Privacy Impact Assessment
Forest Service Computer Base Legacy

Cyber and Privacy Policy and Oversight

- Version: 2.0
- Date: July 19, 2010
- Prepared for: USDA OCIO CPPO

United States Department of Agriculture

Privacy Impact Assessment for the

Forest Service Computer Base Legacy

July 19, 2010

Contact Point
Doreatha Smith
USDA Forest Service
414-297-1385

Reviewing Official
Robert Chadderdon
Internal Controls Manager
USDA Forest Service
(505) 842-3387

Abstract

USDA Forest Service Computer Base Legacy (FSCB Legacy) General Support System (GSS) system provides resources for daily operations of the Washington Office, Regional Offices, Research stations, International Institute of tropical Forestry (IITF), Forests, and Districts. The Privacy Impact Assessment (PIA) is intended to assist USDA FS employees in identifying information privacy when planning, developing, implementing, and operating agency owned applications. The PIA will help USDA FS employees consider and evaluate whether existing statutory requirements are being applied to systems that contain personal information.

Overview

Name of Project: USDA Forest Service (FS) Computer Base (FSCB Legacy)
Program Office: USDA Forest Service
Project's Unique ID: FSCB Legacy
System Owner: Jane Evans
Title: Knowledge Management/Collaboration Tools Program Manager/System Owner
Agency: USDA, Forest Service
Address: Forest Products Laboratory, One Gifford Pinchot Drive, Madison, WI 53726-2398
E-mail: jkevans@fs.fed.us

The FSCB Legacy GSS provides the resources necessary for the Forest Service to manage the Information Technology needs of the Agency. All computer resources (including servers, laptops, desktops, tape storage libraries) located at the local units fall within this GSS.

FSCB Legacy is a general support system that provides resources for daily operations of the Washington Office, Regional offices, Research Stations, International Institute of Tropical Forestry (IITF) Forests and Districts. Although information about individuals may traverse through FSCB Legacy resources, individual applications and their management are responsible for reporting privacy act impact and completion of the USDA Privacy Impact Assessment Checklist.

The FSCB Legacy GSS contains information on government employees, including first name, last name, home unit, phone number, work email address, and job titles. The majority of the information in the system is entered by Forest Service employees either by a system administrator or by the employees themselves.

Typical transactions performed on the FSCB Legacy GSS include the various modules that currently exist on the GSS. These include Email, Data Base Services, and Office Automation.

A security certification of the FSCB Legacy GSS has been conducted in accordance with Office of Management and Budget Circular A-130, Appendix III, *Security of Federal Automated Information Resources*; NIST Special Publication 800-37, *Guide for the Security*

Certification and Accreditation of Federal Information Systems; DM3555-001 *Certification and Accreditation Methodology*; and FSM 6680 *Security of Information, Information Systems, and Information Technology*

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?

FSCB Legacy GSS contains information on government employees, including first name, last name, home unit, phone number, email address, and job title.

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

The majority of the information in the system is entered by Forest Service employees either by a 'system administrator' or by the employees themselves.

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

The information is being used to authenticate a user when they login to the system and for e-mail purposes.

1.4 How is the information collected?

Forest Service employees

1.5 How will the information be checked for accuracy?

Forest Service employees verify.

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

Not Applicable?

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

Access to the system is available by username and password assigned by the Chief Information Office (CIO) Application Hosting Line of Service (AHLOS). Once authenticated, access to data is through appropriate system roles. Roles are designated by a system administrator. Physical access safeguards are in place for any documents containing personal information. Safeguards include: secured file cabinets, secured computer rooms, and/or tape libraries that can be accessed only by authorized personnel. Electronic access to records is controlled through system roles.

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 data collected is used to provided authorized individuals access to email addresses, street addresses and phone number for the Forest Service

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

Data is collected in a variety of means, however the primary point of entry is during the Identification Requesting Process located in the Customer Help Desk (CHD).

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

N/A

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.

Only approved users are allowed access to the CHD where the information is stored. Access to the database that populates this information is limited through roles established in Active Directory (AD).

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?

Retention periods vary per Records Management Handbook – FSH 6209.11

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

Yes

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

The length of time data is retained on the FSCB Legacy GSS is based on an industry standard and in accordance with the Records Management Handbook requirements. Risks are mitigated through a means of off-site data retention (i.e., tape storage).

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?

Information is shared only on a need to know basis. The data collected within this environment is shared both internal and external to the CIO staff. Internal utilization is based on the creation and management of the FS employee's access identification profile. External information is shared through the Email system where the Employee Contact Information is made available.

4.2 How is the information transmitted or disclosed?

Information utilized by the CIO is transmitted through access controlled databases. Information located within the Email system is provided through the Email application system. This data is available to all FS employees.

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 information shared within the Email system is limited to the individual employee name and system location site. Further information is populated by the employee as they deem appropriate. Access to the information is limited based on the security settings in place on the user's access profile and also security controls the employee has the flexibility to manage based on their needs.

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?

The information is not shared externally.

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.

N/A

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

N/A

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

N/A

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?

The information collected is based on Human Resources documentation provided by the employee, at that time the employee is made aware of the information needs. Only basic information is utilized and made available for the initial requirements.

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

Individuals do have the right to decline the provision of the information; however doing so will limit their ability to obtain a profile to gain access to the information technology 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?

No, the individuals do not have the right to accept only particular use of information. They must accept all uses or no uses.

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.

No data is collected that would permit the system to do any profiling. Individuals receive a notification every 30 days to update their personal profile information. This is a voluntary collection of data.

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 individuals may view/update their own information at any time through Lotus Notes profile update.

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

An automated notification process is in place to request updated information to the Email directory. This information collection update is voluntary to the employee.

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

Every 30 days, a notification screen displays on the employee's computer, when the Email application is opened, requesting verification of their information.

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

N/A

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

Information collected in this location is limited based on the original request for access. The individual is allowed to populate the information with more information as they feel is appropriate. Until they choose to add the additional information, outside personnel will not be able to retrieve any information related to the individual.

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 data is authorized through systems roles. Employees have access to their own personal information. A system administrator can make changes based on the individual's needs.

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?

Security and privacy training is provided on an annual basis for individuals who maintain profiles on the system. In addition, an individual is required to recertify their

profile through an access ID table. This requires them to read a statement about employee's responsibilities and data portion.

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

Yes

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

Systems are currently monitored for unusual actions through the Foundstone Scanning. The system logs collect data which is sent to a collection server. This information is reviewed by Vulnerability Management teams and for anomalies and reported when inappropriate activities are noticed.

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 privacy risks identified are minimal based on the notation the information is primarily provided by the employee. They have the authority to limit the information shared through the system. Security controls that are in place are the review of the system access logs, limited access based on security roles (least functionality and roles and responsibilities). Access to sensitive data is limited on an as needed basis and must be approved prior to the granting of the access.

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?

This is a General Support System for the Forest Service environment. The scope of this GSS is the Washington Office, Regional Offices, Research Stations, IITF, Forest and District Offices.

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

No

Responsible Officials

Vaughn Stokes, Chief Information Officer

United States Department of Agriculture, Forest Service

Approval Signature

Name
Title
United States Department of Agriculture