Privacy Impact Assessment (PIA)

Farm Production and Conservation (FPAC)

Technical Service Provider Registry (TechReg)

Date Prepared: November 2020

Template Version: FSA-PIA-2013-08-19

Document Information

System Owner Contact Information	
Name	Aaron Lauster
Contact Number	202-260-9230
E-mail Address	aaron.lauster@usda.gov

Document Revision History		
Date MM/DD/YYYY	**Author Name & Organization**	**What was changed?**
03/04/2014	Charlene Niffen – ISO	Initial creation
10/14/2014	Matthew Knechtel – ISO	Initial consolidated PIA
05/02/2018	Darren Smith – ISO	Portfolio realignment
08/26/2020	Sheila Hallinan – FPAC-BC	Review and minor updates for ATO Renewal

Document Review				
Reviewer	Title	Date	Update: Y/N	If systemic, please provide comments

Table of Contents

Purpose of Document

USDA DM 3515-002 states: “Agencies are responsible for initiating the PIA in the early stages of the development of a system and to ensure that the PIA is completed as part of the required System Life Cycle (SLC) reviews…” and “New systems, systems under development, or systems undergoing major modifications are required to complete a PIA.”

This document is being completed in accordance with NIST SP 800-37 Rev 1 which states, “The security plan also contains as supporting appendices or as references to appropriate sources, other risk and security-related documents such as a risk assessment, privacy impact assessment, system interconnection agreements, contingency plan, security configurations, configuration management plan, incident response plan, and continuous monitoring strategy.”

Abstract

Name of the component and system: **Technical Service Provider Registry (TechReg)**

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.

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) (44 U.S.C. §3551 to §3559) and the E-Government Act of 2002 (Pub. Law. 107-347, 44 U.S.C. §101).

Why the PIA is being conducted: To support federal law, regulations and policies.

System Information

System Information	
Agency:	Farm Production and Conservation (FPAC)
System Name (Acronym):	Technical Service Provider Registry (TechReg)
System Type:	☒ Major Application ☐ General Support System ☐ Non-major Application
System Categorization (per FIPS 199):	☐ High ☒ Moderate ☐ Low
Who is the Information System Owner? (Name, agency, contact information)	Aaron Lauster Conservation Planning Branch Chief United States Department of Agriculture FPAC-BC DCWA2 - 6017-S 1400 Independence Ave., S.W. Washington, D.C. 20250 202-260-9230 aaron.lauster@usda.gov
Who is the Information Systems Security Program Manager (ISSPM)? (Name, agency, contact information)	Lanita Thomas United States Department of Agriculture FPAC-NRCS DCWA2 - 1653C-S 1400 Independence Ave., S.W. Washington, D.C. 20250 202-260-8593 lanita.thomas@usda.gov
Who completed this document? (Name, agency, contact information)	Julian Green IT Specialist – FPAC-BC U.S. Department of Agriculture 1400 Independence Avenue SW Washington, DC 20250 202-260-9193 Julian.Green@usda.gov

Overview

System Name: Technical Service Provider Registry (TechReg)

System Description: TechReg is a system of the Natural Resources Conservation Service (NRCS). NRCS provides private landowners with advice, guidance and technical services to carry out conservation practices. The NRCS is an agency within the USDA that has provided over 75 years of leadership in a partnership effort to help America's private landowners and managers. NRCS works with its partners to conserve their soil, water, and other natural resources by providing financial and technical assistance based on sound science and technology suited to a customer's specific needs.

Users of the TechReg 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 a 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.

TechReg helps to meet the Farm Bill requirements (and Paperwork Reduction Act) by providing professional and contract information for TSPs in order that interested parties may request their services. The Farm Bill authorized the use of TSPs and requires that private landowners benefit from a portfolio of voluntary assistance, including cost-share, land rental, incentive payments, and technical assistance.

TechReg provides 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.

TechReg also includes the Technical Service Payment Rates (TSPR) module. The Technical Service Provider Rates (TSPR) module is an integrated component of the TechReg system and TSPR depends upon 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.

