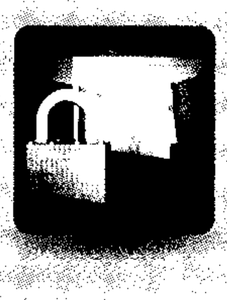
Privacy Impact Assessment

Client Gateway (CG) on Amazon Web Service (AWS)

Technology, Planning, Architecture, & E-Government

- Version: 1.0
- Date: March 26, 2014
- Prepared for: USDA NRCS OCIO CISO



Privacy Impact Assessment for the

Client Gateway (CG) AWS

24 March 2014

Contact Point
Jake Zebell
Natural Resources Conservation Service
970-295-5351

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

Abstract

The Client Gateway (CG AWS) is a system of the Natural Resources Conservation Service (NRCS) that will reside in the Amazon Cloud.
The system has been modified from a commercial off-the-shelf (COTS) product to meet NRCS specifications including alignment with the NRCS environment.

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 Client Gateway (CG AWS) is a system of the Natural Resources Conservation Service (NRCS). The purpose of CG AWS is to provide a system sponsored by Enterprise Business Initiatives (EBI) that is specifically designed to aid farmers, ranchers, landowners and other customers of NRCS who interact with the conservation planners and other specialists at the NRCS.
The PII that is processed and displayed by CG AWS includes contact information for public applicants who have submitted applications or are maintaining agreements. CG AWS will maintain applications that may include typical contact information for applicants. In addition, CG AWS also process and transmit very limited information for NRCS employees and affiliates who are involved with these applications.

The PII information is processed and displayed by CG AWS. This is used to manage applications and agreements through a variety of steps, inputs and workflows. CG AWS follows step by step workflows and processes to enter the data needed to support an application or an agreement. CG AWS allows users within a given role to perform transactions to add or edit applications, as well as to monitor status on existing/active applications or agreements.

CG AWS process and displays a minimal amount of PII about some of the applicants from the CG AWS application database that is used to access transitory read-only PII information from the Service Center Information Management System (SCIMS). Client Gateway **retrieves** processes and displays PII from external dependencies (e.g., SCIMS) to the end user **ONLY.**

The system has been modified from a commercial off-the-shelf (COTS) product to meet NRCS specifications including alignment with the NRCS environment. The PEGA product is within the accreditation boundary of CG AWS. PEGA system is an application platform which allows businesses to solve complex business problems. PEGA system is built on a virtualization layer. On the virtualization layer, PEGA provides NRCS with its own Private Virtual Infrastructure (PVI). The PVI encryption keys are kept on FIPS compliant hardware security appliances in Verizon Terramark location in the United States that are **not** managed by Amazon. Access the keys are exclusively held with the PegaGovCloud administrator.

NRCS administrators will have access to the application level and will maintain access and identification authentication control. PegaGovCloud environment utilizes an active directory domain for centralized identity management for the U.S Pega administrators only.

The Client Gateway application is seeking Authority to Operate in 2014.

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 PII that is processed and displayed by CG AWS includes contact information (name, address, phone, email address) for public applicants who have submitted applications. CG AWS does not maintain contact information—the contact information is maintained in SCIMS.
- CG AWS also maintains limited information for NRCS employees and affiliates who are involved with these applications.
- CG AWS does not disseminate PII information to any other system.
- For further explanation, please refer to the System Description in the CG_AWS SSP.

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

- SCIMS is a source of the PII used in CG AWS for some of the public applicants.
- PII data is also collected by NRCS personnel into "wizard" forms (not within CG AWS), either directly or transcribed from paper application forms. (Wizard forms are data entry forms that move the user to the next form location based on previous entries.)
- CG AWS collects information indirectly from the affected members of the public (i.e., landowners) via external dependencies (e.g., SCIMS). CG AWS does not process any financial transactions, and will never share any type of PII with FMMI. Financial transactions are not a function of CG AWS – this belongs to the application that disperses the money. CG AWS only presents a listing of disbursements that the other application has provided as historical data. In this "financial" regard, CG AWS is a data viewing mechanism only, with that data belonging to other systems.

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

- The information is processed and displayed to aid farmers, ranchers, landowners and other customers of NRCS who interact with the conservation planners and other specialists at the NRCS.
- CG AWS does not directly "collect" PII from landowners.

- CG AWS does not disseminate PII information to any other system.

1.4 How is the information collected?

- PII data is collected by NRCS personnel into "wizard" forms, either directly or transcribed from paper application forms. **This is not done within CG AWS.**
- CG AWS does directly collect PII from landowners (i.e., members of the Public).

1.5 How will the information be checked for accuracy?

- Information in CG AWS is reviewed for accuracy and is verified through manual review and comparison with existing agency data throughout the approval process. This is done by NRCS personnel who have the requisite knowledge and responsibility for the data.
- The accuracy of PII obtained from SCIMS is not within the scope of CG AWS. CG AWS 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?

