Privacy Impact Assessment

for

Fire National Enterprise Support System and Child Applications (Fire NESS)

Policy, E-Government and Fair Information Practices

Version: 1.3

Date: November 13, 2019

Prepared for: Forest Service, Fire National Enterprise Support System (Fire NESS)

Contact Point

Jeff Skirde

System Owner

USDA NRE Forest Service

208-387-5170

Reviewing Official

Cynthia Towers

Privacy Officer

USDA NRE Forest Service

(816) 844-4000

Abstract

This Privacy Impact Assessment (PIA) is about the Fire National Enterprise Support System (Fire NESS). Fire NESS is a General Support System (GSS) for the US Forest Service (FS) Fire and Aviation Management (FAM) mission area. The requirement for a PIA for Fire NESS stems from the Privacy Threshold Analyses (PTA) for Fire NESS and its hosted applications.

Overview

The purpose of the Fire NESS GSS is to consolidate server resources used by various FAM applications. Fire NESS provides Production, Training, and Development/QA environments for Fire Applications hosted at USDA's National Information Technology Center (NITC) in Kansas City, Missouri and at United States Geological Survey (USGS) Earth Resources Observation and Science (EROS) in Sioux Falls, South Dakota.

Fire NESS servers use system virtualization technologies to provide higher efficiencies, lower costs, and better system management. Fire NESS also enhances strategies for managing computing resources to reduce costs in hardware acquisition, software and OS licensing, power, floor space and asset management, as well as a Lightweight Directory Access Protocol (LDAP) services. System configuration and processes lead to increased productivity in administration including system, database, data, network, and security. In addition, Fire NESS implements a highly coordinated and efficient configuration management, change management, and control processes.

For the purposes of the Security Assessment and Authorization, the scope of the Fire NESS GSS includes hosted applications. All security controls for the hosted applications are documented and tested by Fire NESS. The following bullets summarize the key Fire NESS applications.

Enterprise Geospatial Portal (EGP): Fire EGP leverages a central source of spatial data for mapping, decision support, business intelligence, and situational awareness through multiple tools to view and analyze wildland fire data.

e-ISuite: A web-based application which is used at the Incident Command Post (ICP) and in agency offices to manage emergency incidents and planned events.

Fire and Aviation Management Web Applications (FAMWEB): FAMWEB is a group of independent applications and reports using a common database.

Federal Excess Property Management Information System (FEPMIS): Tracks government-owned property provided to State Forestry and Law Enforcement entities for the purpose of incident management.

Geospatial Technology and Applications Center (GTAC) hosted at EROS, and provides a range of remote sensing and related geospatial services. GTAC applications in the Fire NESS enable agency and interagency support to fire danger/risk forecasting, tactical and strategic scale active fire mapping, post-fire mapping and assessment and related resource mapping/monitoring activities.

Incident Information Web (InciWeb): An interagency all risk incident information source for incident related information. InciWeb provides a standardized reporting tool for authorized members of the interagency Public Affairs community. It also provides view-only access to basic incident information to the general public.

Interagency Cache Business System (ICBS) – An automated warehouse management system for supporting ordering, tracking inventories, and controlling inventories in the national and local incident support caches.

Interagency Resource Ordering Capability (IROC), mechanism to status, activate, and deploy a multitude of resources, which includes placing requests/orders for qualified individuals, teams, supplies, services and equipment to fight wildland fires and respond to all-hazard incidents. We are currently provisioning reporting pieces of IROC in the DISC PaaS environment that will continue after ROSS goes away.

NAP application is an authentication tool for those not federal employees used for many of our applications.

National Interagency Fire Center File Transfer Protocol (NIFC FTP): Provides a secure file sharing service across all fire support personnel nationwide (e.g., fire operations and support, radio information, InfraRed data distribution, Incident Action Plans).

National Interagency Situation Reporting System (SIT/209): Used to collect and disseminate status information involving all hazard incident activity and resources allocated by all wildland fire management agencies. Agencies send status information to their Geographic Area Coordination Center (GACC) to generate fire information reports using SIT/209.

Operational Loads Monitoring collects and stores information from the flight data recorders installed in some of our agency-owned and contracted aircraft.

Resource Ordering and Status System (ROSS): The interagency resource ordering and status system used by more than 320 dispatch offices (Federal & State) across the country.

Weather Information Management System (WIMS): The host for the National Fire Danger Rating System (NFDRS) and helps manage information stored in NIFMID.

Wildland Fire Decision Support System (WFDSS) - A decision support tool that helps fire managers and analysts make strategic and tactical decisions for all types of wildland fires.

All of these applications contain name information (first and last name) as part of the LDAP. Some applications also collect work phone number, and work email address. This information is collected to assign a user identifier and to facilitate contacting the user who "owns" the user account if necessary.