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

Legal Authority: This system is regulated by privacy laws, regulations and government requirements, including the Privacy Act (5 U.S.C. §552a); the E-Government Act of 2002 (Pub. Law. 107-347, 44 U.S.C. §101); the Paperwork

Reduction Act of 1995 (44 U.S.C. §3501); the Federal Information Security Modernization Act of 2014 (FISMA) (44 U.S.C. §3551 to §3559); OMB Memos M-03-22, M-10-22, M-10-23, M-16-24, and M-17-12; and OMB Circular A-130, Appendix I.

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?

Information is collected, used, disseminated or maintained in the system.
□ TechReg collects, uses and maintains the minimum amount of PII (e.g. name, contact information (business or home address), education, work experience, license numbers, SCIMS ID) for TSPs. □ TechReg receives PII from the SCIMS database copy (see Section 1.2).

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

Sources of information in the system.
□ Tech Reg collects information from the SCIMS database copy and directly from the TSPs. □ The Service Center Information Management System (SCIMS), maintained by FSA, Service Center Information Management System (SCIMS), CSAM ID # 1672, is the database of customer information that is shared by the three Service Center Agencies, FSA, NRCS, and Rural Development. SCIMS is a repository for USDA business entity and conservation compliance information. This link allows the most current customer information to be printed on forms and letters. It also allows NRCS managers to generate reports on the race, sex, national origin, and disability of program applicants and participants. □ NRCS has access to a copy of the SCIMS database via replication and access to the data from SCIMS for NRCS users is via NPAD and through eAuthentication (eAuth). NRCS users do not have direct access to SCIMS. The landowners and general public applicants may provide information to SCIMS, which is the source of the PII. All information is obtained through a database copy. TechReg does not modify or update any information in SCIMS.

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

Why information being collected, used, disseminated or maintained.
□ TechReg collects, uses and maintains the PII information obtained from the SCIMS database copy to assist NRCS with providing technical services to farmers and ranchers.

1.4 How is the information collected?

How information collected.
□ TechReg collects information directly from the TSPs and also collects information, including the names, addresses, education, work experience, and license numbers, using the SCIMS ID of the affected individual and the SCIMS IDs from the SCIMS database copy. NRCS users do not have a direct access to SCIMS. All information is obtained through a database copy.

1.5 How will the information be checked for accuracy?

How information is checked for accuracy.

□ The accuracy of the information in the TSP profile (collected directly from the TSP) is checked by the TSP during data entry and is validated by the National TSP Team during the TSP approval process.

□ The accuracy of PII obtained from SCIMS or other applications not maintained by NRCS is not within the scope of TechReg. TechReg does not have the ability to update any information in SCIMS, nor does it have the ability to update the information in any other application databases not maintained by NRCS.

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

Legal authority to collect information.

These regulations are applicable:

□ Privacy Act (5 U.S.C. §552a);

□ E-Government Act of 2002 (Pub. Law. 107-347, 44 U.S.C. §101);

□ Paperwork Reduction Act of 1995 (44 U.S.C. §3501)

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

Privacy risks and how mitigated.

□ Privacy risks are mitigated as access to the information will be limited because users are authenticated via the USDA eAuth system and authorized via USDA's role-based authorization for end-user access to the application.

□ 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.

Uses of information.

□ The 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?

Tools used to analyze data and what type of data produced.

□ TechReg does not use any type of tools to analyze PII.

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

Why and how commercial or publicly available data is used.
□ 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.

Controls in place to ensure information is handled in accordance with the above described uses.
□ This application is in compliance with the FISMA and the security and privacy controls provided in the U.S. National Institute of Standards and Technology (NIST) Special Publication 800-53, Revision 4. □ 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?

Time information is retained?
□ All information contained will be retained in compliance with NARA Guidelines, which vary on average in years from less than one year to more than ten years according to the NARA General Records Schedules Transmittal 29, issued December 2017. □ Per the NRCS-1 System of Record Notice (SORN), "Records are maintained as long as the owner, operator, producer, or participant qualifies for conservation programs".

3.2 Has the retention period been approved by the component records officer and the National Archives and Records Administration (NARA)?

Retention period approved by component records officer and National Archives and Records Administration (NARA)?
Yes, in accordance with USDA Directive DR 3080-001: Appendix A: Scheduling Records.

3.3 Privacy Impact Analysis: Please discuss the risks associated with the length of time data is retained and how those risks are mitigated.

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 located 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?

