being collected from the customer?	Data is collected from customers regarding their qualifications for certification as a TSP.

No.	Question	Response
4.2	What USDA agencies are providing data for use in the system?	NRCS.
4.3	What state and local agencies are providing data for use in the system?	None.
4.4	From what other third party sources is data being collected?	None.
5	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 6.
5.1	How will the data collected from customers be verified for accuracy, relevance, timeliness, and completeness?	Data is collected from prospective TSP customers regarding their qualifications for certification as a TSP. Customers are responsible to keep their data current. TSP certifications are good for three years; if the certifications aren't renewed, the data is not publically displayed after this period elapses. Third party agencies who provide licenses and certifications to allow TSPs to meet the criteria for certification have been asked to provide websites where NRCS employees can verify the data. If websites are not available, then they must provide contact phone numbers and staff to certify the TSP data for their agency. Techreg currently requires an authorized NRCS employee to validate each Techreg registration prior to certification. That data is reviewed for completeness through manual review, comparison with existing agency data, and by employees at local offices who have knowledge of the data.
5.2	How will the data collected from USDA sources be verified for accuracy, relevance, timeliness, and completeness?	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.
5.3	How will the data collected from non-USDA sources be verified for accuracy, relevance, timeliness, and completeness?	N/A

2.2 Data Use

No.	Question	Response
6	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?	The data is being collected for the purpose of providing on-line reports for the public, so they can find a certified TSP in their location. TSP's post their information only because they want to become certified to work as a TSP, and to make their information available to potential clients (e.g., farmers and ranchers). They can choose to not use the system, but that will automatically keep them out of this voluntary program, in which they presumably want to be involved. The TSP must sign a certification agreement electronically to complete the application process. This is done within the TSP Profile in TechReg. When an individual applies online for certification as a TSP, the TSP Certification Agreement contains a written Disclosure of On-Line Information which the TSP must agree to, stating that *"I agree that the personal information I enter into my application for certification will be available on-line for public access. I understand that program participants seeking the services of a Technical Service Provider will have access to this information as well as other members of the public that access the Technical Service Provider Web site, TechReg."*
7	Will the data be used for any other purpose?	☐ Yes ☒ No – If NO, go to question 8.
7.1	What are the other purposes?	
8	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
9	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 10. All data collection is known to the customer. The aggregate of all data stored does not produce new revelations except in aggregations that produce agency-level statistics on program delivery.
9.1	Will the new data be placed in the individual's record (customer or employee)?	☐ Yes ☐ No

No.	Question	Response
9.2	Can the system make determinations about customers or employees that would not be possible without the new data?	☐ Yes ☐ No
9.3	How will the new data be verified for relevance and accuracy?	
10	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?	The data being collected is used to provide on-line reports for the public so they can find a certified TSP in their location. The TSP must sign a certification agreement electronically to complete the application process. This is done within the TSP Profile in TechReg. When an individual applies online for certification as a TSP, the TSP Certification Agreement contains a written Disclosure of On-Line Information which the TSP must agree to, stating that *"I agree that the personal information I enter into my application for certification will be available on-line for public access. I understand that program participants seeking the services of a Technical Service Provider will have access to this information as well as other members of the public that access the Technical Service Provider Web site, TechReg."* TechReg also has reports to be used by employees so they can provide technical support to registered and certified TSP's.
11	Will the data be used for any other uses (routine or otherwise)?	☐ Yes ☒ No – If NO, go to question 12.
11.1	What are the other uses?	
12	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 13.
12.1	What controls are in place to protect the data and prevent unauthorized access?	
13	Are processes 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?	