The e-ISuite application collects and maintains first and last name, address, and telephone numbers (including work, cellular, and fax number). The information could be collected about Forest Service employees, Federal interagency employees (e.g., Department of Interior's Bureau of Land Management), state employees, local employees, or individuals. For specific types of individuals (Administratively Determined or ADs), e-ISuite collects the Department of Interior's (DOI) Employee Common Identifier (ECI).

The ICBS application collects and maintains name information for the purpose of shipping cache supplies such as axes. Shipments must be sent to a named individual, so the application contains name, work address, and work phone numbers. Information is collected about Forest Service and other Federal interagency personnel.

Operational Loads Monitoring collects and stores information from the flight data recorders installed in some of our agency-owned and contracted aircraft.

The ROSS application collects and maintains personnel resource ordering and status information including names, contact information (e.g., phone and email), as well as has fields to collect gender and weight. Name and contact information is collected to enable the individual to be contacted to be dispatched to incidents and support wildland fire and all hazard activities. Gender information allows incident team members to be identified to share hotel rooms. Weight information is sometimes collected to load balance helicopters and aircraft. The information in ROSS is for Forest Service employees, Federal interagency employees, state employees, local employees, and individuals (e.g., an individual who provides a bulldozer to support wildland fire fighting activities).

This PIA is organized by two components for each answer. The first component is for Fire NESS and all the applications that collect information to support LDAP services including creation and management of user accounts. The second component is for hosted specific information for the e-ISuite, ICBS, and ROSS applications.

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 Identification

What information is collected, used, disseminated, or maintained in the system?

Fire NESS LDAP Services: Fire NESS and the hosted applications collect information to support the user identifier for accessing the GSS or the application. This information includes:

Last and First Name

Work Email

Work Phone

Contractor or Employee designation

AMIS does not collect, process, generate, or store PII information.

eGP does collect, process, generate, or store the following information on individuals:

Name (full name, mother's maiden name, maiden name of the individual, nickname, or alias)

Street or email addresses

The e-ISuite application collects and retains the following required information for all personnel assigned to an incident:

Last and first name

Optional e-ISuite information collected includes:

Address

Email

Phone numbers (including work, cellular, home, fax)

For AD employees, e-ISuite also collects DOI's ECI number.

FIRESTAT does collect, process, generate, or store the following on individuals:

Name (full name, mother's maiden name, maiden name of the individual, nickname, or alias)

Street or email addresses

GTAC does not collect, process, generate, or store PII information. Collects geospatial data satellite imagery and derived data products (e.g. active fire detections, vegetation indices, etc.); fire geospatial products and maps of wildfire activity locations; fire weather data/information; and fire forecast/risk data.

InciWeb does collect, process, generate, or store the following on individuals:

Name (full name, mother's maiden name, maiden name of the individual, nickname, or alias)

Street or email addresses

The ICBS application collects name information to identify customers and a local contact point for shipping supplies.

OLM does collect, process, generate, or store the following on individuals:

Name (full name, mother's maiden name, maiden name of the individual, nickname, or alias)

Street or email addresses

The ROSS application contains information on resources – personnel and equipment – that are dispatched to support wildland fire and all hazard incidents. The term "resource" will be used throughout this PIA to reference individual people who are dispatched through the ROSS application. These resources do not necessarily have access to the ROSS application. ROSS application users are referred to as "users" in this PIA. The information used by ROSS identifies an individual resource's unique information, matches incident assignments with qualified individual resources, obligates and tracks the status of resources mobilized by the dispatch community for wildland fire protection and other incidents.

ROSS application collects the following required information for resources who wish to be dispatched to incidents:

Last and First Name

Street and email address

Health data (including height, weight, blood pressure, etc.)

The following optional information is collected within the ROSS application:

Middle Name

Phone numbers (work and/or personal)

E-mail Address

Gender

Weight

SIT/209 does collect, process, generate, or store the following on individuals:

Name (full name, mother's maiden name, maiden name of the individual, nickname, or alias)

Street or email addresses

WIMS does collect, process, generate, or store the following on individuals:

Name (full name, mother's maiden name, maiden name of the individual, nickname, or alias)

Street or email addresses

WFDSS does collect, process, generate, or store the following on individuals:

Name (full name, mother's maiden name, maiden name of the individual, nickname, or alias)

Street or email addresses

1.2 Source

What is the source(s) of the information in the system?

Fire NESS LDAP Services: Information on individuals requesting an account for the GSS or any of the applications hosted on Fire NESS is collected from the individual themselves. Account applicants either fill in an on-line form or a paper based form. For the Fire NESS GSS, all accounts are submitted to, reviewed and access approved by the FAM Information System Security

Officer (ISSO). For the application specific accounts, approval processes varies based on business requirements.

Hosted Applications: e-ISuite data is entered by authorized users at various locations (e.g., offices, incident locations). Data about individual resources is provided by the person about themselves for input by authorized e-ISuite Users. In addition, e-ISuite obtains information from other systems. These include the ROSS and ICBS. e-ISuite, ROSS, and ICBS all share the same System Owner. For specific types of individuals (Administratively Determined or ADs), e-ISuite collects the DOI's ECI.

