Privacy Impact Assessment
for
Admin Services (AS) System

International Technology Services (ITS)

- Version: 1.0
- Date: May 2, 2011
- Prepared by: International Technology Services (ITS)

  Governance Services Division (GSD)

  Security Compliance Services Branch (SCSB)

United States Department
of Agriculture

Privacy Impact Assessment for the Admin Services (AS) System

May 2, 2011

<u>Contact Point</u>
Nancy Herbert
OCIO/GSD/SCSB
(816) 994-4207

<u>Reviewing Official</u>
Barry Lipscombe
Information System Security Program Manager
United States Department of Agriculture
(970) 295-5460

Abstract

This Privacy Impact Assessment (PIA) supports the International Technology Services Admin Services (ITS-AS) system. The ITS-AS system is used by ITS and the Service Center Agency's (SCA) Federal employees, contractors, and partners as well as SCA clients, for the ITSM component, for service desk (Help Desk) workflow and ticket tracking, user self-service, and, for the CMIS component, activity-based cost accounting. This PIA is being completed due to a Privacy Threshold Analysis (PTA) that indicated a PIA was required for the ITS-AS system to meet Federal privacy compliance requirements.

Overview

Currently, the International Technology Services (ITS) Admin Services (AS) system consists of the Remedy Information Technology Service Management (ITSM) and Cost Management Information System (CMIS) sub-systems. The sub-systems are briefly described below.

Information Technology Service Management (ITSM)

BMC's Remedy IT Service Management (ITSM) is a tool implemented to centralize various functions for information technology. Some of these functions include service desk workflow, self -service, and in later phases change management.

ITSM provides the following functionality:

- A full set of IT service management applications 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 Service Level Agreements (SLA)
- Real-time performance and Return on Investment (ROI) metrics reporting

Cost Management Information System (CMIS)

The Cost Management Information System (CMIS) is a commercial-off-the-shelf (COTS) activity-based cost management system that allows users to import data from other applications and either view reports on the intranet or use a spreadsheet (if required). The overall function of CMIS is to take general ledger data (the Account and Department costs), together with any other relevant costing information, and apportion costs to specific activities performed within the International Technology Services (ITS). Activities are grouped according to the processes performed by the ITS. Any activities contributing to or that support other activities within ITS can have their costs reallocated, effectively allowing the full costing of all direct activities that impact the cost objectives.

The purpose of CMIS is to report costs related to activities so that this information can be analyzed. CMIS allows the performance of a number of analytical tasks such as internal benchmarking, process analysis, and resource utilization analysis. These analysis tasks are crucial to effective activity-based cost management. These analytical tasks play a vital role in determining the costs of products and in making resource purchase recommendations in the future. In addition, CMIS collects relevant data from other systems to aid the forecasting of costs.

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?

The information that is collected, used, disseminated, or maintained in the ITS Admin Services (AS) system is used for user identification, authorization, and authentication purposes and can include the user's name, organizational unit information, office telephone number, electronic mail address, and physical office address to adequately identify the individual for Help Desk support purposes.

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

The source of the information used is the System Access Authorization Request (SAAR) process, telephone calls to the ITSM Remedy Help Desk, and the eAuthentication system.

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

The information is collected and used to provide ITS and SCA Federal employees, contractors, Service Center Agency (SCA) clients, and other authorized ITS-AS system user's credentials for the authorized use of the system.

1.4 How is the information collected?

Information collected for use in the system is derived from the System Access Authorization Request (SAAR) process, telephone calls to the Help Desk, and the eAuthentication system.

1.5 How will the information be checked for accuracy?

The authorized Federal or contractor personnel that input the data from the SAAR documentation are responsible for checking the information for accuracy when they develop a new user account. Further, Remedy does check the information that is input to ensure that it is in the proper format for use within the component. The information that is input from the SAAR form, collected on the phone call, and the eAuthentication system is supplied by the person requesting that a user account be added to or that a user account is changed/updated and is assumed to be the authoritative source of that information.

