Office of the Chief Information Officer
U.S. DEPARTMENT OF AGRICULTURE

USDA Privacy Impact Assessment

Fiscal Year 2025

Privacy Division (PD)
Cybersecurity and Privacy Operations Center (CPOC)
U.S. Department of Agriculture

Revisions

Date	Version	Notes
09/06/2023	1.0	Documented created.
02/12/2025	1.1	Removed “Gender” and “Sexual Orientation” from Biographical Information in accordance with Executive Order 14168, “Defending Women from Gender Ideology Extremism and Restoring Biological Truth to the Federal Government.”

Table of Contents

Privacy Impact Assessment for the USDA IT System/Project

Detail	Information
System/Project Name	10CIO
Program Office	OCIO
Mission Area	CEC
CSAM Number	2330
Date Submitted for Review	9/11/2025

Mission Area System/Program Contacts

Role	Name	Phone Number
MA Privacy Officer	Hugh Woolard	816-926-3446
Information System Security Manager	Robert Lee	910-431-8634
System/Program Managers	Christopher Stewart	816-823-2798

Abstract

This is a Front-end SSP for a cloud system comprised of two applications running on FedRAMP authorized information systems, the Project Host OneSpan (eSignLive) and the SalesForce Government Cloud Plus systems. Both systems are recognized as Cloud Services Providers (CSP) delivering FedRAMP SaaS compliant cloud solutions for U.S. government agencies and are built on FedRAMP authorized platforms.

Overview

SalesForce provides a 1OCIO Customer Community portal where OCIO customers can access their Inter-Agency Agreements (7600A), Orders (7600B), quotes, and invoices through List Views, Reports, and Dashboards.

OneSpan provides electronic/digital signature functionality to include document package preparation, signature routing, tracking, and notification services.

Section 1: Authorities and Other Requirements

These questions identify all statutory and regulatory authorities for operating the project, application, or system, including the authority for collection, which SORN applies, if an ATO has been completed, and if there is Paperwork Reduction Act coverage:

What legal authorities and/or agreements permit the collection of information by the project, application, or system?

Collection of information by USDA personnel will be governed by the Clinger-Cohen Act of 1996 and the E-Government Act of 2002.

Has Authorization and Accreditation (A&A) been completed for the project, application, or system?

Submitted 12/2/2025.

Which System of Records Notices (SORNs) apply to the information?

None. A SORN is not required because it is not the source system. The source systems are required to meet the Privacy Act requirements of a SORN, if applicable.

Is the collection of information covered by the Paperwork Reduction Act?

No

Section 2: Information Characterization

These questions define the scope of the information requested and collected, as well as the reasons for its collection as part of the project, application, or system being developed:

What information is collected, used, disseminated, or maintained in the project, application, or system? PII is defined as information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual.

Identifying Numbers:

- Business mobile phone number (sole proprietor)
- Personal mobile phone number

Biographical Information:

- Name (including nicknames)
- Personal email address
- Business phone or fax number (sole proprietor)
- Business email address
- Home phone or fax number

Distinguishing Features:

- Signature

What are the sources of the information in the project, application, or system?

Sources are manual input by users.

How is the information collected?

The information is collected and maintained in order to automate and facilitate the process of creating MOU agreements and Financial Agreements (Form 7600 A and 7600 B). The information includes the Master List of CEC, NITC, ENS and Appropriations Customers and Contacts as well as Services offered by OCIO to its clients.

Does the project, application, or system use information from commercial sources or publicly available data? If so, explain why it is used.

Public data can be used by Client Executive team members to plan their activities such as calls or visits to potential clients.

How will the information be checked for accuracy? How often will it be checked?

The information should be checked for accuracy by the user. There is currently no formal audit process in place to assure accuracy of each record.

Does the project, application, or system use third-party websites?

No

What is the purpose of the use of third-party websites?

None

What PII will be made available to the agency though the use of third-party websites?

N/A

Privacy Impact Analysis: Related to the characterization of the information.

Privacy Risk

- **Misclassification of Data**: Incorrectly categorizing PII which can lead to inadequate protection measures, exposing sensitive data to unauthorized access or misuse.