ICBS obtains name information for customers from the people ordering the supplies. ICBS also shares data with ROSS.

Data about individual ROSS resources is often provided by the person about themselves to the Dispatch Center. In addition, ROSS obtains information from several systems. These include two qualification systems: the DOI's Interagency Qualifications and Certifications System (IQCS), and the National Association of State Foresters (NASF) Incident Qualifications System (IQS).

ROSS also exchanges data with the California Department of Forestry and Fire Protection (CALFIRE) Altaris Computer Aided Dispatch (CAD) system.

ROSS also exchanges data with DOI's Integrated Reporting of Wildland-Fire Information (IRWIN) application.

In addition, ROSS exchanges data with the FS Virtual Incident Procurement (VIPR) system.

ROSS and ICBS also exchange data (ROSS and ICBS share the same system owner, along with e-ISuite).

Qualification Systems:

Two qualification systems provide information to ROSS about the qualifications of individual resources. These are summarized below.

Interagency Qualification and Certification System – IQCS provides qualifications data for Federal Employees that work for Wildland

Agencies including: Bureau of Indian Affairs, Bureau of Land

Management, Fish and Wildlife Service, National Park Service, and US Forest Service. Data is transmitted to ROSS from IQCS using secured web services.

IQCS and ROSS exchange personal information including (but not limited to): first name, last name, middle name; employee class; contact method (e.g.,

email, phone); body weight; gender; qualification status; qualification expiration date; fitness rating code; fitness rating code; fitness expiration date; and resource contact information.

Incident Qualifications System (IQS) – IQS provides qualifications data for State Employees that work for State Agencies that are cooperators for Federal Wildland Agencies.

IQS and ROSS exchange personal information including (but not limited to): first name, last name, middle name; employee class; contact method; gender; body weight; qualification status; qualification expiration date; fitness rating code; fitness expiration date; and resource contact information. These individuals are typically State or local agency employees.

Altaris CAD:

One CAD system exchanges data with ROSS. This is CALFIRE's Altaris CAD system. Altaris CAD and ROSS exchange personal information including (but not limited to): name of the contact for the incident radio frequency, the name of the person requesting a resource, name of the person who will pick up an item, address of a person who will pick up an item, phone of the person who will pick up the item, first name of the person resource, last name of the person resource, middle name of the person resource, as well as the first and last name of a person associated with a user account used to make a documentation entry. These individuals could be FS employees, DOI employees, as well as State or local employees, and potentially individuals without an affiliation with a government agency.

IRWIN

IRWIN and ROSS exchange personal information including (but not limited to): incident commander first, last, and middle name; as well as the name and title of the person that approved the final fire report for the incident. These individuals could be FS employees, DOI employees, as well as State or local employees and potentially individuals without an affiliation with a government agency.

VIPR

VIPR and ROSS exchange personal information including (but not limited to):

Vendor company name, VIPR contact first name, VIPR contact last name, VIPR contact middle name, Vendor daytime name, vendor evening phone, vendor cell/alternate contact, vendor fax number, vendor email address, vendor street address, vendor city, vendor state, vendor zip code, as well as other attributes (such as mechanic's last name and mechanic's first name). These individuals could be FS employees, DOI employees, as well as State or

local employees and potentially individuals without an affiliation with a government agency.

ICBS

ICBS and ROSS exchange personal information including (but not limited to): the name of the contact for the incident radio frequency; first, last, and middle name of the person associated with a user account; username; work address; work phone; work email; position title; and name of the shipment driver. These individuals are typically employed by the FS or DOI.

1.3 Justification

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

Fire NESS LDAP Services: Data on the account applicants is collected and maintained to ensure that the user can be contacted if necessary regarding their user account.

Child Applications: All e-ISuite data are collected, used, disseminated for the purposes of supporting incident business operations for the purpose of check-in, demobilization, time reporting, and cost reporting in response to wildland and all hazard incidents.

ICBS collects name information to ensure that shipments are sent to the correct person.

All ROSS data are collected, used, disseminated, and maintained in ROSS for the purpose of dispatching personnel and other resources in response to wildland and all hazard incidents.

1.4 Collection

How is the information collected?

Fire NESS LDAP Services: Data on the Fire NESS account applicants is collected via a paper form which is emailed to FAM ISSO and Fire NESS Contracting Officer's Representative (COR) for contracted employees. For the other child applications, information is collected via a web based form or a paper form.

Child Applications: e-ISuite data are collected from the person themselves and entered by an authorized e-ISuite user. e-ISuite also receives data from ROSS.

Information for ICBS is collected directly from the individual placing the order.

For the ROSS application, data are collected and entered by an authorized ROSS user or via an interface with systems such as IQCS, IQS, EQS, Altaris CAD, and ICBS (as described in 1.2).

1.5 Validation

How will the information be checked for accuracy?

Fire NESS LDAP Services: Account applicant data is checked to ensure that the email address is functional.

