Privacy Impact Assessment

for

Fire National Enterprise Support System (Fire NESS)

Policy, E-Government and Fair Information Practices

Version: 1.5

Date: March 27, 2023

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

Contact Point

Stephen Nelson

System Owner

USDA NRE Forest Service

208-387-5170

Reviewing Official

Cynthia Ebersohn (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

Fire National Enterprise Support Services (NESS) is a General Support System (GSS) designated a high value asset (HVA) that provides a common operating infrastructure to host a range of applications that support the US Forest Service Fire and Aviation Management (FAM) mission area. Many of the FAM applications are interagency in nature and support a wide range of users. Users include not only the Forest Service's wildland firefighting mission – but also the mission of other land management agencies (e.g., Department of Interior's Bureau of Land Management), as well as state and local entities, and commercial users.

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 on NESS managed hardware for Fire Applications hosted at USDA's Digital Infrastructure Services Center (DISC) in Kansas City, Missouri and at United States Geological Survey (USGS) Earth Resources Observation and Science (EROS) in Sioux Falls, South Dakota. Fire NESS also utilizes DISC PaaS offerings to provide Production, Training, and Development/QA environments for Fire Applications hosted on USDA managed hardware and OS layers at USDA's Digital Infrastructure Services Center (DISC) in Kansas City, Missouri.

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 consolidated Active Directory structure across all systems. 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.

FISMA Components

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.

The following components are hosted at EROS:

- 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.
    - Aviation Firefighting Use and Effectiveness (Retardant effectiveness) (AFUE) ○ Aviation Check (AvCheck) - Aviation Check for Aircraft and pilot carding
    - Fire Enterprise Geospatial Portal - (EGP) ○ FLIGHT - Air Tanker management
    - Wildfire Prevention Spatial Assessment and Planning Strategies (WPSAPS) ○ Shorthaul - Location and Availability of Park Service And Forest Service hoist lift for injured Fire Fighters
- 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, postfire mapping and assessment and related resource mapping/monitoring activities. Specific GTAC web applications in the Fire NESS currently include:
○ 7 Day Significant Fire Forecast (7DO) - Daily 7 day significant fire forecast/outlook geographic data and information products by Predictive Service Areas to inform decisions by regional and national fire managers on where/when to stage fire suppression resources. Application is owned by the National Predictive Services Program and operated by GTAC.

- GTAC Post-Fire Event Tracking Database - Contains data harvested from IRWIN and other relevant fire information pertinent to GTAC postfire tracking/mapping needs. Application is owned and operated by GTAC and will be soon migrated to the USGS EROS Science Data Infrastructure.
- Predictive Services Geospatial Portal - Access to geospatial data and mapping products that support daily Predictive Services Program business needs. Application is owned by the National Predictive Services Program and operated by GTAC.
- Active Fire Mapping (AFM) - Strategic scale, satellite-based active fire detection and mapping geospatial data, products, and services. Imagery and geospatial data and products are generated for regional/national wildfire managers to inform decisions regarding strategic planning and response to wildfire incidents, monitor the location, extent, and intensity current wildfire activity, and to provide wildfire mapping information to the general public. Data and products are generated for the interagency wildfire management community and general public and disseminated publicly. Application is owned and operated by GTAC.
- Rapid Assessment of Vegetation Condition after Wildfire (RAVG) - Pre/post-fire satellite imagery and geospatial data and mapping products that provide estimates of post-fire forest conditions on NFS lands and inform restoration prioritization and management decisions. Data and products are generated for FS Forest Management and other resource management staff areas and publicly disseminated. Application is owned and operated by GTAC. ○ Burned Area Emergency Response (BAER) Imagery Support - Pre/post event satellite imagery and vegetation and soil burn severity geospatial data and mapping products. Data and products are generated for FS BAER Teams and publicly disseminated. Application is owned and operated by GTAC.
- National Infrared Operations (NIROPS) - Infrared support ordering application and other content (documents, training, etc.) relevant to the interagency tactical fire mapping community. Application is owned and operated by GTAC. ○ Santa Ana Wildfire Threat Index (SAWTi) - Daily 6

day Santa Ana wind forecast/outlook geographic data and preparedness advisories for four southern California forecast zones. Application is owned by Southern California Geographic Area Predictive Services Program and operated by GTAC.

- 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.

The following components are hosted at DISC:

- 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. ○ Annual Wildfire Summary Report (AWSR) - Accessed through FAMWeb - State data, collect information about wildfire suppression efforts by State and local fire fighting agencies to ensure that Congress has adequate information to implement its oversight responsibilities and to provide accountability for expenditures and activities under the Act.
  - Aviation Management Information System (AMIS): Tracks aviation contracts and invoices for FS-owned aircraft. Due to be decommissioned.
  - Aviation Resource System (ARS): Used to collect, store, and analyze information about aviation resources. Due to be decommissioned.
  - FAMWEB Data Warehouse: An ORACLE database which stores historical data about wildland fire occurrence and weather. Originally populated with Forest Service data from 1970 to the present, the design permits entry of fire occurrence and weather data from earlier years for Forest Service units and weather data from other agencies.
- 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. ○ The Federal Excess Personal Property (FEPP) program refers to Forest Service-owned property that is on loan to State Foresters for the purpose of wildland and rural firefighting.
  - The Law Enforcement Support Office (LESO) has adopted the Federal Excess Property Management Information System (FEPMIS) as the automated property management system that will be used to provide accountability and management for property requisitioned through the Department of Defense (DoD) Defense Logistics Agency (DLA) Disposition Services 1033 Program.