Internal organization(s) in which information is shared, what information is shared and for what purpose?
□ TechReg obtains information related to landowners from SCIMS. TechReg does not share or transmit any information to SCIMS, nor does it update any information in SCIMS. □ TechReg information is shared with Salesforce.

4.2 How is the information transmitted or disclosed?

Information transmittal / disclosure.
□ NRCS has access to a copy of the SCIMS database via replication. Access to the data is through established security rules via eAuth.

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.

Privacy risks associated with the sharing and how they were mitigated.
□ Privacy risks are mitigated by ensuring that access to the data is through established security rules via eAuth. 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?

External organization(s) is the information shared, what information is shared, and for what purpose?
□ N/A- PII is not shared or disclosed with organizations that are external to the USDA.

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.

External PII sharing compatibility and SORN coverage, or legal mechanisms by which system is allowed to share PII.
□ N/A- PII is not shared or disclosed with organizations that are external to the USDA. □ However, TechReg is subject to the NRCS-1 SORN. URL: https://www.ocio.usda.gov/sites/default/files/docs/2012/NRCS-1.txt

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

Externally shared information and security measures.
□ N/A- PII is not shared or disclosed with organizations that are external to the USDA.

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

External sharing privacy risks and mitigation.
□ Privacy risks are mitigated by virtue of NOT sharing information external to the 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?

Individual notice prior to collection of PII information.
□ TechReg is subject to the NRCS-1 SORN. URL: https://www.ocio.usda.gov/sites/default/files/docs/2012/NRCS-1.txt

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

Individual’s right to decline to provide PII information?
□ Yes. NRCS Privacy Policy published on USDA website.

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

Individual’s right to consent to uses of PII and how exercised.
□ Yes, for information that the individuals provide directly to TechReg. The individuals have the opportunity to decline to provide their PII information during the process of registering to become a TSP. □ No, for information that is obtained from the SCIMS system, which is maintained by FSA. Members of the Public do not have access to this application.

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 to individuals and unawareness risk mitigation.
□ Yes, for individuals who provide information directly to TechReg, during the process of registering to become a TSP. Failure to consent will prevent that user from becoming a TSP. □ No, for individuals whose PII information is obtained from the SCIMS system, as that system is maintained by FSA. Members of the Public do not have access to SCIMS.

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?

Individuals access to PII procedures.
□ 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. □ As published in SORN USDA/NRCS-1: “Any individual may request information regarding this system of records, or information as to whether the system contains records pertaining to him/her by contacting the respective district conservationist or other designee. If the specific location of the record is not known, the individual should address his/her request to the Director, Management Services Division, USDA-Natural Resources Conservation Service, P. O. Box 2890, Washington, DC 20013, who will refer it to the appropriate field office. A request for information pertaining to an individual should contain: Name, address,

and other relevant information (e.g., name or nature of program, name of cooperating body, etc.).” □ Any PII information obtained from the SCIMS system would be subject to the applicable procedures to allow individuals to gain access to their SCIMS information, as maintained by the FSA. 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.

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

Correction of erroneous information procedures.
□ 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. □ As published in SORN USDA/NRCS-1: “Any individual may obtain information as to the procedures for contesting a record in the system which pertains to him/her by submitting a written request to the district conservationist or his/her designated representative or to the Director, Management Services Division, USDA-Natural Resources Conservation Service, P.O. Box 2890, Washington, DC 20013.” □ Any PII information obtained from the SCIMS system would be subject to the applicable procedures to allow individuals to gain access to their SCIMS information, as maintained by the FSA. Note that the applicable procedures to allow individuals to gain access to correct their SCIMS information are maintained outside of the accreditation boundary of this application by SCIMS.

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

How individuals notified of correction procedures.
□ 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. □ The SORN USDA/NRCS-1 is published on the USDA.gov website. □ Any PII information obtained from the SCIMS system would be subject to the applicable procedures to allow individuals to gain access to their SCIMS information, as maintained by the FSA. Note that the applicable procedures to allow individuals to gain access to correct their SCIMS information are maintained outside of the accreditation boundary of this application by SCIMS.

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

Alternatives available to individual if no redress.
□ N/A- See section 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.

