Privacy Impact Assessment
CTS Remedy on Demand CS

Policy, E-Government and Fair Information Practices

- Version: 1.0
- Date: June 1, 2017
- Prepared for: USDA OCIO-CTS - Privacy Office

United States Department of Agriculture

Privacy Impact Assessment for the

CTS Remedy On Demand CS

June 1, 2017

Contact Point

David Pfaffenberger
OCIO-CTS-GSD-GAMB
(775) 450-1607

Reviewing Official

Nancy Herbert
OCIO-CTS-GSD-SCSB, ISSPM
United States Department of Agriculture
(816) 926-3836

Abstract

This Privacy Impact Assessment (PIA) addresses the BMC Remedy OnDemand (ROD) of Governance Services Division (GSD). BMC Remedy OnDemand is a SAAS cloud offering by BMC which provides a comprehensive service management suite for its customers. This PIA is being conducted based on the results of the Privacy Threshold Analysis (PTA) OCIO Client Technology Services (CTS) Governance Services Division (GSD) – Remedy OnDemand which indicated that a PIA was required.

Overview

BMC's Remedy OnDemand (ROD) is a SAAS tool implemented to centralize various functions for information technology. Some of these functions include service desk workflow, self-service ticketing, change management, problem management, knowledge management, and asset management.

ROD provides the following functionality:

- A full set of IT service management (ITSM) modules that share a native, purpose-built architecture.
- Embedded best-practice process flows.
- A closed-loop change & release process tied to incidents and problems.
- Self-Service request catalog for IT, Security, and, Business needs.
- Tracking of incident response times and service desk performance against SLAs.
- Real-time Performance and ROI metrics reporting.
- Ability to track asset CI's in a robust CMDB backend.

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?

ROD stores and leverages data in support of a robust IT Service Management (ITSM) application. The data can include people data (ie. Names, Office Site Info, Organizational info, Contact information, etc), incident requests, change requests, problem tickets, knowledge base articles, and hardware assets,

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

Information will be provided by USDA OCIO CTS administrators or USDA personnel that utilize the CTS ROD system.

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

In order to support the ITSM services provided by USDA OCIO CTS. As an example USDA OCIO CTS leverages EEMS data to provide CTS ROD with data such as Name, Phone Number, and Work Numbers to allow users to authenticate and communicate with the CTS ROD system, as well as to identify customers of the services provided by USDA OCIO CTS.

1.4 How is the information collected?

Some of the Personnel information used by CTS ROD will be provided by USDA through the USDA EEMS system. Other information is provided through our Access Control process, input by Agency SAAR POCs during the input process of the specific access requests.

1.5 How will the information be checked for accuracy?

The accuracy of the data provided to ROD by USDA will be the sole responsibility of the data owner. ROD will not have the ability to verify the information.

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.

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 by ROD will be used solely for the purposes of providing ITSM services for USDA.

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

No tools will be used to analyze the privacy data collected by the system; the data will only be used to manage the service.

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

No commercial or publicly available data will be used unless the USDA makes this same information public on their own accord. It will not be provided publicly unless authorized by the USDA.

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.

Access controls are in place to protect the information system and its components. All systems will be segmented from the public and secured or hardened following FedRamp Moderate guidance.

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 will be maintained as long as users are actively using the system. If a user leaves USDA and no longer requires access. Personnel from USDA will be required to disable and then remove the account as required.

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

Per USDA, this system does not qualify as an electronic records keeping system. Records will be maintained in accordance with guidance defined by the Client (US Government Agency that contracts for the use of the system).

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

Data is retained on users as they actively use the system, therefore the account information is required until the user no longer needs access. The active management of accounts will enable USDA to remove personnel that no longer require access and account management features provide for additional security including the ability to change passwords or re-create accounts if needed for security reasons.

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?

None. All information will stay within the accreditation boundary of the ROD system.

4.2 How is the information transmitted or disclosed?

Information will be transmitted through an encrypted connection established between USDA and ROD. Where necessary, secure data transmitted on the open internet or within the USDA secure network environment using federally approved cryptographic procedures to insure confidentiality and integrity of the data.

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.

The same moderate impact NIST 800-53, Revision 4 security controls will be used for all components that hold data within the ROD 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

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.

While OCIO-CTS has no System of Records, many of the client organizations that OCIO-CTS 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 by CTS ROD 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?

None

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

By having data transmitted to and stored at an additional facility the risk is increased, however the use of encryption decreases the potential compromise of data. This risk may be reduced further by USDA by limiting the private information that gets stored and using file level encryption for sensitive data.

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.

The exact mechanism may be slightly different for each government client. Notice is provided during the new account request process. The user must acknowledge the informed consent provisions with a signature during the new account request process.

This was presented to Angela Mauney and Theresa Pinsent in November of 2015 and it was determined that a SORN was not required for this system.

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

The exact mechanism may be slightly different for each government client. Typically the agency employee, contractor, or stakeholder does not have the opportunity to decline to provide non-PII information. The information requested is required to assign and set up the user accounts. The user has the right to correct or update information at any time be sending an email request to the agency help desk.

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

The exact mechanism may be slightly different for each government client. Generally, the requirement is for each account to be uniquely tied to an individual, all other information may be changed, updated or deleted by sending an email request to the agency help desk.

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

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.

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?

The owner of data is responsible for classifying their data based on Federal guidelines. If an owner is unknown for a data asset, the OCIO-CTS or the client organization's ISSPM becomes its caretaker. Each ISSPM is responsible for developing, implementing, and maintaining procedures for identifying all data assets and the associated owners. Personnel information will be available for their review through the use of the Remedy People form maintained by USDA. The user may view their information by going into Remedy, select the "My Profile" option. Once in their People record, the user will see their detailed information.

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

The data owner/user has the right to correct or update information at any time.

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.

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.

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.

Section 8.0 Technical Access and Security

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

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

Access to the system will be limited to administrative personnel in support of the service. The CTS ROD system 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?

All personnel that have access to the system services will be established and controlled by USDA. Contractors for CTS ROD may have access to the system for administrative purposes if a contractor is required in support of the service.

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

OCIO CTS provides security and awareness training to personnel managing the CTS ROD system for employees/contractors on an annual basis. A security training is required during the onboarding process of all users added to the ROD system. A security background check is also required for all users prior being added to the ROD system.

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

CTS ROD received a FedRamp ATO on May 5, 2016.

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

The CTS ROD 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 CTS ROD 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?

CTS ROD is an application that provide ITSM services in a secured managed hosting environment.

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

No known technology of the system would raise privacy concerns as the information collected is information from users (employees and contractors of USDA).

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?

This system does not use or interface with 3rd party websites.

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?

N/A

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

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

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

10.10 Does the system use web measurement and customization technology?

No, the system does not use any web measurement or customization technologies.

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 <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.

N/A

Responsible Officials

NANCY HERBERT Digitally signed by NANCY HERBERT
Date: 2017.06.01 09:08:12 -05'00'

Nancy Herbert

OCIO-CTS, ISSPM

United States Department of Agriculture

Approval Signature

DAVID PFAFFENBERGER Digitally signed by DAVID PFAFFENBERGER
Date: 2017.06.07 11:21:22 -07'00'

David Pfaffenberger
OCIO-CTS
United States Department of Agriculture