Child Applications: e-ISuite data received by incident resources are checked for accuracy and completeness by an authorized e-ISuite user. To ensure that the e-ISuite user enters the data correctly, audits are performed by co-workers by verifying the information entered matches paper copy documentation. Data from other applications (e.g., ROSS), are imported using standard mechanisms that review the data automatically for completeness.

Not applicable for ICBS because the information is part of an employee's job duties.

ROSS resources may call the Dispatch Center to review, verify, or correct their contact information, the ROSS user entering the data in ROSS usually repeats the information provided back to the resource. If other methods are used – such as email, the ROSS user carefully compares their ROSS entries to the information provided to verify accuracy of the data entered. If an individual resource has access to ROSS "self-service" portal, then they are responsible for their own data accuracy.

Data from IQCS, IQS, EQS, and Altaris CAD are imported using standard mechanisms that review the data automatically for completeness.

1.6 Authority

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

Fire NESS LDAP Services: The collection of account applicant information for the purpose of issuing user accounts is governed by the Rules of Behavior that all users must sign prior to obtaining access and the warning banner that all users acknowledge when logging on to the system.

Child Applications: The collection of account applicant information for the purpose of issuing user accounts is governed by the Rules of Behavior and warning banner that all users acknowledge when logging on to the system.

The e-ISuite project has a Charter from the National Wildfire Coordinating Group (NWCG). e-ISuite replaced the I-Suite application, which was covered by a System of Record Notice (SORN). The I-Suite SORN was published in the Federal Register on November 5, 2009 for the I-Suite application.

ICBS has a Charter from the NWCG.

ROSS has a Charter from the NWCG. ROSS operates under the guidance of the National Mobilization Guide and Dispatch Guides/Procedures. Policy is set by NWCG Member Agencies. In addition, ROSS was covered by a SORN, which was published in the Federal Register on January 14, 2005.

1.7 Risk Mitigation

Given the amount and type of data collected, discuss the privacy risks identified and how they were mitigated.

Fire NESS LDAP Services & Child Applications: Privacy risks for account applicant data are minimal because the user account data is only available to the entity responsible for approving and creating the user accounts. Privacy risks are minimal and are mitigated through the following measures.

1. All users must be identified and authenticated before accessing the systems. To obtain a Fire NESS user account, the user must request an account and have that request approved by their supervisor and the FAM ISSO. Application specific user accounts are approved in accordance with business processes specific to that application.

2. Once authenticated, access to the systems is through appropriate system roles. Roles are determined by based upon approved roles and responsibilities.

3. All user actions are attributed to that user name and documented in the system.

4. Rules of Behavior documents (e.g., FS-6600-6, -7, -8) must be reviewed and signed by each user which identifies “ethics and conduct” for using the system.

5. All users must acknowledge the security warning banner that appears upon log on each time. There are criminal penalties for individuals who violate the Privacy Act.

6. All passwords are specifically encrypted by code before they are transferred across the network to the server. The traffic between the server and LDAP is encrypted using 256 bit strength encryption. The passwords are stored encrypted with Advanced Encryption Standard (AES) 256.

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 Usage

Describe all the uses of information.

In addition to those disclosures generally permitted under 5 U.S.C. 552a (b) of the Privacy Act, all or a portion of the records or information contained in this system may be disclosed outside FS as a routine use pursuant to 5 U.S.C. 552a (b) (3) as follows:

A. To the Department of Justice (DOJ), including United States Attorney Offices, or other Federal agency conducting litigation or in proceedings before any court, adjudicative or administrative body, when it is necessary to the litigation and one of the following is a party to the litigation or has an interest in such litigation: USDA or any component thereof; any employee of FS in his/her official capacity; any employee of FS in his/her individual capacity where DOJ or FS has agreed to represent the employee; or the United States or any agency thereof, is a party to the litigation or has an interest in such litigation, and FS determines that the records are both relevant and necessary to the litigation and the use of such records is compatible with the purpose for which FS collected the records.

B. To a congressional office from the record of an individual in response to an inquiry from that congressional office made at the request of the individual to whom the record pertains.

C. To the National Archives and Records Administration or other Federal government agencies pursuant to records management inspections being conducted under the authority of 44 U.S.C. §§ 2904 and 2906.

D. To an agency, organization, or individual for the purpose of performing audit or oversight operations as authorized by law, but only such information as is necessary and relevant to such audit or oversight function.

E. To appropriate agencies, entities, and persons when: FS suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; The Department has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the Department or another agency or entity) or harm to the individual that rely

upon the compromised information; and the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Department's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

F. To contractors and their agents, grantees, experts, consultants, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for FS, when necessary to accomplish an agency function related to this system of records. Individuals provided information under this routine use are subject to the same Privacy Act requirements and limitations on disclosure as are applicable to FS officers and employees.

