Privacy Impact Assessment
for the

Accessibility Compliance Management System (ACMS)

June 22, 2010

Contact Point
Allen Hoffman
Office of Accessible Systems & Technology (OAST)
DHS OCIO
(202) 447-0303

Reviewing Official
Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security
(703) 235-0780

Abstract

The Department of Homeland Security (DHS) Office of Accessible Systems & Technology (OAST) operates the Accessibility Compliance Management System (ACMS). ACMS is intended to bring together a web-based, DHS-wide single point-of-entry reporting system. ACMS will allow documenting and reporting of all Section 508 compliance and accessibility activities and consistently track current status and progress towards meeting Section 508 compliance requirements for OAST and Component Accessible Systems and Technology Programs (ASTP). The PIA is being conducted to determine any privacy issues with customer information.

Overview

The DHS Office of Accessible Systems & Technology (OAST) provides DHS leadership, vision, and direction for ensuring that electronic and information technology (EIT) procured, developed, maintained, or used by DHS is accessible to employees and customers with disabilities as mandated by Section 508 of the Rehabilitation Act Amendments of 1998 which requires federal agencies to make all electronic and information technology accessible to individuals and members of the public with disabilities.

To meet this responsibility, the DHS OAST provides governance and oversight of Component Accessible Systems and Technology Programs (ASTP), as well as similar activities throughout the life cycles of EIT projects across the department, such as Enterprise Architecture Reviews, Change Control Boards, and Acquisition Reviews. Component ASTPs rely upon Section 508 Coordinators to ensure Section 508 compliance is achieved in the various projects underway in that environment. ACMS provides a centralized system to bring all the various pieces of information together to allow Component ASTPs and OAST to manage and track the status of requests and progress towards meeting Section 508 compliance requirements.

ACMS users are analysts with role-based permission accounts, restricted in accessing only requests assigned individually to them. ACMS analysts are not notified of an assigned request and must regularly log in to see the requests assigned to them on the ticket management screen.

The Component administrative account creates Component analyst accounts, views all requests assigned to all their Component's analysts, to enable system administration or reassignment of requests to different analysts within each respective Component. The Component administrative account cannot see the personally identifiable information in a ticket unless that ticket is first assigned to them. If they assign a ticket to themselves, they will have access to the same basic information as any other ACMS analyst as described in Section 1.0. Security is role-based and Components cannot view other Component's information.

OAST system administration account resides with OAST and is the only account that can view all OAST (HQ) and all Component tickets. This allows OAST to create Component user and administrative accounts, and administratively manage OAST analysts.

An individual must submit an initial request to his or her Component's Section 508 Coordinator (hereinafter "the Coordinator") for access to ACMS. Once the initial request is approved the individual is required to complete ACMS training. The Coordinator will create a user account with the specific permission levels described below for individuals who have completed training prior to granting the actual permission to access ACMS:

1. OAST Admin: OAST Admin have the ability to access all ACMS tools, inventory database, accommodation database, global contacts list, ad hoc reporting tool, create user accounts and view all tickets from any user in the system. Additionally the OAST Administrator is the only person that can grant access to the Accommodations database and related tools and reports.

2. OAST Analyst: OAST Analyst can view only tickets they are assigned to; however, they are able to assign tickets to other analyst in different components. Additionally, OAST analysts have the ability to access the Inventory database and Global Contacts list.

3. Component Coordinator: The Component Coordinator can view all tickets that are related to his or her component and that were created by someone in his or her group. The Component Administrator is unable to view tickets created by OAST analyst, unless he or she is assigned to the ticket. The Component Coordinator also has the ability to access most of the ACMS tools, add-hoc reporting tool and can create user accounts. The Component Coordinator is not allowed to grant permission to the accommodations database or any tool or reports related to the accommodations database, when creating a user account.

4. Component Analyst: Component Analysts are only able to view tickets that are assigned to them and they have the ability to create reports using the Preformatted Reports tool.

After a User Account is established, the individual will be notified that they can access ACMS via Single SignOn. No individual can access ACMS without a User Account.

