Privacy Impact Assessment
1OCIO

- Version: 1.1
- Date: June 5, 2019
- Prepared for: USDA OCIO Privacy Office

USDA

United States Department
of Agriculture

Privacy Impact Assessment for the

1OCIO

June 5, 2019

Contact Point

Valencia Fulwood
Product Owner, 1OCIO
Program Manager, OCIO – Client Experience Center (Contractor – Newberry Group)
(301) 504-2482

Reviewing Official

Janell Duke
OCIO-CEC-GSD-SCSB, Director
United States Department of Agriculture
(260) 624-2940

Abstract

The abstract should be a minimum of three sentences and a maximum of four, if necessary, and conform to the following format:

- First sentence should be the name of the component and system.
- Second sentence should be a brief description of the system and its function.
- Third sentence should explain why the PIA is being conducted.

CEC 1OCIO

This is a Front-end SSP for a cloud system comprised of three FedRAMP authorized information systems, the Federal Private Cloud for SalesForce, Spring Cloud (SpringCM) and eSignLive systems. This is being completed due to the nature of the data being collected described in the PTA.

Overview

The overview is the most important section of the PIA. A thorough and clear overview gives the reader the appropriate context to understand the responses in the PIA. The overview should contain the following elements:

- The system name and the name of the Department component(s) who own(s) the system;
- The purpose of the program, system, or technology and how it relates to the component's and Department's mission;
- A general description of the information in the system;
- A description of a typical transaction conducted on the system;
- Any information sharing conducted by the program or system;
- A general description of the modules and subsystems, where relevant, and their functions; and
- A citation to the legal authority to operate the program or system.

This is a Front-end SSP for a cloud system comprised of three FedRAMP authorized information systems, the Federal Private Cloud for SalesForce, the Spring Cloud (SpringCM) system and the eSignLive application for electronic signatures. All three systems are recognized as Cloud Services Providers (CSP) delivering FedRAMP SaaS compliant cloud solutions for U.S. government agencies and are built on the FedRAMP authorized Salesforce platform.

SpringCM provides cloud document management and workflow solutions. eSignLive is an app for sending documents for electronic signature.

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?

Name, and hand writing or image of the signature

Information used in creating Enterprise Agreements and Financial Agreements (7600 A and B Forms) between CEC and its clients (other USDA Agencies)

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

Sources are manual input by users.

Client Executive Team (Rory Schultz)

Enterprise Agreement Services Branch (Nadim Ahmed)

Business Services Division, Financial Execution Branch (Christine Mikkelsen)

Business Services Division, Financial Management Branch (Chris Stewart)

There are also data loads that feed into 1OCIO via MuleSoft interfaces. These data represent Inventory counts and Performance Metrics for CEC. The data feeds bring in NITC customer's resource usage information so they can be invoiced.

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

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.

1.4 How is the information collected?

The information has been collected via previous working relationships (Accounts, Contacts) and via entering daily transactions into the system (Leads, Opportunities, MOU, IAA and Order records)

The information also contains the word and PDF documents that are generated by the system based on Salesforce records (these are MOU documents in Word and 7600 Forms in PDF.)

1.5 How will the information be checked for accuracy?

The information should be checked for accuracy by the user. There is currently not formal audit in place to assure accuracy of each record.

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

Collection of information by USDA personnel will be governed by the Clinger-Cohen Act of 1996 and the E-Government Act of 2002. Guidance can be found in Appendix III to 0MB Circular No. A-130 and NIST SP-800-30, Risk Management Guide for Information Technology Systems.

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

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 A-123 Appendix A, Management’s Responsibility for Federal Information Systems guidance and controls.

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.

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.

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

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.

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

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.

For the Contact records, there is a setting where the user can “opt out” from receiving emails from 1OCIO.

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?

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.

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

Yes

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

Risks can be mitigated by buying more storage and archiving data using full Salesforce Org Data Extract on request.

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?

