Privacy Impact Assessment (PIA)

Resource and Ordering Status System (ROSS)

Revision: 2.0.5

USDA FOREST SERVICE

Prepared By: Fire & Aviation Management

Date: January, 2008

REVISION AND HISTORY PAGE

Document Version #	Revision Date	Description of Change	Section #/ Paragraph #	Page #	Initials
2.0.3	10/07	Resolve formatting changes	All	All	Xacta
2.0.4	10/07	Finalize format	All	All	Xacta
2.0.5	1/08	Update & correct PIA.	1.2.1, 2b 1.2.2, 1 1.2.4, 5	9, 11, 16	JCS

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 ROSS maintains identifiable form of information on individual employees. The system stores and tracks all tactical, logistical, and support resources that are mobilized by the incident dispatch community. A completed USDA Privacy Impact Assessment Form is provided as Attachment A.

USDA Privacy Impact Assessment Form

Agency: Forest Service

System Name: Resource Ordering and Status System (ROSS)

System Type: Major Application

System Categorization (per FIPS 199): Moderate

Description of the System:
The ROSS system provides automated support to interagency and agency dispatch and coordination offices within the wildland fire organization. The system: 1) provides current status of resources available to support all-risk activities such as wildfires and floods; and 2) enables dispatch offices to exchange and track resource order information electronically.

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
Sponsor: National Wildfire Coordinating Group (NWCG)

Who is the security contact for this system? (Name, agency, contact information)
Stephen Simon – ROSS Security Officer
USDA-Forest Service
USFS Billings Fire Cache
Airport Industrial Park – Building IP7
551 Northview Drive
Billings, MT 59105

Jay Peters, NITC Information Systems Security Program Manager
USDA National Information Technology Center
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	Yes
Social Security Number	No	Yes
Telephone Number	No	Yes
Email address	No	Yes
Street address	No	Yes
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	Yes
Is any portion of a social security numbers used?	No	Yes
Are social security numbers extracted from any other source (i.e. system, paper, etc.)?	No	Yes

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.	Customer Data: None Employee Data: The employee information used by this system identifies an individual's unique information, matches incident assignments with qualified individuals, obligates, and tracks the status of resources mobilized by the dispatch community for wildland fire protection and other incidents. The following required information is collected within the ROSS application: • Social Security Number (SSN) (used to generate a Unique Identifier for ROSS) • Last and First Name • Home organization • Providing organization • Owning organization • Managing dispatch office • Position(s) qualified to perform • Position(s) qualified to perform as a trainee The following optional information is collected within the ROSS Application: • Middle Name • Employment Status (Regular Employee, Ad/EFF, Other) • Phone numbers (home, work, pager, fax) • E-mail Address • Weight • Gender • Home Location • Preferred jetport for mobilization and demobilization. • Fitness rating and expiration date • Employee Status (Available, Unavailable, At Incident, Mob-In-Route, Demob-In-Route, Reserved, Returned From Incident). • Employee Area of Availability (National, Geographic, Local)

	• Employee Unavailability Dates The maximum number of days an employee may be assigned during a single assignment. <u>Other data (modules in the ROSS application)</u>: • Airports • Aviation Hazards • Locations • Organizations • Political Units • Contracts
2a. What are the sources of the information in the system?	With the exception of the following data sources, all data within ROSS is entered by the user: <u>Qualification Systems</u>: • Qualification systems maintain individual qualifications; experience and training records needed to certify employees in wildland and prescribed fire positions. This information is imported into the ROSS application. When data is imported, each employee's record must include the employees Social Security Number (to assure uniqueness). When records are manually input into the system, the SSN is not required as ROSS generates a unique number for the record). The SSN or ID number is NOT DISPLAYED to the user. <u>USGS (Geographic Names and Places)</u>: • Description data for populated areas (Cities, Counties, and States) is imported from the USGS Names and Places database. <u>Federal Aviation Agency (FAA)</u>: • Airports and navaids are imported into the ROSS.
2b. What USDA files and databases are used? What is the source agency?	ROSS is an interagency system. Data files / databases used for import come from a variety of agencies. Some system databases come from multiple agencies that all use the same database. The following is a listing of these sources and agencies