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

Both Office of Management and Budget (OMB) Circular A-130, Appendix II and the Federal Information Security Management Act of 2002 (FISMA) (Title III, Pub. L. No. 107-347) require that all users of a system be uniquely identified to be able to use a Federal information system. Remedy, a critical component of the ITS-AS system, implements this requirement by using the individual's name as part of the unique identification process.

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

No other personal information besides the individual's name, email address, and telephone number is used within the AS system and not shared with other systems and applications. Risks associated with data collection in the AS are minimal and include the possibility of the data being accessed by unauthorized personnel. Furthermore, additional risks to the system data are mitigated through the use of regular system scans, testing, and reviews.

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.

The information that is collected, used, disseminated, or maintained in the ITS EUC system is utilized by the Remedy component for user identification, contact, authorization, and authentication purposes.

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

Custom scripts are used to gather account information. This information is processed and formatted to produce access control reports. These reports are produced on a monthly, quarterly, and annual basis for review and approval by the responsible parties.

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

The ITS-AS system does not use commercial or publicly available data.

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.

The ITS-AS does not share the person's name with other systems or applications. Only the information on a specific user's authorization to use a given system or application is shared to ensure that the system or application is only accessed by authorized users. Because of this control of shared information, the risk to an individual's privacy is considered to be very low.

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?

Contact, authorization, and authentication information is only maintained for the duration of time that an individual is a Federal employee, contractor, or other partner requiring access to the ITS-AS system and for the National Archives and Records Administration (NARA) required retention period for computer operational records.

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

No, records retention requirements for this system have not specifically been approved by NARA.

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 associated with data retention for the ITS-AS system are minimal and include the possibility of the data being accessed by unauthorized personnel. Additionally, risks associated with the length of time the data is retained are mitigated through the use of regular system scans, testing, and reviews.

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?

The information gathered for the creation of accounts within the ITS-AS system is shared with the user’s agency security office where it is distributed for review and approval by the appropriate parties.

4.2 How is the information transmitted or disclosed?

Reports on account information are posted to an SSL encrypted Sharepoint site. Access to the site is restricted to appropriate parties.

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.

Risks associated with data sharing outside the ITS-AS system are minimal and include the possibility of the data being accessed by unauthorized personnel. Risks associated with data sharing are mitigated through the use of regular system scans, testing, and reviews.

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?

Contact, authorization, and authentication information is not shared outside the USDA.

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.

Contact, authorization, and authentication information is not shared outside the USDA.

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

Contact, authorization, and authentication information is not shared outside the USDA.

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

Contact, authorization, and authentication information is not shared outside the USDA; therefore the risk to an individual's privacy is minimal. However, all risks to the system data are mitigated through the use of regular system scans, testing, and reviews.

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

Yes, all users are made aware during the SAAR process and telephone calls to the Help Desk that their name will be used as part of the user identification for their access to the ITS-AS, its components, and other applications and systems.

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

No, the individual's name is required for their inclusion as an authorized user within the ITS-AS so that they may perform the tasks of their assigned job or for services which they are requesting. Only authorized Federal employees, contractors, Service Center Agency (SCA) clients, and other partners that require access to the ITS-AS are asked for this information.

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

The contact within the ITS-AS is to determine whether an individual is an authorized user or SCA client of the ITS-AS and associated applications and systems.

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

To mitigate risks associated with individuals being unaware of the data collection, all users are made aware during the SAAR process or telephone call that their name and contact information will be used as part of the user identification for their access and use of the ITS-AS, its components, and other applications and systems. Additional risks to the system data are mitigated through the use of regular system scans, testing, and reviews.

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?

Once the information for an individual is input into the ITS-AS using the SAAR form or from the telephone call to the Help Desk it is not changed. Individuals do not have access to the information except to make updates to the contact information. Other than the authentication credentials (i.e., password), which are changed on a regular basis, only a system administrator can delete the information for an individual.

