# Privacy Impact Assessment (PIA)

## OneUSDA Contact Center

OneUSDA Contact Center COE

- Date: March, 26th, 2019
- Prepared for: USDA

United States Department of Agriculture

| Document Revision and History | | | |
|---|---|---|---|
| **Revision** | **Date** | **Author** | **Comments** |
| Draft | 3/26/2019 | Adam Murgittroyd | Initial draft for OneUSDA Contact Center |
| Draft | 4/8/2019 | Adam Murgittroyd | Updates from USDA Detailees |
| Draft | 5/10/2019 | Adam Murgittroyd | Updates from preliminary ATO review |
| Draft | 6/12/2019 | Adam Murgittroyd | Updates from Checklist of PIA/PTA review |
| | | | |
| | | | |

# Abstract

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

- OneUSDA Contact Center is Salesforce Government Cloud Integrated platform using Service Cloud module
- Public facing community knowledge base provides unauthenticated public users the ability to self-service existing USDA agency knowledge articles to learn about agency offerings/ programs. Provides for the relevant public updates of existing knowledge; and programs that provides government personnel the tools to review and manage an evolving knowledge base.
- Customers can submit case inquiries through multiple channels: phone, email, chat and webform and government personnel can support all these channels through a single integrated platform
- Integration Bucher & Suter (B+S) Connector, a Salesforce Native Managed Package, compliant and certified by Salesforce to work with Government Cloud. It works within the USDA's current call center technology landscape, connecting with Cisco Finesse Server through CSR's browser to Salesforce for routing telephony calls. B+S Connects is used actively by two known federal applications.

# 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:

OneUSDA Contact Center – Contact Center COE

The OneUSDA Contact Center will support the operational and analytical needs of USDA COE contact center consolidation effort. The major goals of this initiative are to develop a platform that:

1. Allows the public to self-service knowledge articles about the programs, initiatives and agencies of USDA
2. Interfaces with the public and collects customer inquiry information regarding USDA agencies
3. Provides government personnel the integrated systems and process tools needed to fully support contact center interactions. This system will collect name, phone number and email address of the inquiring person.
4. Provides the integrated systems and process tools needed to transfer inquiry cases to other USDA contact centers

The OneUSDA contact center may replace the existing contact centers that interfaces with the public and supports customer inquiries into USDA. The system will leverage existing USDA platforms including a new instance (org) of Salesforce and extension of Cisco Unified Contact Center.

The OneUSDA Contact Center Application is comprised of a publicly facing web portal leveraging the Salesforce Customer Community Cloud that will be accessed by unauthenticated customers.

This system will be integrated with Identity, Credential and Access Management (ICAM) system to enable single sign-on for authorized OneUSA Contact Center Customer Service Representatives (federal employees).

A typical transaction in the system would be for customers inquiring into OneUSDA the capability to create case/ticket through different communication channels (phone, email, webform, or chat).

- Any information sharing conducted by the program or system;
- Information that can be shared with general public through knowledge articles; and customers' name, phone number as well as email address with other mission areas when escalating an inquiry to tier-2 or tier-3. This sharing will be either within the SalesForce system or through emails or phone call without any system interconnectivity,
- 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 provided by 7 U.S.C. 1431 and 2018 Farm Bill, Public Law No: 115-334.

# 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? PTA questions 7&8

- First Name of the person contacting USDA
- Last Name of the person contacting USDA
- Phone number of the person contacting USDA
- Email address of the person contacting USDA
- Address of the of the person contacting USDA
- Knowledge Articles from various mission areas explaining USDA programs and other public information.
- General Inquiry Case Information (Subject, Description – Inquiry Details/Case History, Case Number, Contact, Account, Nature of Inquiry)

### 1.2 What are the sources of the information in the system? PTA questions 7, 11 & 12.

- User supplied information in OneUSDA Contact Center (USDA system)
- Knowledge Articles, FAQs – existing knowledge bases and other documentation.
- USDA Cisco Unified Contact Center implementation information through B+S connector

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

The information being collected, used, and disseminated, or maintained to support external customer inquiry and responses.

### 1.4 How is the information collected?

Information is collected through a combination of manual and structured system data loads of knowledge articles and user supplied data collected through secure web pages, email, chat and Cisco telephony integration.

### 1.5 How will the information be checked for accuracy?

Information will be checked for accuracy through a combination of real time data validation and inspection of operational reports by authorized government personnel.