While CG AWS does indirectly "collect" PII from landowners (via external dependencies), these pertain:

- 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.)
- Rules of engagement exist between Wymond and Amazon to provide PEGA AWS infrastructure support.

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

- CG AWS does indirectly "collect" PII from landowners via external dependencies.
- The only PII data in the application that poses privacy risks is the minimal amount of PII that is used to identify stakeholders (e.g., public landowners) who are involved in new and existing applications. 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. ZRoles Role-Based Access Control (RBAC) provides access enforcement

which is extended by Pega screen or item specific access. No data access is provided to Amazon cloud personnel.
- 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 farmers, ranchers, landowners and other customers of NRCS interacting with conservation planners and other specialists at the NRCS.
- This information is not available to the Amazon cloud provider. This data does not reside in the cloud. No data access is provided to Amazon cloud personnel.

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

- N/A – CG AWS does not use any type of tools to analyze PII. No PII data is 'produced' and 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 – CG AWS 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)
  - Audit and Accountability (AU)
  - 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.
- The controls listed in this section will be implemented in compliance with Federal and USDA standards regardless of deployment environment.
- The Amazon cloud provider is FISMA-compliant.

Section 3.0 Retention

The following questions are intended to outline how long information will be retained after the initial collection. As a U.S. Government provider, PEGA/AWS must be compliant with Federal government/USDA retention regulations.

3.1 How long is information retained?

- Application-specific information is retained while the application (CG AWS) is processing the information (PII) in temporary storage and then is purged/overridden (dispersed because the information (PII) is not stored but only processed). Per NARA General Records Schedule 20, application-specific information has been authorized by the NRCS Records Manager for erasure or deletion when the agency determines that this information is no longer needed for administrative, legal, audit, or other operational purposes.
- Retention is addressed outside the Client Gateway accreditation boundary. The Document Management System (DMS) controls the document retention period. The Customer Toolkit System (CST) manages the record retention.

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

- This is inherited from DMS. CG AWS does not directly control this.

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 members of the public. 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 – CG AWS information is not shared with (or transmitted to) any other internal USDA organizations. While CG AWS obtains transitory information related to some landowners from SCIMS, CG AWS does not maintain this transitory information in the application database. Furthermore, CG AWS does not share or transmit any information with SCIMS nor does it update any information in SCIMS.
- Customer requests to update their SCIM profiles are saved to an NRCS enterprise database outside the CG AWS accreditation boundary. The information is retrieved from CG AWS by authorized NRCS personnel. They view it in CG AWS, but then login to SCIMS and input the information in SCIMS—using the FSA SCIMS application.
- **Note:** We do not have an SLA with SCIMS. However, **SCIMS is the official repository of customer information used by NRCS and other USDA agencies**. The ultimate use of the information from SCIMS is to provide linkage to applications already using SCIMS.
    - SCIMS is outside the accreditation boundary of CG AWS. Information is put into the FSA SCIMS application through FSA-owned application screens.
    - FSA does not allow NRCS or other agencies to have write access to any of their databases.
    - Even read-only access is through screens or services that FSA provides.

4.2 How is the information transmitted or disclosed?

- N/A – CG AWS information is not shared with any other internal USDA organizations.
- CG AWS information is sent by CG AWS Integration Services to enterprise databases (such as NPAD) that are outside the accreditation boundary of CG AWS. NRCS employees access the data in these databases from ProTracts,

Toolkit and other applications according to the roles and restrictions that they have in those applications.

- The essential function of CG AWS is to allow the customers to view their own information—for multiple applications—without the necessity of a trip to the field office. By transferring any input data to enterprise databases, CG AWS does not maintain ownership of any data it receives from the clients. The existing applications have established access controls and data protection for customer information.

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.

- CG AWS does not "share" PII with any other internal USDA organization.
- Privacy risks are mitigated by only processing and displaying (not transmitting to) information from NRCS enterprise databases and maintaining the access controls already in place for the applications that access those databases. CG AWS itself does not need to set up an entire system of access controls that could vary by application.
- 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.
- Information is not shared with Pega or Amazon cloud infrastructure. This data does not reside in the cloud.

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. Since no PII information is contained in CG AWS, no SORN is available. Please see the Source System for the SORN.

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.
- AWS is simply a hosting provider; no external sharing is to take place.

Section 6.0 Notice

The following questions are directed at notice to the individual of the scope of information collected, the right to consent to uses of said information, and the right to decline to provide information.

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

- N/A – No notice is provided to any individual landowner. The indirect collection of PII (via external dependencies) is done prior to access to this application and the individual landowner must agree to the CG AWS usage of this data in order to access CG AWS. The only indirect collection of PII that is present is confirmation of existing PII as correct or requesting a change in incorrect PII.

