Privacy Impact Assessment (PIA)

Fire Program Analysis System Phase 2 (FPA-2)

Revision: 1

USDA FOREST SERVICE

Prepared By:

Dan Keller
Senior Project Manager

Date: November 29, 2007

REVISION AND HISTORY PAGE

Document Version #	Revision Date	Description of Change	Section #/ Paragraph #	Page #	Initials

REVIEW PAGE

The following signatures represent the review and acceptance of the Privacy Impact Assessment (PIA) for the Forest Service (FS) Fire Program Analysis System (FPA).

Date	IRM C&A Project Manager	Signature

Comment:

Date	IRM C&A System Project Manager	Signature

Comment:

Date	Information System Security Officer	Signature

Comment:

Date	System Owner	Signature

Comment:

TABLE OF CONTENTS

1 PRIVACY IMPACT ASSESSMENT

1.1 Introduction

The objective of the PIA is 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. These requirements are drawn from the Privacy Act of 1993, Children's Online Privacy Protection Act of 1998, Freedom of Information Act, Paperwork Reduction Act of 1995, Office of Management and Budget Memoranda M-99-18 dated June 2, 1998 and M-00-13 dated June 22, 2000 and OCIO memorandum, Use of Cookies on Web Pages, DR 3410-1, Information Collection Activities, and DR 3080-1, Records Disposition

The PIA is a Government requirement that helps to ensure that system owners and developers consider and evaluate existing statutory information management requirements that must be applied to new or modified applications that contain personal information. The goals accomplished in completing this PIA include:

- Providing USDA FS management with the tools to make informed policy and system design decisions.
- Ensuring accountability for privacy issues.
- Ensuring a consistent format and structured process for analyzing both technical and legal compliance of the application.
- Providing basic documentation on the flow of personal information within the application.

1.2 Summary of Results of the Privacy Impact Assessment

A review of the application, as installed by USDA FS, indicates that FPA does not maintain identifiable form of information on individual employees.

USDA Privacy Impact Assessment Form

Agency: Forest Service

System Name: FPA

System Type: Major Application

System Categorization (per FIPS 199): Moderate

Description of the System:
Fire Program Analysis - Phase 2 (FPA-2), is an interagency project of the five federal wildland fire management agencies:

- US Forest Service (USFS)
- Department of Interior (DOI) Bureau of Land Management (BLM)
- DOI National Park Service (NPS)
- DOI U.S. Fish & Wildlife Service (FWS)
- DOI Bureau of Indian Affairs (BIA).

FPA-2 has involved the National Association of State Foresters as well as state and local fire organizations.

The FPA-2 project will close important performance gaps for the interagency wildland fire management agencies, including gaps identified in: Federal Wildland Fire Policy, National Fire Plan, The Hubbard Report (i.e., Developing an Interagency, Landscape Scale Fire Planning Analysis and Budget Tool, November 2001), as well as discussions with and direction from OMB and the Congressional Appropriations Committee.

FPA is chartered by the US Forest Service and Department of Interior (DOI). The FPA Scope Definition (draft dated April 6, 2007) states: "FPA will provide information relative to cost-effective, interagency, wildland fire management programs for a range of budget levels." Cost-effective program scenarios will recognize the interactions among fire program components (e.g., the synergistic interactions of fuels treatments, wildland fire use, and suppression of unwanted wildland fires). These scenarios will be evaluated at the Fire Planning Unit (FPU) and national level to develop effective program options.

A functional prototype is scheduled for completion in June 2007 and an operational application by June 2008. Training and implementation will be provided, as will two years of Operations and Maintenance (O&M), as part of the FPA project. FPA-2 is managed according to established OMB and Project Management Institute (PMI) standards and practices, including ANSI 748 Earned Value Management (EVM) and Certification and Accreditation (C&A) activities.

Who owns this system? (Name, agency, contact information)

USDA Forest Service
Deputy Chief, State and Private Forestry
P.O. Box 96090
Washington, D.C. 20090-6090

Who is the security contact for this system? (Name, agency, contact information)
Stephen A. Simon
Senior Information Management System Project Manager
US Forest Service – Fire and Aviation Management
USFS Billings Fire Cache
Airport Industrial Park – Building IP7
551 Northview Drive
Billings, MT 59105
406-896-2877

Greg Schmitz, Information Systems Security Program Manager
USDA National Information Technology Center (NITC)
8930 Ward Parkway
Kansas City, MO 64114
Phone: 816-926-2338

Who completed this document? (Name, agency, contact information)
Forest Service Information Resource Management (FS IRM)
Fire and Aviation Management

DOES THE SYSTEM CONTAIN INFORMATION ABOUT INDIVIDUALS IN AN IDENTIFIABLE FORM?

Indicate whether the following types of personal data are present in the system.