G. To an appropriate Federal, State, tribal, local, international, or foreign law enforcement agency or other appropriate authority charged with investigating or prosecuting a violation or enforcing or implementing a law, rule, regulation, or order, where a record, either on its face or in conjunction with other information, indicates a violation or potential violation of law, which includes criminal, civil, or regulatory violations and such disclosure is proper and consistent with the official duties of the person making the disclosure.

H. To the news media and the public, in consultation with counsel, when there exists a legitimate public interest in the disclosure of the information or when disclosure is necessary to preserve confidence in the integrity of FS or is necessary to demonstrate the accountability of FS's officers, employees, or individuals covered by the system, except to the extent it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy.

2.2 Analysis and Production

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

Fire NESS LDAP Services: There are limited reports which can be reviewed on the applicant user accounts (e.g., a system generated report listing user names and associated roles). These reports are available only to a limited set of users, such as the Interagency Incident Application Help Desk (IAHD).

Child Applications: Reports are at the discretion of each individual child application.

e-ISuite data can be retrieved through application provided screens for standard reports. All e-ISuite Enterprise data are stored in the FAMWEB DW and available to meet diverse needs of stakeholders.

Reporting tools are available only to authorized ROSS and ICBS users to analyze data. These reports use the Cognos reporting tool. Standard and customized reports are available and may be displayed in text or spreadsheet format.

2.3 Commercial/Public Use

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

Fire NESS LDAP Services & Child Applications: None of the data discussed in this PIA comes from commercially or publicly available data.

2.4 Risk Mitigation

Describe any types of controls that may be in place to ensure that information is handled in accordance with the above described uses.

Fire NESS LDAP Services & Child applications: Not Applicable. None of the data comes from commercially or publicly available sources.

Section 3.0 Retention

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

3.1 Time Period

How long is information retained?

Fire NESS LDAP Services & Child applications: Because Fire NESS and child application data deals with wildland fire incidents, information is retained indefinitely per Forest Service requirements.

3.2 Approval

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

Fire NESS LDAP Services & Child applications: Yes.

3.3 Risk Mitigation

Please discuss the risks associated with the length of time data is retained and how those risks are mitigated.

Fire NESS LDAP Services & Child applications: The risks that data are retained indefinitely are outweighed by the benefits of being able to associate the user account information with information specifically entered by the user about the incident.

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 Identification and Purpose

With which organization(s) outside of the Forest Service, but still within the Department of Agriculture is the information shared? What information is shared and for what purpose?

Fire NESS LDAP Services: LDAP information is not shared with anyone.

Child Applications: Not Applicable

4.2 Delivery and Disclosure

How is the information transmitted or disclosed?

Fire NESS LDAP Services: N/A.

Child Applications: N/A

4.3 Risk Mitigation

Considering the extent of internal information sharing, discuss the privacy risks associated with the sharing and how they were mitigated.

Fire NESS LDAP Services: N/A.

Child Applications: N/A

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 Identification and Purpose

With which external organization(s), outside of both the Forest Service and the Department of Agriculture, is the information shared? What information is shared, and for what purpose?

Fire NESS LDAP Services: None of the LDAP data is shared with an external organization.

Child Applications: At the close of an incident, e-ISuite Site data is provided to the incident host agency and transferred to e-ISuite Enterprise. The host agency may be external to the Forest Service (e.g., it may be a Department of Interior incident).

ROSS data are exchanged with the DOI, IQCS; NASF's IQS; APHIS' EQS, CALFIRE's Altaris CAD.

The interface with IQCS is documented through an existing, signed Interconnection Security

Agreement (ISA). The ISA was signed in 2015 and is valid for three years. Data sent from IQCS to ROSS include: first, last, and middle name; phone number; and work email. Data sent from ROSS to IQCS include first and last name. ROSS receives inbound requests from IQCS over a secure HTTPS connection using Transport Layer Security and uses a certificate to validate the trusted source. Messages from ROSS to IQCS use the same protocol configuration.

ROSS data are also exchanged with CALFIRE's Altaris Computer Aided Dispatch CAD system. This interface is documented through an existing, signed ISA. The ISA was signed in 2015 and is valid for three years. ROSS receives inbound requests from their Integration Server through a FIPS 140-2 approved encryption mechanism based upon a certificate to validate the trusted source. Messages from ROSS to CAD integration server use the same protocol configuration.

An Interconnection Security Agreement is in the development stage for the IQS interface. Data imported from IQS is done via file import and is not through a live interface. Data that is exchanged between ROSS and IQS

includes but, is not limited to, first, middle, and last name; gender; and body weight.

5.2 Compatibility

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.

Fire NESS LDAP Services: None of the LDAP data is shared with an external organization.

Child Applications: e-ISuite's predecessor application, I-Suite, was covered by a SORN. There is a SORN in place for ROSS (USDA/FS–52, Resource Ordering and Status System (ROSS)). Both the e-ISuite and ROSS SORNs are being updated.

5.3 Delivery and Security Measures

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

Fire NESS LDAP Services: None of the LDAP data is shared with an external organization.