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

Customer and employee information is protected by the following legal authorities:

- Privacy Act of 1974, as Amended (5 USC 552a);
- Computer Security Act of 1987, Public Law 100-235, ss 3 (1) and (2), codified at 15 U.S.C. 272, 278 g–3, 278 g-4 and 278 h which establishes minimum security practices for Federal computer systems;
- OMB Circular A-130, Management of Federal Information Resources, Appendix III, Security of Federal Automated Information Resources, which establishes a minimum set of controls to be included in Federal automated information security programs; assigns Federal agency responsibilities for the security of automated information; and links agency automated information security programs and agency management control systems;
- Freedom of Information Act, as Amended (5 USC 552), which provides for the disclosure of information maintained by Federal agencies to the public while allowing limited protections for privacy.
- The E-Government Act of 2002, 44 U.S.C. 3531 et seq.
- House Resolution 6124, also known as the Food, Conservation, and Energy Act of 2008 (Farm Bill).

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

RISK: Data collected is used to resolve customer inquiries related to USDA programs/services.
MITIGATION: Data is stored in a secure, but unencrypted Salesforce Government cloud environment. Salesforce Government Cloud is a partitioned instance of Salesforce's platform as a service (PaaS) and software as a service (SaaS). It is a multitenant community cloud infrastructure specifically for use by U.S. federal, state, and local government customers, U.S. government contractors, and federally funded research and development centers. See the System Security Plan (SSP) security controls Accountability, Audit and Risk Management (AR), and Data Minimization and Retention (DM). Personal case data can only be accessed authorized federal employees of the OneUSDA Contact Center with eAuth level 2 authentication.

## 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.

Customer information is used for submitting and resolving customer inquiries into the OneUSDA Contact Center and how USDA can better serve customer in the future.

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

Salesforce and Cisco data reporting tools to analyze data related to case information, generates contact statistics like call volume and abandonment rate and published knowledge articles usage and to manage the contact center.

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

No commercially or publicly available data is used.

### 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.

1 Access is controlled by User ID and password. Access rights are granted to designated individuals only when a written request is approved by their supervisor, the site system manager, and the ISSPM.

2 Users must have a Level 2 eAuth ID and are uniquely identified with a user ID. The system maintains the identity of the user and links allowable actions to specific users.

3 Privileges granted are based on job functions and area of authority like Knowledge Manage and Customer Service Representative.

4 Authority to see any privacy data within the system is restricted to those users with access approval. This is a special authority added to a logon ID. Logon ID set up, changes and termination goes through User Access Management Process.

5 Public unauthenticated users will have access to view unrestricted knowledge content using Salesforce Customer Community portal.

The National Institute of Standards and Technology (NIST) 800-53 controls for the CLSS system are discussed in detail in the System Security Plan and specifically the Access Controls (AC 1-6, 11, 12, 14, 17, 20, and 21), Identification and Authentication (IA 1-8) controls are in place to prevent unauthorized access restricting users from accessing the operating system, other applications or other system resources not needed in the performance of their duties and is restricted by eAuthentication (eAuth). The Authority and Purpose (AP 1-2) compensating controls give explanation of why PII is allowed on the system. Systems and Communication Protection (SC 1, 2, 4, 5, 7, 8, 10, 12, 13, 17, 20-23, 28, and 39) controls are in place to prevent unauthorized access.

# 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?

Information is retained at minimum of 7 years.

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

System of Record (SOR) 8484586 was completed and submitted to NARA in accordance with Section 207(e) of the E-Government Act of 2002 [44 U.S.C. 3601] and NARA Bulletins 2008-03, Scheduling Existing Electronic Records, and 2006-02, NARA Guidance for

Implementing Section 207(e) of the E-Government Act of 2002. Please refer to PO&AM 29248 in CSAM.

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

RISK: Information being retained for an indefinite or definite length can potentially be a risk. With data stored for this length of time there is the potential of unauthorized access or unauthorized disclosure as well as performance, storage considerations and costs would have to be considered.
MITIGATION: Archival of data after a certain period (7 years) can save on storage and still provide access to the data (not real-time) for reporting as well as increase the performance of the system if the data set gets too large. Additionally, purging of on a periodic basis of non-essential could also aide in keeping storage costs lower and increased performance. See the System Security Plan (SSP) security controls Accountability, Audit and Risk Management (AR), Data Quality and Integrity (DI) and Data Minimization and Retention (DM).

## 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? PTA question 11

Sharing of PII information with other USDA Mission Areas part of OneUSDA Contact Center for escalated inquiries that require mission area expertise to respond.