Privacy risks associated with redress and risk mitigation.
□ Any PII information obtained from the SCIMS system would be subject to the applicable procedures to allow individuals to gain access to their SCIMS information, as maintained by the FSA. Note that the applicable procedures to allow individuals to gain access to correct their SCIMS information are maintained outside of the accreditation boundary of this application by SCIMS. □ 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 procedures and documentation.
□ Access to TechReg application/system is determined via the USDA eAuth system (level II) and authorized via USDA's Role Based Access Control (RBAC) model for end-user access to the application. □ The application/system has documented Access Control Procedures, in compliance with FISMA and USDA directives. See Section 2.4. including specifying authorization for accessing the system. (Refer to Notice IRM-440) In addition, access to FSA web applications is gained via an on-line registration process similar to using the FSA-13- A form. For system specific detailed access see SSP.

8.2 Will Department contractors have access to the system?

Contractor access.
□ Yes. Department contractors with a need to know will have access to this application 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?

User privacy training.

□ NRCS requires that every employee and contractor receives information security awareness training before being granted network and account access, which contains the requisite privacy training, and Annual Security Awareness and Specialized Training, as required by FISMA (NIST SP 800-53 rev 4) and USDA policies (USDA OCIO DR 3545-001 – Information Security Awareness and Training Policy and USDA OCIO DR 3505-003 - Access Control Policy).

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

Certification & Accreditation.

□ Yes. TechReg’s most recent authorization to operate (ATO) is dated on 12/27/2017.

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

Auditing measures and technical safeguards.

□ NRCS complies with the "Federal Information Security Modernization Act of 2014” (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, Rev. 4. Additionally, the system provides technical safeguards to prevent misuse of data including:

o 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).

o Integrity: Masking of applicable information is performed for this application (e.g., passwords are masked by eAuth).

o Access Control: The systems implement least privileges and need to know to control access to PII (e.g., by RBAC). Administrative and management operational controls in place to ensure proper access termination.

o 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).

o Audit: Logging is implemented for this application (e.g. by logging infrastructure).

o 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?

Privacy risks identified and risk mitigation.
□ TechReg does directly collect any PII from TSPs or potential TSPs. □ TechReg utilizes PII within the system, which is obtained from SCIMS, which is maintained by FSA (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 PII information is obtained from the SCIMS database, copied from the SCIMS system, which is maintained by FSA. □ 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?

Project / System type.
□ TechReg is an NRCS custom-developed application.

9.2 Does the project employ technology which may raise privacy concerns? If so, please discuss their implementation.

Technology privacy risks.
□ 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"?

SO and/or ISSPM review of Web guidance.
Yes, no 3rd party website (hosting) or 3rd party application is being used.

10.2 What is the specific purpose of the agency's use of 3rd party websites and/or applications?

Purpose of 3rd-party websites and/or applications?
□ N/A - Third 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.

PII availability through 3rd-party websites and/or applications.
□ N/A - Third 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?

Use of PII available through 3rd party websites and/or applications.
□ N/A - Third 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?

Maintenance and security of PII available through 3rd party websites and/or applications.
□ N/A - Third 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?

Periodic purging of PII available through 3rd party websites and/or applications.
□ N/A - Third 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?

Access to PII available through 3rd party websites and/or applications.
□ N/A - Third 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?

Internal / external sharing of PII available through 3rd party websites and/or applications.

□ N/A - Third 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)?

SORN requirements for sharing of PII available through 3rd party websites and/or applications.
□ N/A - Third party websites / applications are not used.

10.10 Does the system use web measurement and customization technology?

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?

User rights for web measurement and customization technology.
□ N/A - See section 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.

3rd party websites and/or applications privacy risks and mitigation.
□ TechReg does not provide access or link to Third Party websites or applications. In addition, the system does not use web measurement or customization technology.

Appendix A. Privacy Impact Assessment Authorization Memorandum

I have carefully assessed the Privacy Impact Assessment for the Technical Service Provider Registry (TechReg)

Aaron Lauster
TechReg Information System Owner

Date

LANITA THOMAS

Digitally signed by LANITA THOMAS
Date: 2020.12.14 12:52:25 -05'00'

Lanita Thomas
Information Systems Security Program Manager

Date

Digitally signed by AMBER ROSS
Date: 2020.12.14 15:27:48 -06'00'

Amber Ross
FPAC Privacy Officer

Date