2.3 Data Retention

No.	Question	Response
14	Is the data periodically purged from the system?	☐ Yes ☒ No – If NO, go to question 15.
14.1	How long is the data retained whether it is on paper, electronic, in the system or in a backup?	
14.2	What are the procedures for purging the data at the end of the retention period?	
14.3	Where are these procedures documented?	
15	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?	Data is imported from SCIMS on a daily basis. 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.
16	Is the data retained in the system the minimum necessary for the proper performance of a documented agency function?	☒ Yes ☐ No

2.4 Data Sharing

No.	Question	Response
17	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 18.
17.1	How will the data be used by the other agency?	
17.2	Who is responsible for assuring the other agency properly uses the data?	
18	Is the data transmitted to another agency or an independent site?	☐ Yes ☒ No – If NO, go to question 19.
18.1	Is there appropriate agreement in place to document the interconnection and ensure the PII and/or Privacy Act data is appropriately protected?	
19	Is the system operated in more than one site?	☐ Yes ☒ No – If NO, go to question 20.
19.1	How will consistent use of the system and data be maintained in all sites?	

2.5 Data Access

No.	Question	Response
20	Who will have access to the data in the system (i.e., users, managers, system administrators, developers, etc.)?	System managers, developers, agency field personnel, and NRCS managers will have access to the data in the system. Select information is also provided to the general public for Web browser viewing.
21	How will user access to the data be determined?	The application system controls access to the data by the use of roles that authorize the information that a particular user can view and update. Specific applications and user privileges are assigned to employees and contractors' depending on the user's need-to-know.
21.1	Are criteria, procedures, controls, and responsibilities regarding user access documented?	☒ Yes ☐ No
22	How will user access to the data be restricted?	Customers & Employees do not have direct access to the TechReg database. NRCS employee's access is restricted to specific actions allowed by the software application. Access to specific application web screens is controlled by the eAuthentication and zRoles security systems.
22.1	Are procedures in place to detect or deter browsing or unauthorized user access?	☒ Yes ☐ No The TechReg System Owner identifies very specific access privileges and authority. Each user is restricted to specific actions allowed by the software application. Developers only have access to the systems they are working on. Database administrators control and grant permissions for access to specific databases as authorized by the business application owners.
23	Does the system employ security controls to make information unusable to unauthorized individuals (i.e., encryption, strong authentication procedures, etc.)?	☒ Yes ☐ No System developers design in the appropriate security controls and the IT General Support Systems manage, control and maintain the specified controls.

2.6 Customer Protection

No.	Question	Response
24	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.)?	Privacy and accessibility rules are identified and specified by the Agency management system owners.
25	How can customers and employees contact the office or person responsible for protecting their privacy rights?	The TechReg website instructs the TSP to contact their local USDA Service Center (e.g., to correct errors or make other changes to their SCIMS record).
26	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 27. ☐ No
26.1	If NO, please enter the Plan of Action and Milestones (POA&M) number with the estimated completion date.	
27	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 28.
27.1	Explain how this will be mitigated?	
28	How will the system and its use ensure equitable treatment of customers?	Documentation on the TechReg website informs Technical Service Providers of their civil rights responsibilities.
29	Is there any possibility of treating customers or employees differently based upon their individual or group characteristics?	☐ Yes ☒ No – If NO, go to question 30
29.1	Explain	

3 System of Record

No.	Question	Response
30	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 31 Data is only accessible through business applications, and only to specifically authorized users. Customers do not have direct access allowing retrieval of the data by personal identifier.
30.1	How will the data be retrieved? In other words, what is the identifying attribute (i.e., employee number, social security number, etc.)?	
30.2	Under which Systems of Record (SOR) notice does the system operate? Provide number, name and publication date. (SORs can be viewed at www.access.GPO.gov.)	
30.3	If the system is being modified, will the SOR require amendment or revision?	☐ Yes ☐ No

4 Technology

No.	Question	Response
31	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.
31.1	How does the use of this technology affect customer privacy?	

5 Completion Instructions

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 FOR CYBER SECURITY.

Privacy Impact Assessment Authorization

Memorandum

I have carefully assessed the Privacy Impact Assessment for the

Technical Service Provider Registry (TechReg)
(System Name)

This document has been completed in accordance with the requirements of the E-Government 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.

_____ _____

Frank Geter
ITC Branch Chief (Natural Resource Data)

Date

_____ _____

Mary Alston
NRCS FOIA/PA Officer

Date

_____ _____

Kevin Wickey
NRCS CIO, Acting

Date