	responsible for the data. • Incident Qualifications and Certifications System (IQCS) – This system was developed by the Department of Interior, but is used by all Federal Wildland Agencies (Bureau of Indian Affairs, Bureau of Land Management, Fish and Wildlife Service, National Park Service, Forest Service). • Incident Qualifications System (IQS) – IQS is managed by State Forestry agencies nationwide. • Incident Cache Business System (ICBS) – ICBS is managed by the Forest Service. ICBS is being re-engineered and will be released in 2008.
2c. What Federal Agencies are providing data for use in the system?	• Bureau of Indian Affairs • Bureau of Land Management • Fish and Wildlife Service • National Park Service • Forest Service • Animal Plant and Health Inspection Service • Federal Aviation Administration • Federal Emergency Management Administration
2d. What State and Local Agencies are providing data for use in the system?	Wildland Fire Agencies from all 50 States and the Colorado Department of Public Safety provide data for use in ROSS.
2e. From what other third party sources will data be collected?	None
2f. What information will be collected from the customer/employee?	Employee information collected uniquely identifies the individual. That information may include: • Social Security (used to generate a Unique Identifier for ROSS) • Last and First Name • Home Unit • Provider • Owner • Home Dispatch Office • Middle Name • Employment Status • Phone numbers (home, work, pager, fax) • E-mail Address • Weight • Gender

	• Position(s) qualified to perform • Position(s) qualified to perform as a trainee • Home Location • Preferred Jetport • Fitness Rating • Fitness Rating Expiration Date Unavailable dates Maximum days may be assigned
3a. How will data collected from sources other than the USDA FS records and the customer be verified for accuracy?	Data from other agency or interagency systems is collected through user input or import mechanisms designed specifically for import of the data.
3b. How will data be checked for completeness?	Import mechanisms within ROSS review data for completeness. Records that do not have good data integrity are rejected.

1.2.2 ACCESS TO THE DATA

1. Who will have access to the data in the system (Users, Managers, System Administrators, Developers, Other)?	Access to data is authorized through systems roles. Data related to Social Security Number or system security cannot be accessed by a user. Access to this data must be through system security officers at the host computer center. In addition, all SSNs are encrypted in the database. All data except as discussed previously is accessible to users with designated roles that permit access.
2. How is access to the data by a user determined? Are criteria, procedures, controls, and responsibilities regarding access documented?	Access to the system is available only by username and password. Once authenticated access to data is through appropriate system roles. Physical access safeguards are in place for any records 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. Any sensitive data transmitted over a network is encrypted (i.e., phone number, gender, weight).
3. Will users have access to all data on the system or will the user's access be restricted? Explain.	ROSS is a role-based system. Access to different roles is determined by the account manager. Username and passwords are required for all users.
4. What controls are in place to prevent the misuse (e.g. browsing, unauthorized use) of data by those having access?	System roles have been established to control the level of use by a customer. System roles are administered on a local, geographic, and national basis. During system training, security and rules of behavior are instructed. A ROSS Rules of Behavior document must be signed by each user which identifies "ethics and conduct" for using the system. Any action taken by a user is attributed to that username and documented in the system. Persons using the system should be aware that the ROSS System is a Privacy Act system of records. There are criminal penalties for individual's who violate the Privacy Act. All user agencies of the system have internal agency standard security awareness training that is outside the scope of the ROSS system.
5a. Do other systems share data or have access to data in this system?	No. ROSS does not directly share (electronically) data with another system.