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

A SAAR form or telephone call must be initiated to change the information contained in the ITS-AS.

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

During initial training for the system, users are instructed to contact their Information System Security Point of Contact (ISSPOC) to utilize the SAAR process to make any updates to their account information. If an individual subsequently needs to update their account information, they contact their ISSPOC to input a SAAR in the Remedy tool detailing what needs to be updated. As updates are made, the information on account maintenance is delivered via email or web site to the user's agency Information Security Support Staff (ISSS) office. This information is then forwarded via email through the management chain to the user.

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

Formal redress is provided through the SAAR process.

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

All users are made aware during the SAAR process or during the telephone call that their name will be used as part of the user identification for their access to the ITS-AS system, its components, and other applications and systems. Additionally, system information is not shared outside the USDA; therefore the risk to an individual's privacy is minimal. However, additional risks to the system data are mitigated through the use of regular system scans, testing, and reviews.

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?

All users of the ITS-AS must be Federal ITS or SCA employees, contractors, or authorized partners of the USDA and must complete a background investigation and the SAAR process prior to being given access to the system. The process for determining which users may access the system is documented in the hiring and SAAR process documents.

8.2 Will Department contractors have access to the system?

Yes, and they must have a current contract with ITS or the SCAs to have and maintain that access.

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

All ITS and SCA Federal, contractor, and authorized partner users receive initial security and privacy training prior to being given access to the ITS-AS system and annually thereafter as long as they work for ITS or the SCAs.

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

Yes and the security authorization process (formerly known as Certification and Accreditation) was completed and an Authorization to Operate (ATO) was given in August 2010.

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

The ITS-AS has an extensive list of audit parameters that are monitored on a regular basis including auditing of user account changes.

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?

Microsoft AD and eAuthentication system information is not shared outside the USDA; therefore the risk to an individual’s privacy is minimal. Additionally, system security controls have been designed to limit sharing of data and to identify privacy risks on the system. Furthermore, risks to the system data are mitigated through the use of regular system scans, testing, and reviews.

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?

The ITS-AS system is used by ITS and the Service Center Agency’s (SCA) Federal employees, contractors, and partners for ongoing Help Desk and cost accounting needs in support of the ITS and SCA’s mission areas and includes hardware, software, connectivity, and miscellaneous networked devices.

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

This application does not employ technology which may raise privacy concerns.

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, the system owner and the ISSPM have reviewed the referenced OMB memoranda.

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

Not applicable, the ITS-AS does not use 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.

Not applicable, since the ITS-AS does not use third party websites or applications, no PII will become available through that use.

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

Not applicable, the ITS-AS does not use third party websites or applications.

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?

Not applicable, the ITS-AS does not use third party websites or applications.

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

Not applicable, the ITS-AS does not use third party websites or applications.

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

Not applicable, the ITS-AS does not use third party websites or applications.

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?

Not applicable, the ITS-AS does not use third party websites or applications.

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)?

Not applicable, the ITS-AS does not use third party websites or applications.

10.10 Does the system use web measurement and customization technology?

Not applicable, the ITS-AS does not use third party websites or applications.

10.11 Does the system allow users to either decline to opt-in or decide to opt-out of of all uses of web measurement and customization technology?

Not applicable, the ITS-AS does not use third party websites or applications.

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.

Microsoft AD and eAuthentication information is not shared outside the USDA; therefore the risk to an individual's privacy is minimal. Additionally, potential risks to the system data are mitigated through the use of regular system scans, testing, and reviews.

Privacy Impact Assessment Authorization Memorandum

The below signatures indicate that this Privacy Impact Assessment for the **ITS Admin Services (ITS-AS) System** has been carefully reviewed for completeness and accuracy and has been completed in accordance with the requirements of the EGovernment Act of 2002 and the Privacy Act of 1974.

Phillip Rendina, System Owner	Date
David Shearer, ITS Associate CIO	Date
Barry Lipscombe, ITS ISSPM	Date