- The NRCS CPA 1200 form is a document based financial/technical support from NRCS. The NRCS CPA 1200 form is presented with pre-populated SCIMS information (based on their SCIMS ID). The AD 1200 is attached showing the fields that can be pre-populated—all the NRCS CPA 1200 fields, other than Section 1.1 contact information is maintained outside the CG AWS accreditation boundary.

- The information that CG AWS indirectly collects does not reside in the Amazon cloud.

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

- Yes – and access to the application is then also denied. If the applicants want to participate, they must indirectly allow their information to be made available to

CG AWS. Consent to use an individual's information is required in order to indirectly retrieve the information into the application.

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

- N/A – The PII that is indirectly collected from any landowner by this application is upon the individual landowner's request – for changing of incorrect data purposes.

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 landowner would be unaware of "collection," because the landowner is required to manually enter the data, into the external dependencies, which is being collected.

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?

- The individual landowners associated with plans and agreements are only allowed to gain access to CG AWS through a role provided by an authorization mechanism outside of CG AWS (eAuthentication).
- 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 some of the PII used by this application.
- Information is not maintained or shared in the Amazon cloud.

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

- The individual landowners associated with plans and agreements are allowed to gain access to CG AWS through eAuthentication and a role based mechanism, so any PII information processed or displayed in CG AWS is available to the individual landowners themselves (i.e., members of the Public) to request

updates or changes (i.e., "correct") of any inaccurate or erroneous PII information.

- An individual may make a request to correct information through CG AWS. However, any actual information correction takes place in SCIMS. 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 (owned by the Farm Service Agency), which is the source of some of the PII used by this application.
- Information is not maintained or shared in the Amazon cloud.

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

- N/A – no notification is provided related to procedures to allow individual landowners to correct their PII.
- No PII is collected from any landowner by this application directly. See Q 1.3.
- 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 some of the PII used by this application.
- Information is not maintained or shared in the Amazon cloud.

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.
- Residual privacy risks associated with the redress process for individual landowners 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. Detail for the section is addressed in the contract between NRCS and Wymond.

8.1 What procedures are in place to determine which users may access the system and are they documented?

- Access to the CG AWS 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. As a U.S. Government provider, PEGA/AWS must be compliant with Federal government/USDA technical access and security regulations.

8.2 Will Department contractors have access to the system?

- Yes. Department contractors, with a need to know, will have access to CG AWS 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.
- Amazon cloud provider (PEGA/AWS) personnel will have access to the infrastructure, but not to the data itself—enforced via vendor agreement.

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.
- To remind users of their responsibilities (which they acknowledged during their Annual Security Awareness Training), the application reiterates that documents passed to DMS may contain sensitive information, and that this information must not be disclosed to anyone unless the recipient has a direct need-to-know in the performance of their official duties.

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

- CG AWS is seeking an Authorization to Operate (ATO) via an A&A that is currently in progress, to be completed by 8/2014.

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).
    PII data used by the CG Application is **not** stored in the AWS Environment. Client Gateway **does not** own any data outside of workflow data. In the process of providing workflow steps through a user interface, Client Gateway **retrieves** processes and displays PII from external dependencies to the end user **ONLY**. See Q3.1—the PII information is not stored but only processed.
  - 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). The encryption keys are kept on FIPS compliant hardware security appliances in Verizon Terramark location in the United States that are **not** managed by Amazon. Access the keys are exclusively held with the PegaGovCloud administrator.
  - 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 end to end for this application (e.g. by logging infrastructure). All audit logs from the PVI instance and Pega's Network Operation Center (NOC) environments are centrally located in our Splunk event management system for routine audit tracking.
  - 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?

- CG AWS does not directly "collect" any PII from any landowner, or "share" (internally or externally) any PII, 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 process 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?

- CG AWS is an NRCS COTS (Pega) application that is seeking 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.
- The Amazon cloud is an infrastructure provider and does not control the application. Third party infrastructure does not apply as PEGA/AWS will not be controlling.

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. No web measurement or customization will be occurring at the applicatioan level.

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 <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. CG AWS does not provide access or link to 3rd Party Applications. In addition, the system does not use web measurement and customization technology.

Responsible Officials

jason.zebell@usda.gov

Digitally signed by jason.zebell@usda.gov
DN: cn=jason.zebell@usda.gov
Date: 2014.04.03 08:12:14 -06'00'

Jake Zebell
NRCS
United States Department of Agriculture

Date

This signature certifies that the above PIA responses are provided to the best of my knowledge and understanding.

Approval Signature

MICHAEL SHEAVER

Mr. Lian Jin
Acting Chief Information Security Officer
United States Department of Agriculture

Date

This signature certifies that the PTA analysis and PIA determination due diligence has been conducted pursuant to Department guidance and NIST regulations.