Privacy Impact Assessment

for

Information Technology Service Desk System (ITSDS)

Policy, E-Government and Fair Information Practices

Version: Version: 1.7

Date: February 20, 2020

Prepared for: USDA OCIO-Policy, E-Government and Fair Information Practices (PE&F)

Contact Point

Mary Boda

System Owner

USDA NRE Forest Service

614-285-8561

Reviewing Official

Cynthia Towers

Privacy Officer

USDA NRE Forest Service

(816) 844-4000

Abstract

Information Technology Service Desk System (BMC Remedy On-Demand (ROD) 9.1) is the platform for Information Technology Service Management (ITSM). ITSDS is a cloud-based solution with anytime, anywhere access to self-service service desk, change and release management, asset and service level management tools, as well as incident and problem management tools.

PIA requirement was determined by Privacy Threshold Analysis (PTA) dated December 3, 2018, to have met criteria for PIA submission. The ROD system stores the following information about USDA employees, contractors, and volunteers; Name, Business Phone Number, E-Mail Address, Home Phone Number (only if used as Business Phone Number), Job Title, eAuthentication ID, Agency Status, Organization Levels, Work Location information and incident number. The system also requires the user to use eAuthentication for access, which is integrated with USDA Enterprise Entitlements Management Service (EEMS) and Windows Active Directory Services.

Overview

The IT Service Desk is a cloud-based solution with anytime, anywhere access to self-service service desk, change and release management, asset and service level management tools, as well as incident and problem management tools.

USDA employees can contact the Service Desk 24x7x365 in a number of ways; Call, Chat, Service Request, Web Incident, Email and Fax. Information about the end user's IT problem is collected and resolved or escalated to the next Support Tier as appropriate. The data collected enables efficient resolution of the issue as well as allowance for data analysis, resulting in money saving process improvements.

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 Identification

What information is collected, used, disseminated, or maintained in the system?

Name (Includes first name and last name):

The system gets a data feed from EEMS. This includes the name of the employee and their email, phone and address where they do their business. It is the information the end users puts into the database as their business contact information.

Address Information (includes Region, Site Group and Site to include Desk Location); specifically, business e-mail address, and work location information.

Phone Number (Includes business or home phone numbers); specifically, business e-mail and business phone number. There are some cases where individuals may provide their home number as their business number in the official contact database.

Client Type (This uses several codes to identify if the customer is an employee, contractor, volunteer, affiliate, Interim or Fellow)

Job Title

Profile Status (This uses codes to identify whether the customer's record is active, suspended, on leave, future, terminated, deceased or retired)

Company, Organization and Department (Used for reporting)

eAuth Internal ID (Used for the Remedy login via Single Sign-On (SSO))

E-Mail Address (Used for sending e-mail notifications via the ITSM system)

1.2 Source

What is the source(s) of the information in the system?

Customers enter web incidents via the Service Request Management console.

Tier 1 helpdesk agents entering information given to them by the customer over the telephone.

EEMS connects to a Remedy Web Service to feed data to Remedy to create people records.

Windows Active Directory is polled quarterly to augment people records

1.3 Justification

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

This system is a Computer Help Desk (CHD) for the Forest Service. It automates the identification and tracking of incidents, proper incident escalation, expedient problem resolution, and accurate reporting that have led to continuous improvement efforts.

1.4 Collection

How is the information collected?

The ITSM system will receive a nightly feed via the EEMS system with any updated people records. EEMS connects to a Remedy Web Service to feed data to Remedy in order to create people records with information contained within the EEMS system.

Customers enter their web incidents via the Service Request Management Console.

Tier 1 helpdesk agents entering information given to them by the customer over the telephone.

Windows Active Directory is polled quarterly to augment people records

1.5 Validation

How will the information be checked for accuracy?

For web-based submission of incidents, the customer will be validated with USDA's eAuthentication Systems: An eAuthentication account consists of a User ID, a password and the customer's profile which contains information that will permit USDA applications to identify if the person has the correct permissions for access. The data within eAuthentication Systems is a collection of authoritative data received from system of record sources.

Customers will see their own incidents, and can update ticket information (but not PII) in ITSDS if it is not correct, via the web.

Tier 1 agents will verify accuracy of customer data during the process of entering the incident information into ITSDS via phone, chat, e-mail, or fax.

1.6 Authority

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

F S Policy 6640.42i – Employees

It is the responsibility of the employee to: Understand there is no expectation of privacy with government provided telecommunications equipment. Records and usage of any equipment can be requested and examined by management at any time, without prior notification of the employee.