Mitigation

- Adhere to departments data classification policy that categorizes PII based on sensitivity and the potential impact of unauthorized access or disclosure.
- Information collected on the 1OCIO system may include (but not be limited to) full names, Personal Phone and work numbers and e-mail address. The actual information collected will be from all fields held within the USDA Enterprise Active Directory (EAD) that is used to synchronize data with Microsoft; therefore, the above fields are just examples.
- The information for USDA personnel will be protected using all moderate impact security controls required by National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 4, Recommended Security Controls for Federal Information Systems and OMB A123 Appendix A, Management's Responsibility for Federal Information Systems guidance and controls.

Section 3: Information Uses

These questions delineate the use of information and the accuracy of the data being used.

Describe why and how the information collected, used, disseminated and/or maintained will support the project, application, or system's business purpose.

Information collected in 1OCIO is used to generate MOU and Financial Agreements (7600 A and B forms.)

The information related to Inventory Counts and Performance Metrics that is loaded from internal CEC systems via MuleSoft interface is displayed on Community Portal. It can be viewed and downloaded by CEC clients who have access to Community Portal.

Does the project, application, or system use technology to conduct electronic searches, queries, or analysis in an electronic database to discover or locate a predictive pattern or anomaly? If so, state how USDA plans to use such results.

Out-of-the box reporting functionality of Salesforce can be used to analyze data stored in the system. The data can be also downloaded into Excel by users who have download permission.

Public data can be used by Client Executive team members to plan their activities such as calls or visits to potential clients.

Privacy Impact Analysis: Related to uses of the information.

Privacy Risk

- **Unauthorized Use of Data**: PII may be used for purposes other than those for which it was collected, violating privacy principles and user expectations.
- **Data Misuse**: Employees or third parties may misuse PII, either intentionally or unintentionally, leading to breaches of confidentiality and trust.

Mitigation

- **Purpose Limitation**: Clearly define and communicate the specific purposes for which PII is collected and used, ensuring that it is not used for unrelated purposes without consent.
- **Data Minimization**: Collect and use only the minimum amount of PII necessary to achieve the intended purpose, reducing the risk of misuse.

Section 4: Notice

These questions are intended to provide notice to the individual of the scope of information collected, the right to consent to use of the information, and the right to decline to provide information.

How does the project, application, or system provide notice to individuals prior to collection?

The individual's information would be logged in the Contact Object (name, address, title, company, and phone number.) Individuals (Contacts) have not been notified that their information is stored in 1OCIO.

What options are available for individuals to consent, decline, or opt out of the project?

No, individuals can opt out from receiving communications from 1OCIO. They cannot decline being entered as a Contact into the system. No private info as shared as part of Contacts record (social security numbers or birthdate).

No. Except for "opting" out from receiving marketing materials.

Privacy Impact Analysis: Related to notice.

Privacy Risk

- **Inadequate Disclosure**: Notices may fail to adequately inform individuals about how their personal information will be collected, used, and shared, leading to misunderstandings about privacy practices.

Mitigation

- The exact mechanism may be slightly different for each government client. The risk to the individual is very low. The user must acknowledge the informed consent provisions with a signature during the new account request process. The information collected is not considered to be PII and there is no perceived risk.
- Ensure that privacy notices are written in clear, accessible language which avoids legal jargon to make it understandable for all users.

Section 5: Data Retention

These questions outline how long information will be retained after the initial collection.

What information is retained and for how long?

The information is retained as needed in Salesforce and can also be archived. It is archived for 3 years then customer data is deleted if not used at the end on that retention period.

Has the retention schedule been approved by the USDA records office and the National Archives and Records Administration (NARA)? If so, indicate the name of the records retention schedule.

N/A, see response to question 1.3.

Privacy Impact Analysis: Related to data retention.

Privacy Risk

- **Excessive Data Retention**: Retaining PII longer than necessary can violate data minimization principles, increasing the risk of unauthorized access and exposure.
- **Data Breaches**: The longer PII is retained, the greater the risk of data breaches occurring, whether through hacking, accidental disclosures, or insider threats.

Mitigation

- Use NARA data retention policies that outlines how long different types of PII will be retained and the rationale for those timeframes and ensure sufficient storage space is available.

Section 6: Information Sharing

These questions define the content, scope, and authority for information sharing.

With which internal organizations and/or systems is information shared, received, and/or transmitted? What information is shared, received, and/or transmitted, and for what purpose? How is the information transmitted?

External Customers (Contacts from Other Agencies that are clients of CEC) can access the information about Inventory and Performance Metrics report by logging to Community Portal. They can review their information and compare with their own records.

See 4.1. Community Portal users can only download Inventory Data associated with their own Agency.