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 need to view their information and compare with their own records. Please contact Robin Reynold and Nadim Ahmed from FMB for further explanation how the info is used.

4.2 How is the information transmitted or disclosed?

See 4.1. Community Portal users can download the reports. They can only see Inventory Data associate with their own Agency.

4.3 <u>Privacy Impact Analysis</u>: Considering the extent of internal information sharing, discuss the privacy risks associated with the sharing and how they were mitigated.

Policies and procedures designed to protect the privacy of PII are defined in sections PS-1, AT-1, and AU-1 in the SSP. The System Owner is responsible for the implementation of the policies and procedures. The same moderate impact NIST 800-53, Revision 4 security controls will be used for all components that hold data within the CEC accreditation boundary.

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?

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. Who has access to the Community Portal is controlled by CEC (they can create or delete Community Portal Users.)

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.

No. 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. Use an Interconnection Security Agreements (ISA) to share data between interconnected systems. Refer to the processes and procedures defined in NIST SP 800-47, Security Guide for Interconnecting Information Technology Systems, or its replacement.

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

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.

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

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 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 Does this system require a SORN and if so, please provide SORN name and URL.

No

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

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

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

No, they 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)

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

No. Except for “opting” out from receiving marketing materials.

6.5 Privacy Impact Analysis: Describe how notice is provided to individuals, and how the risks associated with individuals being unaware of the collection are mitigated.

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.

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?

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).

7.2 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.

7.3 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.

7.4 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.

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 additional privacy risks associated with the redress. Customers are responsible for the accuracy and currency of any PII that they provide while using 1OCIO.

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?

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.

8.2 Will Department contractors have access to the system?

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

8.3 Describe what privacy training is provided to users either generally or specifically relevant to the program or system?

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

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

In Progress.

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

The 1OCIO system uses the baseline moderate impact security controls from NIST SP 800-53 Revision 4 in establishing security mechanisms to protect the system. This includes border protection, auditing and alerting for tracking and monitoring events on the system.

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?

The information collected to support the use of the service is general information on users. The moderate impact NIST 800-53, Revision 4 security controls have been implemented on the system to protect the data within the CEC 1OCIO accreditation boundary.

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?

All systems (Salesforce, SpringCM, eSignLive) are recognized as Cloud Services Providers (CSP) delivering FedRAMP SaaS compliant cloud solutions for U.S. government agencies and are built on the FedRAMP authorized Salesforce platform.

.

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

1OCIO is comprised of FedRamp accredited cloud services consistent with a FIPS 199 Moderate rating. Potential damage to the agency and its personnel should not exceed the criteria established by the government in its FIPS 199 Moderate classification.

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?

There are no Third-party websites or applications

10.3 What personally identifiable information (PII) will become available through the agency's use of 3rd party websites and/or applications.

None

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

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

10.6 Is the PII that becomes available through the agency's use of 3rd party websites and/or applications purged periodically?

No

If so, is it done automatically?

<< ADD Answer Here >>

If so, is it done on a recurring basis?

<< ADD Answer Here >>

10.7 Who will have access to PII that becomes available through the agency's use of 3rd party websites and/or applications?

No

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?

No

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)?

No

10.10 Does the system use web measurement and customization technology?

No

If so, is the system and procedures reviewed annually to demonstrate compliance to OMB M-10-23?

<< ADD Answer Here >>

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?

No

If so, does the agency provide the public with alternatives for acquiring comparable information and services?

<< ADD Answer Here >>

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.

None

Responsible Officials

JANELL DUKE Digitally signed by JANELL DUKE
Date: 2019.06.17 11:34:05 -05'00'

Janell Duke – Director, OCIO-CEC-GSD-SCSB

United States Department of Agriculture

Approval Signature

NANCY HERBERT Digitally signed by NANCY HERBERT
Date: 2019.06.16 16:47:31 -05'00'

Nancy
Herbert
OCIO-CEC-GSD-SCSB, ISSPM
United States Department of Agriculture