If yes, explain.	
5b. Who will be responsible for protecting the privacy rights of the customers and employees affected by the interface.	The protection of the employee data is the responsibility of the local manager.
6a. Will other agencies share data or have access to data in this system (International, Federal, State, Local, Other)?	Other agencies not identified as a user of the system do not have access to data in the system. Disclosure may be made to the Department of Justice to the extent that each disclosure is compatible with the purpose for which the record was collected and is relevant and necessary to litigation or anticipated litigation in which one of the following is a party or has an interest: (a) the agency, (b) the agency employee in his or her official capacity, (c) an agency employee in his or her individual capacity where the Department of Justice is representing or considering representation of the employee, or (d) the Untied States where the litigation is likely to affect the agency. Records may be disclosed to a Member of Congress or to a Congressional staff member in response to an inquiry of the Congressional office made at the written request of the person about whom the record is maintained.
6b. How will the data be used by the agency?	Such disclosure identified in 6a include those made in the course of presenting evidence, conducting settlement negotiations, responding to subpoenas, and requests for discovery.
6c. Who is responsible for assuring proper use of the data?	Proper use of the system and associated data is the responsibility of the unit managers where the system is utilized.

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?	Yes
2a. Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected?	No
2b. Will the new data be placed in the individual's record (customer or employee)?	No
2c. Can the system make determinations about customers or employees that would not be possible without the new data?	Not applicable
2d. How will the new data be verified for relevance and accuracy?	Not applicable.
3a. If data is being consolidated, what controls are in place to protect the data from unauthorized access or use?	Not applicable – data will not be consolidated.
3b. If processes are being consolidated, are the proper controls remaining in place to protect the data and prevent unauthorized access? Explain.	Not applicable – processes will not be consolidated.
4a. How will the data be retrieved? Can it be retrieved by personal identifier? If yes, explain.	Data are generally retrieved through various screens in the software and through reports. The personal identifier is not displayed to any user and cannot be requested through a reporting mechanism. Person data which is used for incident assignments can be archived from the production system into the system data warehouse. Access to the data is through data

	exports and reporting mechanisms for users on a "need to know" (role-based access) basis. Access to sensitive information is blocked except for those specifically authorized to have access.
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.	None
4c. How are the effects to be mitigated?	Not Applicable

1.2.4 MAINTENANCE OF ADMINISTRATIVE CONTROLS

1a. Explain how the system and its use will ensure equitable treatment of customers and employees.	All decisions that affect employees are determined outside of the system. Documentation regarding the results of a decision may be documented through actions within the system.
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?	Data is not stored at individual sites. Data is stored in a centralized national database. The ROSS application assures (through the use of business rules) the integrity of all data entered in the system.
2b. Explain any possibility of disparate treatment of individuals or groups.	Decisions regarding equitable treatment of customers and employees are not a part of this system. These decisions remain with management at the unit level.
2c. What are the retention periods of data in this system?	The records are stored in an electronic data warehouse and electronic media for a minimum of 7 years after the closure of an incident record. Historically, the retention needs for this type of data exceeds 20 years.
2d. What are the procedures for eliminating the data at the end of the retention period? Where are the procedures documented?	At this time, there are no procedures as the agency (Forest Service) direction is to retain the data indefinitely.
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?	Data within ROSS is moved to the system data warehouse after the closure of an incident. Once an incident is closed, further editing of the data is restricted.
3a. Is the system using technologies in ways that the USDA has not previously employed (e.g. Caller-ID)?	No, there is no additional effect on individuals whose information will reside on this system as that information was used in the previous manual system.
3b. How does the use of this technology affect customer/employee privacy?	Sensitive information about employees is needed in order for the employee to be activated (mobilized) in support of mission critical wildland resource protection operations, which are administered by state and Federal agencies.
4a. Will this system provide the capability to identify, locate, and monitor individuals? If yes,	Yes. Routine use of the system is to match incident assignments with qualified individuals. The system also provides the capability to status and track all tactical,

explain.	logistical, service, and support resources mobilized by the dispatch community.
4b. Will this system provide the capability to identify, locate, and monitor groups of people? If yes, explain.	Yes, the system provides the capability to status and track groups of people such as Incident Management Teams, Fire crews, or any other groups of people identified by a roster.
4c. What controls will be used to prevent unauthorized monitoring?	Username and password is required to access the system. System roles permit monitoring on an as authorized basis.
5a. Under which Systems of Record notice (SOR) does the system operate? Provide number and name.	USDA/FS-52, Resource Ordering & Status System
5b. If the system is being modified, will the SOR require amendment or revision? Explain.	A SORN was published in the Federal Register on January 14, 2005.

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