

Appendix B – WebCAAF (E-Authentication) Privacy Impact Assessment

Introduction

This document reports the results of a Privacy Impact Assessment conducted on the Electronic Access Initiative (EAI) Web-based Centralized Authentication and Authorization Facility (WebCAAF) on 10 March 2003. The assessment was conducted by the EAI WebCAAF Operations Team according to the guidelines set forth in *Cyber Security Guidance on Privacy Impact Assessments (I*CAMSs)*, and presents the information requested in Attachment 2, USDA Privacy Impact Assessment Form.

Assessment Results

Project Name: Web-based Centralized Authentication and Authorization Facility (WebCAAF)

Description of Your Program/Project:

The WebCAAF provides single sign-on to both internal and validated external users for access to various hosted applications. This capability allows access to protected information after proper identification, authentication and authorization of the user, using the Netegrity SiteMinder® product. Authorized information across multiple Web farms is made available to an authenticated user based on the initial validation of proper credentials. This prevents the user from being required to enter multiple credentials while accessing multiple web-based applications across the USDA.

DATA IN THE SYSTEM

<p>1. Generally describe the information to be used in the system in each of the following categories: Customer, Employee, and Other.</p>	<p>Customer: Name, SSN, SCIMS ID, Password</p> <p>Employee: Name, Status, Password, Office ID, Work E-Mail, and Work Phone</p> <p>Other - Affiliates (Contractors/Partners): Name, Password</p>
<p>2a. What are the sources of the information in the system?</p>	<p>SCIMS, OIP, CAMS, CCE Active Directory</p>
<p>2b. What USDA files and databases are used? What is the source agency?</p>	<p>SCIMS (SCA), OIP (NRCS), CAMS (SCA), CCE Active Directory (SCA)</p> <p>SCA- Service Center Agencies</p>
<p>2c. What Federal Agencies are providing data for use in the system?</p>	<p>USDA- NRCS; RD; FSA</p>
<p>2d. What State and Local Agencies are providing data for use in the system?</p>	<p>None</p>

2e. From what other third party sources will data be collected?	Customer information collected at county level directly from the customers.
2f. What information will be collected from the customer/employee?	Customers provide name and SCIMS ID. Other relevant customer information is pulled from the SCIMS database directly.
3a. How will data collected from sources other than the USDA records and the customer be verified for accuracy?	None
3b. How will data be checked for completeness?	Web Registration process (WebReg).

ACCESS TO THE DATA

1. Who will have access to the data in the system (Users, Managers, System Administrators, Developers, Other)?	System Administrators have access to data fields.
2. How is access to the data by a user determined? Are criteria, procedures, controls, and responsibilities regarding access documented?	Users do not access the data. Data is used to make authentication and authorization decisions regarding the users.
3. Will users have access to all data on the system or will the user's access be restricted? Explain.	Users do not access the data.
4. What controls are in place to prevent the misuse (e.g. browsing, unauthorized use) of data by those having access?	Access is limited to system administrators on a least privilege basis.
5a. Do other systems share data or have access to data in this system? If yes, explain.	Upon authorization, data elements can be passed from the WebCAAF Active Directory to an application.
5b. Who will be responsible for protecting the privacy rights of the customers and employees affected by the interface.	WebCAAF assumes responsibility of passing data to applications upon initial authorization. Application owners are then responsible for securing information within their application.
6a. Will other agencies share data or have access to data in this system (International, Federal, State, Local, Other)?	WebCAAF is a Service Center Agency sponsored system. FSA, RD, and NRCS are all users of WebCAAF.
6b. How will the data be used by the agency?	To make authentication and authorization decisions.
6c. Who is responsible for assuring proper use of the data?	WebCAAF system owner