FS Policy 6684.3 - Security Monitoring/Audit Controls

Use data collected through security monitoring only to:

a. Assist the Forest Service in achieving audit compliance.

b. Monitor service levels.

c. Support official administrative or criminal investigations.

d. Limit Forest Service liability.

Contractors, volunteers, and their agents, grantees, experts, consultants, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for FS are subject to the same Privacy Act requirements and limitations on disclosure as are applicable to FS officers and employees.

1.7 Risk Mitigation

Given the amount and type of data collected, discuss the privacy risks identified and how they were mitigated.

There is minimal risk to the user or named participants of the system. The collection of the name and working information does not pose any kind of foreseeable harm. The release of information in this system is identifying information, but not personally sensitive information. The mitigation of risk is handled by making sure that there is limited use and sharing of information, and only to relevant staff.

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 Usage

Describe all the uses of information.

Information about the end user's IT problem is collected and resolved or escalated to the next Support Tier as appropriate. The data collected enables efficient resolution of the issue as well as allowance for data analysis, resulting in money saving process improvements. PII is utilized for contacting end users.

2.2 Analysis and Production

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

Remedy Action Request (AR) reports and the analytics module within ROD are used to analyze data. The data can be exported to various formats (.xlsx, .pptx, .docx, etc.), with Microsoft Excel being the most common format.

2.3 Commercial/Public Use

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

Not Applicable

2.4 Risk Mitigation

Describe any types of controls that may be in place to ensure that information is handled in accordance with the above described uses.

Information is handled in accordance with described uses and secured through defense in depth (infrastructure), secure transmission protocol (TLS v1.2), Role-Based Access Controls (RBAC), input validation, and end user training.

Locked locations (drawers, cabinets, offices) are used for paper files.

Section 3.0 Retention

The following questions are intended to outline how long information will be retained after the initial collection.

3.1 Time Period

How long is information retained?

Official Agency Records covered by GRS 3-1, item 20 are designated as temporary records and are to be retained for 3 years after agreement, control measures, procedures, project, activity, or transaction is obsolete, completed, terminated or superseded, but longer retention is authorized if required for business use.

Official Agency Records covered by GRS 24-10 are designated as temporary record and are to be retained as follows:

Item GRS 24-10a: Destroy/delete 1 year after record is superseded or obsolete

Item GRS 24-10b: Destroy/delete when 1 year old or when no longer needed for review and analysis, whichever is later.

3.2 Approval

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

Yes, the data in the system is retained under two General Records Schedules

The Information technology and operations records are retained under GRS 3-1, item 020

General Technology Management Records - Information technology operations and maintenance records: These records relate to the activities associated with the operations and maintenance of the basic systems and services used to supply the agency and staff with access to computers and data telecommunications. Includes activities associated with IT equipment, IT systems and storage media, IT system performance testing, asset and configuration management, change management, and maintenance on network infrastructure.

The IT Customer Service Files are retained under GRS 24-10 a. and b.:

Information Technology Operations and Management Records - IT Customer Services Files

Records related to providing help desk information to customers, including pamphlets, responses to “Frequently Asked Questions,” and other documents prepared in advance to assist customers.

Help desk logs and reports and other files related to customer query and problem response; query monitoring and clearance; and customer feedback records; and related trend analysis and reporting.

3.3 Risk Mitigation

Please discuss the risks associated with the length of time data is retained and how those risks are mitigated.

There is minimal risk to the user or named participants of the system. The collection of the name and working information does not pose any kind of foreseeable harm. The release of information in this system is identifying information, but not personally sensitive information. The mitigation of risk is handled by making sure that there is limited use and sharing of information, and only to relevant staff.

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 Identification and Purpose

With which organization(s) outside of the Forest Service, but still within the Department of Agriculture is the information shared? What information is shared and for what purpose?

Not Applicable

4.2 Delivery and Disclosure

How is the information transmitted or disclosed?

Not Applicable

4.3 Risk Mitigation

Considering the extent of internal information sharing, discuss the privacy risks associated with the sharing and how they were mitigated.

Not Applicable

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 Identification and Purpose

With which external organization(s), outside of both the Forest Service and the Department of Agriculture, is the information shared? What information is shared, and for what purpose?

Not Applicable

5.2 Compatibility

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.

Not Applicable

5.3 Delivery and Security Measures

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

Not Applicable

5.4 Risk Mitigation

Given the external sharing, explain the privacy risks identified and describe how they were mitigated.

Not Applicable

Section 6.0 System of Records Notice (SORN)

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 Requirement and Identification

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

(Note: If a SORN is not required, answer “No” to this question, and “N/A” for questions 6.2 through 6.5.)