Child Applications: e-ISuite data that are uploaded to the ESB are encrypted and the transmission itself is encrypted as specified in the SSP.

As documented in the ROSS-IQCS ISA, all information exchanged between ROSS and DOI's IQCS is encrypted. See the IQCS ISA section entitled, "Information Exchange Security, it states: "Security of the information exchange is through secured network connections between systems and the Enterprise Service Bus. The connections at each end are located within controlled access facilities, which are monitored 24 hours a day. Each system will authenticate its connection with the other prior to the exchange of encrypted data."

As documented in the ISA with CALFIRE's Altaris CAD, all information exchanged is encrypted. Also, the connections at each end are "located within controlled access facilities which are protected through security mechanisms provided by each agency."

5.4 Risk Mitigation

Given the external sharing, explain the privacy risks identified and describe how they were mitigated.

Fire NESS LDAP Services: None of the LDAP data is shared with an external organization.

Child Applications: All e-ISuite data sets are encrypted prior to being transmitted to the ESB. In addition, the transmission is also encrypted.

Section 6.0 System of Records Notice (SORN)

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 Requirement and Identification

Does this system require a SORN and if so, please provide SORN name and URL?

(Note: If a SORN is not required, answer "No" to this question, and "N/A" for questions 6.2 through 6.5.)

Yes, a SORN is required. A SORN is in place for Resource Ordering and Status System (ROSS) (USDA/FS–52,), however it is being updated on the Forest Service SORN page.

6.2 Individual Notification

Was notice provided to the individual prior to collection of information?

Fire NESS LDAP Services: An account applicant is given notice of the need to collect the information for Fire NESS and the hosted applications when they submit their request for a user account.

Child Applications: All users who wish to be employed on an incident must be in eISuite.

For ICBS users, this is part of their job duties.

The same ROSS information was collected manually, prior to the inception of the ROSS application. All users who wish to participate in incident management activities must be in ROSS in order to be dispatched.

6.3 Right to Decline

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

Fire NESS LDAP Services: Yes, an applicant can opt out of providing the information to obtain a user account. However, no user account will be issued without such information.

Child Applications: Yes, an individual resource can decline to submit all required information; however, doing so may disqualify the individual from

being dispatched to incidents within ROSS and could delay the payment process for AD and contract resources for e-ISuite. Individual resources can decline to submit any and all Optional information identified in Section 1.1 and Section 6.1 and will still be able to be dispatched to incidents.

ICBS information is required as part of the individual's job duties.

6.4 Right of Consent

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

Fire NESS LDAP Services: Yes. The applicant can decline to provide the information and not use the application; however, their job may not be performed without accessing the application.

Child Applications: Yes. The only use of information provided in e-ISuite is for work at an incident. If an individual does not wish to work at an incident, they need not be in e-ISuite. ICBS information is required as part of the individual's job duties. The only use of information provided in ROSS is for incident dispatch activities. If an individual does not wish to be dispatched to an incident, they do not have to be in ROSS.

6.5 Risk Mitigation

Describe how notice is provided to individuals, and how the risks associated with individuals being unaware of the collection are mitigated.

Fire NESS LDAP Services: For the account applicant, notice is provided on the web form or the user request paper form that users must fill out.

Child Applications: Notice is provided to individuals through the SORN. The only use of e-ISuite information is to support incident activities. If an individual does not wish to work on an incident, they do not have to be in e-ISuite. ICBS information is required as part of the individual's job duties. The risk that individuals are unaware of the collection is minimal – if a person wishes to be dispatched to support incident activities they must be in ROSS.

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 Access

What are the procedures that allow individuals to gain access to their information?

Fire NESS LDAP Services: For Fire NESS users, account applicants can call the FAM ISSO to review their information. For the applications, they can follow the established business processes.

Child Applications: Resources entered in e-ISuite review their information by receiving a Draft copy printout of their invoice(s) to review for accuracy and completeness.

ICBS information can be reviewed in various Agency specific Human Resource (HR) systems.

Resources dispatched through ROSS can review their information in two ways. One way is to contact their home Dispatch Office via phone to review, verify, and correct their information. Another way is available to users whose Dispatch Offices set up the "self-service" functionality in ROSS. For those users who have self-service access, they can access their information and update it as necessary.

In accordance with the Freedom of Information Act (FOIA) and USDA regulations at

7 Code of Federal Regulations (CFR), any person can request access to USDA Forest Service (FS) records. The FOIA requires the FS to disclose records unless the information is exempt from mandatory disclosure under the FOIA (e.g., classified national security, business proprietary, personal privacy, investigative). See http://www.fs.fed.us/im/foia/

Your request must be in writing (view a sample FOIA request letter). Indicate that you are making a request under the FOIA, and address the request to the Region or Station that is responsible for the information you are requesting. If you are not sure which Region or Station within the FS has the information you want, send your request to the FS FOIA Officer at the following address:

USDA Forest Service, FOIA Service Center

1400 Independence Avenue, SW

Mail Stop: 1143

Washington, DC 20250-1143

VIA E-MAIL: wo_foia@fs.fed.us

VIA FAX: (202) 260-3245

7.2 Correction

What are the procedures for correcting inaccurate or erroneous information?