Individuals with access to ACMS have the ability to create reports and create, modify, reassign, search, and close a ticket. Tickets are related to the following categories and corresponding descriptions:

- Document and Accommodations Request – requestors provide contact information for a specific accommodation or document. ACMS does not collect the details of the accommodation request.
- Acquisition Request – contract documentation is provided to determine if Section 508 compliance language is sufficient.
- Application Reviews – a request the review of specific software to test and evaluate to determine is compliant with Section 508
- Enterprise Architecture (EA) Reviews – tracks EA reviews and comment submissions
- Outreach Activities – tracks events and tasks necessary to attend conferences
- Component Accomplishments – summary of important events to identify accomplishments for progress reporting to management

- Internal Projects – tracks progress of EA reviews projects until complete
- Technical Assistance – tracks status and completion of the installation of software
- Training Request – tracks trainings and attendee contact information
- Complaints – tracks complaints regarding the accessibility of a web page application from initial submission to the resolution
- Inventory - tracks the software licensed and used for accessibility compliance including the location of the installation
- Customer Feedback – internal mechanism to review customer feedback to improve services
- Reporting - generates reports on the average time per ticket, number of open tickets, and number of customers served for a given time period

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 ACMS collects basic contact information from individuals who submit requests or attend trainings as identified above. This information includes:

- Full Name
- Component, if applicable
- E-mail address
- Phone number
- Business address
- Name of training
- Date of training

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

ACMS information is provided and directly entered by Component Section 508 Coordinators, members of OAST, and personnel supporting those efforts in those locations. No external data is collected from any other sources. The ACMS utilizes single sign-on to ensure security requirements are met and that user data for contact fields is automatically verified.

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

ACMS collects this information to manage and report on all aspects of program management, accessibility compliance, technical assistance, and reasonable accommodations for the OAST, and associated Component Accessible Systems and Technology Programs point of contact information is required. The ACMS tracks and activities required to answer the individual Section 508 related inquiries or individual requests for reasonable accommodation. Without this information, OAST could not reliably respond to individual needs or ensure tracking of licenses for software required in support of accessibility.

In addition, ACMS creates the following reports: Application Reviews, Acquisition Reviews, Reasonable Accommodations, EA Reviews, Help Desk Requests, Training Requests, Asset Management, Accomplishments, Complaints, Outreach Activities and Customer Satisfaction Reviews. In all instances there is a point of contact for each request or indication who requested the review, using the contact information above.

1.4 How is the information collected?

Information is collected directly from the individual submitting a request for service or training via web, phone, or email.

1.5 How will the information be checked for accuracy?

The information is reviewed by the submitter before submission. Confirmation of receipt of the request is sent to the submitter via email as part of the request procedure.

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

DHS is authorized to collect information under the following:

- MD 0007.1- Information Technology Integration and Management ;
- MD Number 4010.2- Section 508 Program Management Office & Electronic and Information Technology Accessibility, which includes references to numerous public laws, regulations and DHS directives:
    - The Homeland Security Act of 2002, P.L. 107-296 (November 25, 2002), Section 102;
    - Section 508 of the Rehabilitation Act of 1973, as amended in the Workforce Reinvestment Act of 1998 (PL 105-220, 1998);
    - 36 CFR Part 1194, "Electronic and Information Technology (EIT) Accessibility Standards;"
    - 48 CFR 39.204, Federal Acquisition Regulations (FAR) –"Acquisition of Information Technology;"

- OMB Circular A-130, Management of Federal Information Resources (61 FR 6428, February 20, 1996);
- 40 U.S.C. 11101 (6), Clinger-Cohen Act of 1996;
- Section 202(d) of the E-Government Act of 2002, "Accessibility to Persons with Disabilities;"
- DHS Management Directive 3500; Operational Roles and Responsibilities of the Officer for Civil Rights and Civil Liberties and the Office of Chief Counsel;
- 6 CFR 15, DHS Section 504 regulation, "Enforcement of Nondiscrimination on the Basis of Disability in Programs or Activities Conducted by the Department of Homeland Security;" and
- DHS Management Directive 0760; Government Purchase Card Program.

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

Privacy Risk: The main privacy concern is identification of customers via their contact information.

Mitigation: OAST requires individual accommodations information to remain private and only allow access by authorized personnel. This is accomplished through establishing initial system requirements that support the common enterprise authentication platform implemented at DHS including Single Sign-On, AES 256 encryption for data storage, and the ability to allow or restrict access to system functions, features, data, and documents based upon user role and identity. We only collect the required information necessary to service the individual request and provide contact back to the requestor. Additionally, contact information for component tickets is restricted to only that component, except when DHS OAST must also participate in resolving a ticket.