Not Applicable

6.2 Individual Notification

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

Not Applicable

6.3 Right to Decline

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

Not Applicable

6.4 Right of Consent

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

Not Applicable

6.5 Risk Mitigation

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

Not Applicable

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 Access

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

Not Applicable (PII provided by EEMS)

7.2 Correction

What are the procedures for correcting inaccurate or erroneous information?

Not Applicable (PII provided by EEMS)

7.3 Notification

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

Not Applicable (PII provided by EEMS)

7.4 Redress Alternatives

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

Not Applicable (PII provided by EEMS)

7.5 Risk Mitigation

Please discuss the privacy risks associated with the redress available to individuals and how those risks are mitigated.

Not Applicable (PII provided by EEMS)

Section 8.0 Technical Access and Security

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

8.1 Procedures

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

The system is integrated with the USDA eAuthentication Application systems. Authentication for the eAuth system is managed at the USDA enterprise level. An eAuthentication account consists of a User ID, a password and the customer's profile which contains information that will permit USDA applications to identify if the person has the correct permissions for access. Homeland Security Presidential Directive 12 (HSPD-12) mandates that federal agencies screen employees and contractors and issue credentials – or smartcards – that meet National Institute of Standards and Technology (NIST) guidelines. LincPass is the USDA smartcard. Using LincPass improves the security of the network and supported information systems in compliance with Federal Information Processing Standard (FIPS) 199.

8.2 Contractor Access

Will Department contractors have access to the system?

Yes

8.3 Privacy Training

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

All users are required to undergo computer security training (FS's Security Awareness Test) prior to accessing the Agency's system and must complete refresher training annually in order to retain access. Interaction with the system occurs only with authorized users who are U.S. Government employees or contractors with work-related and need-to-know responsibility, specific to the access and use of the system's data. Access and uses are in compliance with the law and the FS policies.

8.4 System Authority to Operate

Has Assessment & Authorization been completed for the system(s) supporting the program? If so, answer “Yes” and provide ATO expiration date(s).

Yes, Authority to Operate (ATO) was granted by the USDA CIO in June 2018.

8.5 Audit and Technical Safeguards

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

The system provides auditing and logging for unsuccessful logon attempts to applications, systems, or networks. Furthermore, it provides auditing and logging for user access to data in the database, ticket creation, and ticket updates.

Each authentication, authorization, and validation activity is logged by the eAuthentication Applications System. Successful and unsuccessful logins beyond specific thresholds are reported and reviewed on a daily basis.

8.6 Risk Mitigation

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 is mitigated through defense in depth (infrastructure), secure transmission protocol (TLS v1.2), Role-Based Access Controls (RBAC), input validation, and end user training.

Locked locations are used for paper files.

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 Description

What type of project is the program or system?

General Support System (GSS)

9.2 Privacy Concerns

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

No

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 Review

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 Purpose

What is the specific purpose of the agency’s use of 3rd party websites and/or applications?

Not Applicable

10.3 PII Availability

What Personally Identifiable Information (PII) will become available through the agency’s use of 3rd party websites and/or applications.

Not Applicable

10.4 PII Usage

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

Not Applicable

10.5 PII Maintenance and Security

How will the PII that becomes available through the agency’s use of 3rd party websites and/or applications be maintained and secured?

Not Applicable

10.6 PII Purging

Is the PII that becomes available through the agency's use of 3rd party websites and/or applications purged periodically? If so, is it done automatically? If so, is it done on a recurring basis?

Not Applicable

10.7 PII Access

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

Not Applicable

10.8 PII Sharing

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?

Not Applicable

10.9 SORN Requirement

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)?

Not Applicable

10.10 Web Measurement and Customization

Does the system use web measurement and customization technology? If so, is the system and procedures reviewed annually to demonstrate compliance to OMB M-10-23?

Not Applicable

10.11 Web Measurement and Customization Opt-In/Opt-Out

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

Not Applicable

10.12 Risk Mitigation

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.

Not Applicable

Responsible Official

OMAR THOMPSON
Digitally signed by OMAR THOMPSON
Date: 2020.04.25 23:01:44 -05'00'

Omar Thompson
System Owner (SO)
Natural Resources and Environment, Forest Service
United States Department of Agriculture

Approval Signature

CYNTHIA TOWERS
Digitally signed by CYNTHIA TOWERS
Date: 2020.04.30 14:05:46 -05'00'

Cynthia Towers
Privacy Officer (PO)
Natural Resources and Environment, Forest Service
United States Department of Agriculture

LAURA HILL
Digitally signed by LAURA HILL
Date: 2020.05.04 08:21:21 -06'00'

Laura Hill
Information System Security Program Manager (ISSPM)
Natural Resources and Environment, Forest Service
United States Department of Agriculture