Fire NESS LDAP Services: For Fire NESS users, account applicants can call the FAM ISSO to review their information. For the applications, they can follow the established business processes.

Child Applications: The appropriate and authorized e-ISuite user is contacted to correct inaccurate or erroneous information. The correction is made and another Draft copy printout is presented to the resource for review.

ICBS information can be corrected by coordinating with their respective HR organization.

For ROSS, as described in 7.1, the procedures are either to make a phone call to the Dispatch Center to review, verify, and correct information or to use self-service to access their information. Note: there is incentive for both the Dispatch Office and the resource to have up to date accurate information in ROSS. The Dispatch Office needs and wants to be able to contact resources quickly so they can be mobilized quickly in response to an incident. The resource wants the Dispatch Office to be able to contact them so that they can be assigned to an incident.

In accordance with FOIA and USDA regulations at 7 CFR, any person can request access to USDA Forest Service records. The FOIA requires the FS to disclose records unless the information is exempt from mandatory disclosure under the FOIA (e.g., classified national security, business proprietary, personal privacy, investigative). See http://www.fs.fed.us/im/foia/

Your request must be in writing (view a sample FOIA request letter). Indicate that you are making a request under the FOIA, and address the request to the Region or Station that is responsible for the information you are requesting. If you are not sure which Region or Station within the FS has the information you want, send your request to the FS FOIA Officer at the following address:

USDA Forest Service, FOIA Service Center

1400 Independence Avenue, SW

Mail Stop: 1143

Washington, DC 20250-1143

VIA E-MAIL: wo_foia@fs.fed.us

VIA FAX: (202) 260-3245

7.3 Notification

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

Fire NESS LDAP Services: Account applicants are notified by the application owners regarding how to correct information.

Child Applications: All of the available options for correcting personal information are known through long-standing business practices.

7.4 Redress Alternatives

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

Fire NESS LDAP Services: No formal redress is necessary for the applicant user accounts.

Child Applications: No alternatives are necessary since both the Dispatch Center and the resource (for ROSS) and the Incident and resource (for e-ISuite) share motivation for ensuring accuracy of information.

Alternatives for ICBS are at the discretion of the Agency's HR organization.

7.5 Risk Mitigation

Please discuss the privacy risks associated with the redress available to individuals and how those risks are mitigated.

Fire NESS LDAP Services: There are no privacy risks associated with the redress available to those with user accounts.

Child Applications: Privacy risks to the resources who contact the appropriate personnel to update their information are mitigated in several ways. First, the person with the ability to update e-ISuite must be an authorized e-ISuite user. This means that they must be authorized to use e-ISuite by their Supervisor,

have taken appropriate security awareness training, sign the Rules of Behavior, and acknowledge the warning banner.

Privacy risks are the responsibility of the Agency's HR organization for ICBS.

Privacy risks to the resources who contact the Dispatch Office by phone to update their information are mitigated in several ways. First, the person at the Dispatch Office with the ability to update ROSS must be an authorized ROSS user. This means that they must be authorized to use ROSS, have taken appropriate security awareness training, sign the Rules of Behavior, and acknowledge the warning banner. For those who use self-service, the Web site is https and requires a user ID and password to access the information. Only the personal information of the approved self-service users is available for review and update.

Section 8.0 Technical Access and Security

The following questions are intended to describe technical safeguards and security measures.

8.1 Procedures

What procedures are in place to determine which users may access the system and are they documented?

Fire NESS LDAP Services: Fire NESS and each application have their own procedures for determining which users may access the system or application. These are documented in accordance with each project.

Child Applications: All e-ISuite users are specifically identified as authorized in accordance with NIST 800-53 control for AC-2, Account Management. All e-ISuite Enterprise accounts must be reviewed and approved via the NAP; e-ISuite Site accounts must be approved by the IMT Command and General staff, who follow established business processes when reviewing account requests.

For ICBS, users are specifically identified as authorized in accordance with NIST 800-53 control for AC-2, Account Management.

All ROSS users are specifically identified and authorized in accordance with NIST 800-53 control for AC-2, Account Management. All ROSS accounts must be reviewed and approved by a Dispatch Center Manager, who follows established business processes to determine whether the request is appropriate and to define the functions that the user will need within the ROSS system.

8.2 Contractor Access

Will Department contractors have access to the system?

Fire NESS LDAP Services: Yes, Fire NESS contractors are able to access NESS and the hosted applications.

Child Applications: Fire NESS contractors have access to ROSS and e-ISuite. No contractors have access to ICBS.

8.3 Privacy Training

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

Fire NESS LDAP Services & Child Applications: All Federal Agency employees and FS contractors are required to take annual security awareness and privacy training in accordance with Federal requirements.