The system must meet applicable DHS Security requirements from MD 4300.

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 ACMS analyst uses the requestor information to maintain contact as-needed with the requestor, typically via email or via phone, to provide updates, clarify information, request additional information, and notify the requestor of changes until requests are complete.

Also, ACMS generates reports intended to show volume, work progress, and status. These reports do not contain any PII, but indicate information such as the date a ticket was assigned, who it was assigned to, how long the ticket has been open, and the ticket status (Open, pending, closed).

These reports are used by management to determine progress and analyze performance. Progress details are recorded in each individual ticket as notes, and not provided in reports. ACMS Analysts have to maintain their own notes to be able to provide rationale and progress to management as requested.

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

Reporting is simple, providing only a running total of individual ticketing information. It does not report using personally identifiable information, but allows searching of tickets by the assigned person responsible for solving and closing a ticket (the individual administratively responsible for the ticket's solution).

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

AMCS does not use commercially 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.

Privacy Risk: There is a possible risk of misusing of information.

Mitigation: To mitigate this risk, users of ACMS are notified by the system that all information is used for official purposes. ACMS Administrators ensure information and requests from end-users submitting requests are for official duties as an employee or contractor within DHS, and are not of a personal nature. In addition, only authorized users with accounts are allowed access to the system. Component-to-component POC sharing is not allowed, and reporting based on POC is not intended or implemented.

Section 3.0 Retention

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

3.1 What information is retained?

ACMS retain all information previously listed in Section 1.1.

3.2 How long is information retained?

ACMS information is retained for one year or when information is no longer needed for review and analysis, whichever is later.

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

Yes, the retention schedule has been approved by NARA.

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

Privacy Risk: There is a possibility of retaining more information than necessary.

Mitigation: The information merely indicates the person contacted the DHS Accessibility Help Desk and that their request was completed. This information likely poses no significant risk, therefore but no formal plan or evaluation process has been created at this time.

Section 4.0 Internal Sharing and Disclosure

The following questions are intended to define the scope of sharing within the Department of Homeland Security.

4.1 With which internal organization(s) is the information shared, what information is shared and for what purpose?

AMCS shares information with OAST and the following DHS Component Section 508 Program Offices: Customs & Border Protection (CBP), Citizenship & Immigration Services (CIS), Domestic Nuclear Detection Office (DNDO), Federal Emergency Management Agency (FEMA), FEMA Emergency Management Institute (EMI), FEMA U.S. Fire Administration (USFA), Intelligence & Analysis (IA), Federal Law Enforcement Training Center (FLETC), Immigration & Customs Enforcement (ICE), National Protection & Programs Directorate (NPPD), Office of the Inspector General (OIG), Science & Technology (S&T), Transportation Security Administration (TSA), U.S. Coast Guard (USCG), U.S. Secret Service (USSS), U.S. Visitor & Immigration Status Indicator Technology (USVISIT).

OAST will have access to all information, but Component ACMS analysts will only have access to their respective Component's information. Component analysts will not have access to or use of the inventory management module. Component access to the accommodations functionality is restricted to component staff designated as Disability Program Managers (DPM). This includes the tracking of IT

products and programs purchased, licensed, or controlled by OAST. Examples include a screen reader program license assigned to a user.

4.2 How is the information transmitted or disclosed?

Information is retained in a centralized system and accessed by authorized personnel only via web browser.

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.

Privacy Risk: There is a risk of sharing information to individuals without a valid need to know.

Mitigation: Centralization of the data using a web application has mitigated most of the risks associated with the inadvertent release of information. Role-based access will enforce Component access to Component data only, while also allowing DHS OAST access to such data as needed.

Section 5.0 External Sharing and Disclosure

The following questions are intended to define the content, scope, and authority for information sharing external to DHS 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?

ACMS does not share information with external organizations.

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 DHS.

ACMS does not share information with external organizations.

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

ACMS does not share information with external organizations.

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

ACMS does not share information with external organizations.

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. Notice is provided to the individual via this PIA and the General Information Technology Access Account Records System (GITAARS) SORN, DHS/ALL-004, May 15, 2008, 73 FR 28139.