List the privacy risks and mitigations related to internal information sharing and disclosure.

Privacy Risk

- **Unauthorized Access**: Employees may access PII without proper clearance, leading to potential misuse.
- **Data Breaches**: Internal systems can be vulnerable to breaches, compromising PII.

Mitigation

- Access Controls: Implement role-based access controls to limit who can access PII based on their job responsibilities.

With which external organizations (outside USDA) is information shared, received, and/or transmitted? What information is shared, received and/or transmitted, and for what purpose? How is the information transmitted?

None. The information in Opportunity, MOU, IAA and Order objects will be only visible to internal users of 1OCIO. Information in Inventory and Performance Metrics objects is shared with Community Portal users. Access to the Community Portal is controlled by CEC (they can create or delete Community Portal Users.)

While OCIO-CEC has no System of Records, many of the client organizations that OCIO-CEC support have business functions that require a System of Records. Mere maintenance of information about an individual is not enough to trigger the SORN requirements of the Privacy Act, although it is enough to trigger the conduct of a privacy impact assessment (PIA). To trigger the SORN requirements of the Privacy Act, information must actually be retrieved by a personal identifier. The information that is shared in the 1OCIO System is compatible with the intent of the original collection — to create/maintain user accounts, in accordance with the contractual Statement of Work.

All data transmission sessions are conducted with secure transmission protocols utilizing either SSL configured with valid third-party certificates from trusted sources or FIPS 140-2 validated encryption modules to protect the confidentiality and integrity of remote access sessions.

List the privacy risks and mitigations related to external information sharing and disclosure.

Privacy Risk

- **Unauthorized Access**: Sharing PII with third parties increases the risk of unauthorized access, especially if those parties do not have adequate security measures in place.

Mitigation

- Establish written agreements or contracts with third parties that outline their responsibilities for safeguarding shared data and compliance with privacy laws.
- For the information that is shared externally via Community Portal (Inventory and Performance Metrics) there is a sharing rule implemented in Salesforce that will restrict the info available to user based on the Agency to which they belong. I.e. Rural Development agency representative will only see the records of Rural Development Agency. The users must go via SSO to log into 1OCIO. Both internal and Community users must have a Salesforce license and SSO to be able to log in.

Section 7: Redress

These questions address the individual's ability to ensure the accuracy of the information collected about him or her.

What are the procedures that allow individuals to gain access to their information?

Users authenticate to Salesforce through the eAuth PIV card authentication, which is tied to Windows Active Directory architecture, under the Accredited & Authorized Enterprise Active Directory (EAD) major application information system (CSAM #2330).

What are the procedures for correcting inaccurate or erroneous information?

Data Stewards group has been set up with four individuals from each team: CEC, EASB, FEB and FMB. This group will be tasked with ensuring with data accuracy. The process around that will still need to be established.

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

During the new user request process users are informed of their right to correct or update information at any time. Customers are responsible for the accuracy and currency of any PII that they provide while using 1OCIO.

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

The user has the right to correct or update information at any time. Customers are responsible for the accuracy and currency of any PII that they provide while using 1OCIO.

Privacy Impact Analysis: Related to redress.

Privacy Risk

- **Inadequate Processes**: If the processes for individuals to seek redress for privacy violations are unclear or cumbersome, it can deter individuals from exercising their rights and lead to unresolved complaints.
- **Lack of Transparency**: Not providing clear information about how redress mechanisms work can create confusion and mistrust among individuals regarding their rights and the agency's accountability.

Mitigation

- Develop and communicate clear procedures for individuals to submit complaints or requests for redress related to privacy violations.

Section 8: Auditing and Accountability

These questions describe technical safeguards and security measures:

How is the information in the project, application, or system secured?

The 1OCIO Access Control are provided by CEC-Enterprise Active Directory (EAD). Users must authenticate to EAD through a domain trust, before accessing the 1OCIO system. Account management for the access and use of 1OCIO is governed by the SAAR process, with accounts created in EAD. 1OCIO SSP details which groups have access to the various components of the system based on their relevant roles.

What procedures are in place to determine which users may access the project, application, or system, and are they documented?

Users can gain access provided they have been given Salesforce license and that they have Fed ID/SSO.

How does the project, application, or system review and approve information sharing requirements?

N/A.

Describe what privacy training is provided to users either generally or specifically relevant to the project, application, or system.

OCIO CEC provides security and awareness training to personnel managing the 1OCIO system for employees/contractors on an annual basis.