8.4 System Authority to Operate

Has Assessment & Authorization been completed for the system(s) supporting the program? If so, answer "Yes" and provide ATO expiration date(s).

Fire NESS LDAP Services & Child Applications: Fire NESS has an ATO signed in November 2017.

8.5 Audit and Technical Safeguards

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

Fire NESS LDAP Services & Child Applications: All NIST 800-53 auditing controls are provided by the host General Support System, Fire NESS.

8.6 Risk Mitigation

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?

Fire NESS LDAP Services & Child Applications: Privacy risks for account applicant data are minimal because the user account data is only available to the entity responsible for approving and creating the user accounts.

Privacy risks are minimal and are mitigated through the following measures.

1. All users must be identified and authenticated before accessing the systems. To obtain a Fire NESS user account, the user must request an account and have that request approved by their supervisor and the FAM ISSO. Application specific user accounts are approved in accordance with business processes specific to that application.

2. Once authenticated, access to the systems is through appropriate system roles. Roles are determined by based upon approved roles and responsibilities.

3. All user actions are attributed to that user name and documented in the system.

4. Rules of Behavior documents (e.g., FS-6600-6, -7, -8) must be reviewed and acknowledged by each user which identifies “ethics and conduct” for using the system.

5. All users must acknowledge the security warning banner that appears upon log on each time. There are criminal penalties for individuals who violate the Privacy Act.

6. All passwords are specifically encrypted by code before they are transferred across the network to the server. The traffic between the server and LDAP is encrypted using 256 bit strength encryption. The passwords are stored encrypted with AES 256 standard.

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 Description

What type of project is the program or system?

Fire NESS LDAP Services & Child applications: Fire NESS is a GSS providing primary computing platforms (IBM RIS), AIX, Intel (Linux, Windows), Storage Area Network (SAN), and Tape Backup Storage as well as network support. Fire NESS provides enterprise software licensing (e.g., WebSphere, Oracle, COGNOS, and ESRI GIS) for all applications hosted.

9.2 Privacy Concerns

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

No.

Section 10.0 Third Party Websites/Applications

The following questions are directed at critically analyzing the privacy impact of using third party websites and/or applications.

10.1 Review

Has the System Owner (SO) and/or Information Systems Security Program Manager (ISSPM) reviewed Office of Management and Budget (OMB) memorandums M-10-22 “Guidance for Online Use of Web Measurement and Customization Technology” and M-10-23 “Guidance for Agency Use of Third-Party Websites and Applications”?

Yes

10.2 Purpose

What is the specific purpose of the agency’s use of 3rd party websites and/or applications?

N/A

10.3 PII Availability

What Personally Identifiable Information (PII) will become available through the agency’s use of 3rd party websites and/or applications.

N/A

10.4 PII Usage

How will the PII that becomes available through the agency’s use of 3rd party websites and/or applications be used?

N/A

10.5 PII Maintenance and Security

How will the PII that becomes available through the agency’s use of 3rd party websites and/or applications be maintained and secured?

N/A

10.6 PII Purging

Is the PII that becomes available through the agency's use of 3rd party websites and/or applications purged periodically? If so, is it done automatically? If so, is it done on a recurring basis?

N/A

10.7 PII Access

Who will have access to PII that becomes available through the agency's use of 3rd party websites and/or applications?

N/A

10.8 PII Sharing

With whom will the PII that becomes available through the agency's use of 3rd party websites and/or applications be shared—either internally or externally?

N/A

10.9 SORN Requirement

Will the activities involving the PII that becomes available through the agency's use of 3rd party websites and/or applications require either the creation or modification of a system of records notice (SORN)?

N/A

10.10 Web Measurement and Customization

Does the system use web measurement and customization technology? If so, is the system and procedures reviewed annually to demonstrate compliance to OMB M-10-23?

N/A

10.11 Web Measurement and Customization Opt-In/Opt-Out

Does the system allow users to either decline to opt-in or decide to opt-out of all uses of web measurement and customization technology? If so, does the agency provide the public with alternatives for acquiring comparable information and services?

N/A

10.12 Risk Mitigation

Given the amount and type of PII that becomes available through the agency's use of 3rd party websites and/or applications, discuss the privacy risks identified and how they were mitigated.

N/A

Responsible Official

STEPHEN NELSON
Digitally signed by STEPHEN NELSON
Date: 2020.04.27 08:50:42 -06'00'

Stephen Nelson
System Owner (SO)
Natural Resources and Environment, Forest Service
United States Department of Agriculture

Approval Signature

CYNTHIA TOWERS
Digitally signed by CYNTHIA TOWERS
Date: 2020.04.30 14:10:22 -05'00'

Cynthia Towers
Privacy Officer (PO)
Natural Resources and Environment, Forest Service
United States Department of Agriculture

LAURA HILL
Digitally signed by LAURA HILL
Date: 2020.05.04 08:36:39 -06'00'

Laura Hill
Information System Security Program Manager (ISSPM)
Natural Resources and Environment, Forest Service
United States Department of Agriculture