QUESTION 1 Does the system contain any of the following type of data as it relates to individual:	Citizens	Employees
Name	No	No
Social Security Number	No	No
Telephone Number	No	No
Email address	No	No
Street address	No	No
Financial data	No	No
Health data	No	No
Biometric data	No	No
QUESTION 2 Can individuals be uniquely identified using personal information such as a combination of gender, race, birth date, geographic indicator, biometric data, etc.? NOTE: 87% of the US population can be uniquely identified with a combination of gender, birth date and five digit zip code[1]	No	No
Are social security numbers embedded in any field?	No	No
Is any portion of a social security numbers used?	No	No
Are social security numbers extracted from any other source (i.e. system, paper, etc.)?	No	No

If all of the answers in Questions 1 and 2 are NO, 

You do not need to complete a Privacy Impact Assessment for this system and the answer to OMB A-11, Planning, Budgeting, Acquisition and Management of Capital Assets, Part 7, Section E, Question 8c is:

3. No, because the system does not contain, process, or transmit personal identifying information.

If any answer in Questions 1 and 2 is YES, provide complete answers to all questions below.

[1] Comments of Latanya Sweeney, Ph.D., Director, Laboratory for International Data Privacy Assistant Professor of Computer Science and of Public Policy Carnegie Mellon University To the Department of Health and Human Services On "Standards of Privacy of Individually Identifiable Health Information". 26 April 2002.

1.2.1 DATA IN THE SYSTEM

1. Generally describe the information to be used in the system in each of the following categories: Customer, Employee, and Other.	
2a. What are the sources of the information in the system?	
2b. What USDA files and databases are used? What is the source agency?	
2c. What Federal Agencies are providing data for use in the system?	
2d. What State and Local Agencies are providing data for use in the system?	
2e. From what other third party sources will data be collected?	
2f. What information will be collected from the customer/employee?	
3a. How will data collected from sources other than the USDA FS records and the customer be verified for accuracy?	
3b. How will data be checked for completeness?	

1.2.2 ACCESS TO THE DATA

1. Who will have access to the data in the system (Users, Managers, System Administrators, Developers, Other)?	
2. How is access to the data by a user determined? Are criteria, procedures, controls, and responsibilities regarding access documented?	
3. Will users have access to all data on the system or will the user's access be restricted? Explain.	
4. What controls are in place to prevent the misuse (e.g. browsing, unauthorized use) of data by those having access?	
5a. Do other systems share data or have access to data in this system? If yes, explain.	
5b. Who will be responsible for protecting the privacy rights of the customers and employees affected by the interface.	
6a. Will other agencies share data or have access to data in this system (International, Federal, State, Local, Other)?	
6b. How will the data be used by the agency?	
6c. Who is responsible for assuring proper use of the data?	

1.2.3 ATTRIBUTES OF THE DATA

1. Is the use of the data both relevant and necessary to the purpose for which the system is being designed?	
2a. Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected?	
2b. Will the new data be placed in the individual's record (customer or employee)?	
2c. Can the system make determinations about customers or employees that would not be possible without the new data?	
2d. How will the new data be verified for relevance and accuracy?	
3a. If data is being consolidated, what controls are in place to protect the data from unauthorized access or use?	
3b. If processes are being consolidated, are the proper controls remaining in place to protect the data and prevent unauthorized access? Explain.	
4a. How will the data be retrieved? Can it be retrieved by personal identifier? If yes, explain.	
4b. What are the potential effects on the due process rights of customers and employees of: • consolidation and linkage of	

files and systems; • derivation of data • accelerated information processing and decision making; • Use of new technologies.	
4c. How are the effects to be mitigated?	

1.2.4 MAINTENANCE OF ADMINISTRATIVE CONTROLS

1a. Explain how the system and its use will ensure equitable treatment of customers and employees.	
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?	
2b. Explain any possibility of disparate treatment of individuals or groups.	
2c. What are the retention periods of data in this system?	
2d. What are the procedures for eliminating the data at the end of the retention period? Where are the procedures documented?	
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?	
3a. Is the system using technologies in ways that the USDA has not previously employed (e.g. Caller-ID)?	
3b. How does the use of this technology affect customer/employee privacy?	
4a. Will this system provide the capability to identify, locate, and monitor individuals? If yes, explain.	

4b. Will this system provide the capability to identify, locate, and monitor groups of people? If yes, explain.	
4c. What controls will be used to prevent unauthorized monitoring?	
5a. Under which Systems of Record notice (SOR) does the system operate? Provide number and name.	
5b. If the system is being modified, will the SOR require amendment or revision? Explain.	

PRIVACY IMPACT ASSESSMENT AUTHORIZATION MEMORANDUM

I have carefully assessed the Privacy Impact Assessment for the

_____

(System Name)

This document has been completed in accordance with the requirements of the E-Government Act of 2002.

We fully accept the changes as needed improvements and authorize initiation of work to proceed. Based on our authority and judgment, the continued operation of this system is authorized.

_____ _____

System Manager/Owner
OR Project Representative
OR Program/Office Head.

Date

_____ _____

Agency's Chief FOIA officer
OR Senior Official for Privacy
OR Designated privacy person

Date

_____ _____

Agency OCIO

Date