ATTRIBUTES OF THE DATA

<p>1. Is the use of the data both relevant and necessary to the purpose for which the system is being designed?</p>	<p>Yes, the system was designed as a security front-end to provide authentication and authorization to web-based applications. The data stored within WebCAAF is used exclusively to determine application access.</p>
<p>2a. Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected?</p>	<p>WebCAAF relies upon outside sources of information. The system itself does not collect or derive data.</p>
<p>2b. Will the new data be placed in the individual's record (customer or employee)?</p>	<p>Not Applicable</p>
<p>2c. Can the system make determinations about customers or employees that would not be possible without the new data?</p>	<p>Not Applicable</p>
<p>2d. How will the new data be verified for relevance and accuracy?</p>	<p>Not Applicable</p>
<p>3a. If data is being consolidated, what controls are in place to protect the data from unauthorized access or use?</p>	<p>Data is consolidated from a variety of sources. Controls in place over that data include: Intrusion Detection Sensors, Limited Physical Access, Limited number of System Administrators, Least Privilege Access Control for Sys Admins.</p>
<p>3b. If processes are being consolidated, are the proper controls remaining in place to protect the data and prevent unauthorized access? Explain.</p>	<p>Processes are not consolidated.</p>
<p>4a. How will the data be retrieved? Can it be retrieved by personal identifier? If yes, explain.</p>	<p>Data is retrieved to make authentication and authorization decisions by SiteMinder once a user (employee or customer) enters their ID/Password.</p>
<p>4b. What are the potential effects on the due process rights of customers and employees of:</p> <ul style="list-style-type: none"> • consolidation and linkage of files and systems; • derivation of data • accelerated information processing and decision making; <p>use of new technologies.</p>	<p>Not Applicable</p>
<p>4c. How are the effects to be mitigated?</p>	<p>Not Applicable</p>

MAINTENANCE OF ADMINISTRATIVE CONTROLS

<p>1a. Explain how the system and its use will ensure equitable treatment of customers and employees.</p>	<p>WebCAAF centralizes the authentication and authorization process for web-based applications. Access control is centrally managed ensuring equitable treatment for all employees and customers using web-based applications protected by WebCAAF.</p>
<p>2a. If the system is operated in more than one site, how will consistent use of the system and data be maintained in all sites?</p>	<p>WebCAAF is operated in three sites (Fort Collins, CO; Kansas City, MO; St. Louis, MO). The system including the data repositories are replicated between the cities to ensure consistency.</p>
<p>2b. Explain any possibility of disparate treatment of individuals or groups.</p>	<p>Password expiration settings for employees and customers differ. Employee expiration settings are consistent with USDA-OCIO's requirements. Customer password expirations are consistent with current public standards.</p>
<p>2c. What are the retention periods of data in this system?</p>	<p>Data is not retained within WebCAAF, it is constantly refreshed from its data sources.</p>
<p>2d. What are the procedures for eliminating the data at the end of the retention period? Where are the procedures documented?</p>	<p>Not Applicable</p>
<p>2e. While the data is retained in the system, what are the requirements for determining if the data is still sufficiently accurate, relevant, timely, and complete to ensure fairness in making determinations?</p>	<p>Data is refreshed from its sources periodically throughout the day. The source applications are responsible for maintaining current and complete data.</p>
<p>3a. Is the system using technologies in ways that the USDA has not previously employed (e.g. Caller-ID)?</p>	<p>Not Applicable</p>
<p>3b. How does the use of this technology affect customer/employee privacy?</p>	<p>Not Applicable</p>
<p>4a. Will this system provide the capability to identify, locate, and monitor <u>individuals</u>? If yes, explain.</p>	<p>No</p>
<p>4b. Will this system provide the capability to identify, locate, and monitor <u>groups of people</u>? If yes, explain.</p>	<p>No</p>
<p>4c. What controls will be used to prevent unauthorized monitoring?</p>	<p>WebCAAF does not provide monitoring capabilities above and beyond normal audit logging requirements.</p>

5a. Under which Systems of Record notice (SOR) does the system operate? Provide number and name.	Not Applicable
5b. If the system is being modified, will the SOR require amendment or revision? Explain.	No

--