### 4.2 How is the information transmitted or disclosed?

Transferring of PII information is transmitted via email from the OneUSDA Contact Center to SME Contacts and through Cisco Telephony Integration

### 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.

**RISK**: The risk to internal information sharing would be the unauthorized disclosure of customer contact and inquiry information.

**MITIGATION**: The NIST 800-53 controls are discussed in the SSP. System and Communication Protection (SC) to prevent unauthorized and unintended information transfer. System and Integrity (SI) controls are in place to provide integrity and confidentiality. The security and control of PII is the responsibility of the System Owner and OneUSDA employees.

Risk is mitigated with the implementation of OneUSDA ISSS NIST policies, standards and procedures as well as Employee Security Training. Also, the data is stored in a secure environment behind the secure Salesforce Government Cloud infrastructure.

# 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

### 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

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

N/A

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

N/A

# 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.

Yes, OneUSDA Contact Center, https://contact.usda.gov, Please refer to PO&AM 29248 in CSAM

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

Provides informational notices to individuals prior to collecting customer information clearly identifying the purpose of the information collection and legal nature of the information collection. This is done in accordance with current USDA OGC guidance to support non-repudiation.

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

Yes

## 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. The information required and how it will be used is documented in agency regulations and published on the USDA Privacy Policy of the website.

## 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.

Notice is provided to customers at the time of their inquiry submission. It is during this process that the customer has the opportunity to cancel the request.

# 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?

Information will be collected on a regular basis directly from the customer. The customer has the ability up and until the point at which they submit the inquiry to OneUSDA Contact Center (webform, email, chat or phone call) to decide whether they provide their contact information or not.  After submission, customers contact the call center directly request change of their contact information. Customers' telephone number is collected when they place a call to the call center.

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

Information is available for review and change by customers up and until they submit the inquiry. Current procedures for correcting inaccurate or erroneous information are in place and would be leveraged after customer submission. These processes are currently understood and used by customers.

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

The agency regulations provide customers notification of procedures to correct information.

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

All formal and alternative processes for redress are part of existing agency regulation as part of SORN <TBD>. The agency regulations provide customers notification of procedures to correct information. Please refer to PO&AM 29248 in CSAM.

### 7.5 Privacy Impact Analysis: Please discuss the privacy risks associated with the redress available to individuals and how those risks are mitigated.

There would be no additional risk associated with the redress process available to users.

## Section 8.0 Technical Access and Security

The following questions are intended to describe technical safeguards and security measures. 33

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

OneUSDA Contact Center system is discussed in detail in the System Security Plan and specifically the Access Control (AC), Identification and Authentication (IA) and Systems and Communication Protection (SC) controls are in place to prevent unauthorized access. Access control is also addressed in the individual systems desk procedures.

Desk Procedures document the process for establishing, activating, and modifying IDs. This process is defined by System Owners. System Owners define Groups and account types. System Point of Contact (POC) assigns group membership and determines Need-to-know validation. The Program Manager is responsible for verifying user identification; the User Access Management Team (UAMT) relies on a POC supplying the correct UserID and password to UAM to identify themselves. UAM tickets are the tool used to track authorized requests by approving Point of Contact.

Digital Service Center (DSC) works with the Application's POC to add/remove users from the system. App POC will create a ticket using DSC portal and one of our admins will handle that as part of O&M. Currently the DSC reviews reports from HR on a quarterly basis. The organization employs automated mechanisms to support the management of information system accounts. Temporary and emergency accounts are not used or authorized. Guest and Anonymous accounts are not managed by ISS UAM Team. POCs (empowered by OneUSDA IT managers) are responsible for notifying UAMT if access or roles need to be modified and periodically reviewing and certifying established access.

## 8.2 Will Department contractors have access to the system?

Yes, OneUSDA Contact Center Uses Role Based Access Control. All internal OneUSDA access is managed through the USDA Enterprise Entitlement Management System (EEMS). The standard ISSPM SAAR process will be followed for requesting internal access.

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

The NIST 800-53 controls for the OneUSDA Contact Center system are discussed in detail in the System Security Plan and specifically the Awareness and Training (AT) controls are in place to provide privacy training. USDA requires annual Information Security Awareness Training (ISAT) for all employees and contractors. OneUSDA is responsible for ensuring all new employees and contractors have taken the Department Security Awareness Training developed by OCIO-CS. Training must be completed with a passing score prior to access to a OneUSDA system. All OneUSDA employees/contractors are required to complete ISAT and USDA Privacy Basics on an annual basis.