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

Yes. Individuals can choose not to use the system and escalate this request to their immediate manager. Since they would have to sign into the system for any guidance to be provided, there is no opportunity to train the user to not use the system.

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

Yes. ACMS collects information solely for the purpose of providing service based on the request of individuals. ACMS will not be able to respond to the request if an individual does not provide contact information.

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.

Privacy Risk: There is a possibility of individuals not being aware of the collection of information.

Mitigation: Notice of the collection of information is provided via this PIA and the GITAARS SORN mitigating this 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?

Where personal information is collected, information is from the users themselves. Users do not review their information but after it had been submitted can track any request via a tracking ticket number. An email is sent to the user upon submission of a ticket either from the Web or over the phone and contains the initial information collected.

In addition, individuals may gain access to their own information by submitting a Privacy Act (PA)/Freedom of Information Act (FOIA) request. Individuals may also contact the DHS Privacy Office with ACMS PA/FOIA requests at the following: The Privacy Office U.S. Department of Homeland Security, 245 Murray Drive SW, Building 410, STOP-0550, Washington, DC 20528-0550.

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

Individuals may gain access to their own information by submitting a Privacy Act (PA)/Freedom of Information Act (FOIA) request. Individuals may also contact the DHS Privacy Office with ACMS PA/FOIA requests at the following: The Privacy Office U.S. Department of Homeland Security, 245 Murray Drive SW, Building 410, STOP-0550, Washington, DC 20528-0550.

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

Individuals may gain access to their own information by submitting a Privacy Act (PA)/Freedom of Information Act (FOIA) request. Individuals may also contact the DHS Privacy Office with ACMS PA/FOIA requests at the following: The Privacy Office U.S. Department of Homeland Security, 245 Murray Drive SW, Building 410, STOP-0550, Washington, DC 20528-0550.

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

None required. Users can open a new request with new contact information.

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

Privacy Risk: An individual may not be aware of the process for accessing and/or correcting information.

Mitigation: To mitigate this risk, individuals are able to review all information included on a ticket request. In addition, individuals can submit a FOIA request through the process described above.

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?

Request for access is controlled and approved by OAST and component Section 508 Coordinators. Only personnel with secret clearance and completed suitability approval for their component shall be granted access to ACMS.

8.2 Will Department contractors have access to the system?

Yes.

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

All individuals with access to ACMS are required to take the standard DHS or component privacy training.

Note, the Component administrators and Component analysts must complete ACMS training to gain access following this policy/procedure:

Before being granted access to the ACMS, DHS employees or contractors must:

- Hold an active secret security clearance,
- Hold an active DHS background suitability clearance,
- Have an active DHS A-LAN Network account,
- Provide a signed, completed certification of completion of role-based training on the operation of the ACMS system,

- Have DHS responsibilities for the management, tracking, or fulfillment of accessibility or accommodations related services

The ACMS is operated by the OAST. User access to the ACMS is assigned to members of OAST and Component Section 508 Coordinators by the OAST ACMS systems administrator. Section 508 Coordinators may assign ACMS access to their personnel as needed, provided they meet the access requirements listed above. OAST will maintain a list of people who have completed the ACMS training.

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

Yes, the ATO will expire on June 22, 2013.

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

User authentication and authorization integrated with DHS single sign-on using recommended AppAuth, means only users authorized for A-LAN accounts can gain access. This allows standard network login controls for user access and removal from access to the system, including password reset. Access to data is only provided to authenticated individuals.

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?

A privacy risk exists of exposure of contact information for an individual who has a ticket in the ACMS, however this risk is mitigated since all such information is controlled by role-based access and use to ensure that only authorized ACMS users see such information in the course of conducting activities which directly relate to that information. Reporting capacities of ACMS do not directly provide access to aggregated contact information.

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, RFID, biometrics and other technology.

9.1 What type of project is the program or system?

This is an operational system.

9.2 What stage of development is the system in and what project development lifecycle was used?

System is in the Integration & Test stage, following the life-cycle requirements of the DHS SELC.

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

None. The system is following the requirements using technologies approved for use by the DHS Enterprise Architecture.

Responsible Officials

Bill Peterson

Director, Office of Accessible System & Technology

Department of Homeland Security

Approval Signature

Original signed copy on file with the DHS Privacy Office

Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security