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

No

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

The NIST 800-53 controls for the OneUSDA Contact Center system are discussed in detail in the System Security Plan and specifically the Audit and Accountability (AU) controls are in place to prevent misuse of data. OneUSDA has an Application Auditing and Monitoring Policy in place that defines the following auditable events: server startup and shutdown, loading and unloading of services, installation and removal of software, system alerts and error messages, user logon and logoff attempts (both successful and unsuccessful), granting of elevated privileges (root access success and failure), modifications of privileges and access controls, all root commands (success and failure), and sensitive files accessed, modified and added. These controls, including full compliance, inheritance and risk acceptance descriptions, are available in Cyber Security Assessment and Management (CSAM).

### 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?

**RISK**: There is minimal risk given the sensitivity and scope of the information collected, as well as any information sharing conducted on the system.

**MITIGATION**: However, OneUSDA Contact Center has the following controls in place - collecting auditable events: date and time of the event, the component of the information system where the event occurred, type of event, user/subject identity, and the outcome (success or failure) of the event. Audit logs will be reviewed by the DSC quarterly and suspicious activity will be investigated. Items that will be reviewed are:

1. Login History - Review of successful and failed login attempts for all users in the Salesforce org which includes reviewing the IPs where the users logged in from and any 3rd party apps.
2. Regularly maintain active and inactive users in the system - Review of users who haven't logged in for more than 8 weeks.
3. Review of all users in the system and licenses available in the org.
4. Review all admin users in the system and revoke/restrict privileges if necessary.
5. Setup Audit Trail - Review modifications made to org's configuration.
6. Record Modification Fields - All objects include fields to store the name of the user who created the record and who last modified the record. This provides some basic auditing information.
7. Field History Tracking - Enable auditing for individual fields, which will automatically track any changes in the values of selected fields for some objects.
8. Review what apps and packages are installed and running in the org and how the installed apps and Integrations interact with the org.

Per the General Records Schedule 20 Section 1C, the following items will be deleted/ destroyed when the agency determines they are no longer needed for administrative, legal, audit, or other operational purposes: electronic files and hard copy printouts created to monitor system usage, including, but not limited to, log-in files, password files, audit trail files, system usage files, and cost-back files used to assess charges for system usage.

# 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 using the Agile framework and processes.

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

OneUSDA contact center does not raise any privacy concerns because of its employed technology.

## 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?

1. Salesforce Government Cloud Application
   a. Customer Relationship Management System and Community Portal
   b. B+S Connects for Salesforce 4.7, CTI integration between Salesforce and Cisco
   c. Survey Force for survey distribution and tracking (Appexchange managed within Salesforce)
   d. Knowledge Base Dashboards & Reports / Webform Deflection Report Packages AppExchange

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

PII data will be captured within Salesforce of the combination of Name, Address and Phone number information of contacts within the Salesforce Government Cloud Application.

### 10.4 How will the PII that becomes available through the agency's use of 3rd party websites and/or applications be used?

PII data is only available through Eauth login of authorized users into the USDA contact center Salesforce Government Cloud Environment

### 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?

PII data is maintained and secured through within the Salesforce Government Cloud Environment and been verified through the Fedramped approval of the use of the ool.

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

No purging or archiving is setup currently but expecting to keep at least for 7 years prior to archival, since this is a pilot this will would be reassess after the pilot phase to get a better idea of data storage required.

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

PII data is only available through Eauth login of authorized users into the USDA contact center Salesforce Government Cloud Environment

### 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?

PII data is only available internally through Eauth login of authorized users into the USDA contact center Salesforce Government Cloud Environment and connection to Cisco Unified Call Center.

### 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)?

Yes, SORN will be created for this system and updates for the Cisco Unified Call Center

### 10.10 Does the system use web measurement and customization technology?

No Web Measurements at this time.

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

Yes – annual concurrency review and controls testing

### 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

### 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.

N/A- Not Expecting to Share Data with 3rd Party Applications

# Responsible Officials

CEDRIC BRAGG Digitally signed by CEDRIC BRAGG
Date: 2019.06.17 14:05:04 -04'00'

Cedric Bragg
Assistant CIO

# Approval Signature

NANCY HERBERT Digitally signed by NANCY HERBERT
Date: 2019.06.17 12:52:50 -05'00'

Nancy Herbert
Information Systems Security Program Manager