- 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.
- National Application Portal (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 and 209.
    - SIT (Dispatch Side) Interagency Situation Report Program ○ 209 (Data form) Incident Status Summary ICS 209
- Operational Load Monitoring System (OLM) that collects flight information from tankers, etc.
- Weather Information Management System (WIMS): The host for the National Fire Danger Rating System (NFDRS) and helps manage information stored in the National Interagency Fire Management Integrated Database (NIFMID).
- National Advanced Fire and Resource Institute: Learning courses for Fire Incident Management
- National Wildfire Coordinating Group: The National Wildfire Coordinating Group provides national leadership to enable interoperable wildland fire operations among federal, state, local, tribal, and territorial partners.
- National Wildland Fire Training: Portal for Wildland Fire learning.
- Geographic Area Coordination Center: Used by the Geographic Area Coordination Centers to post fire information. Fire information includes Fire Team rosters, Team Rotations, Weather, Outlooks, and Preparedness Levels.
- Wildland Fire Management Research, Development & Application: The Wildland Fire Management Research, Development, and Application (WFM RD&A) program was created to promote application of wildland fire scientific knowledge; develop decision support tools; and provide science application services to the interagency wildland fire community.

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?

e-ISuite and ICBS applications collects and retains the following required information:

Last and first name

Address

Email

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

Other information that may be seen as personal (DOI ECI number)

1.2 Source

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

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. This includes ICBS. e-ISuite and ICBS 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.

1.3 Justification

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

All e-ISuite data is 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.

1.4 Collection

How is the information collected?

e-ISuite data are collected from the person themselves and entered by an authorized e-ISuite user.

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

1.5 Validation

How will the information be checked for accuracy?

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 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.

1.6 Authority

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

SORN - OPM GOVT-1

1.7 Risk Mitigation

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

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 via two factor (PIV or Password) 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 username 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.

Section 2.0 Uses of the Information

The following questions are intended to clearly delineate 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. DOI Federal Personnel Payment System: At the close of an incident, e-ISuite Site data is provided to the incident host agency and transferred to eISuite Enterprise.

B. 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.

C. 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.

D. 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.

2.2 Analysis and Production

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

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 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

Not applicable

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.

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?

Because Fire NESS and Component application data deals with wildland fire incidents, information is retained indefinitely per Forest Service requirements.

File Code 5180 - Permanent

3.2 Approval

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

Yes

3.3 Risk Mitigation

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

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?

Not Applicable

4.2 Delivery and Disclosure

How is the information transmitted or disclosed?

Not Applicable

4.3 Risk Mitigation

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

Not Applicable

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?

DOI Federal Personnel Payment System: At the close of an incident, e-ISuite Site data is provided to the incident host agency and transferred to e-ISuite Enterprise.

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.

e-ISuite's and ICBS's PII data is covered by SORN OPM GOVT-1. Per this SORN all categories of records may include identifying information, such as name(s), date of birth, home address, mailing address, social security number, and home telephone. Fire NESS does not collect SSN, however, all other data elements are collected.

5.3 Delivery and Security Measures

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

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

5.4 Risk Mitigation

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

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 that covers the PII retained by Fire NESS, OPM GOVT-1.

6.2 Individual Notification

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

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

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

6.3 Right to Decline

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

Yes, an individual resource can decline to submit all required information; however, doing so 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?

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 eISuite.

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

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.

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.

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?

Individuals wishing to request access to their records should contact the appropriate OPM or agency office, as specified in the Notification Procedure section. Individuals must furnish the following information for their records to be located and identified: a. Full name(s). b. Date of birth. c. Social security number. d. Last employing agency (including duty station) and approximate date(s) of employment (for former Federal employees). e. Signature. Individuals requesting access must also comply with the Office's Privacy Act regulations on verification of identity and access to records (5 CFR part 297).

7.2 Correction

What are the procedures for correcting inaccurate or erroneous information?

Current employees wishing to request amendment of their records should contact their current agency. Former employees should contact the system manager. Individuals must furnish the following information for their records to be located and identified. a. Full name(s). b. Date of birth. c. Social security number. d. Last employing agency (including duty station) and approximate date(s) of employment (for former Federal employees). e. Signature. Individuals requesting amendment must also comply with the Office's Privacy Act regulations on verification of identity and amendment of records (5 CFR part 297).

7.3 Notification

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

Individuals wishing to inquire whether this system of records contains information about them should contact the appropriate OPM or employing agency office, as follows: a. Current Federal employees should contact the

Personnel Officer or other responsible official (as designated by the employing agency), of the local agency installation at which employed regarding records in this system. b. Former Federal employees who want access to their Official Personnel Folders (OPF) should contact the National Personnel Records Center (Civilian), 111 Winnebago Street, St. Louis, Missouri 63118, regarding the records in this system. For other records covered by the system notice, individuals should contact their former employing agency. Individuals must furnish the following information for their records to be located and identified: a. Full name. b. Date of birth. c. Social security number. d. Last employing agency (including duty station) and approximate date(s) of the employment (for former Federal employees).

7.4 Redress Alternatives

Current employees wishing to request amendment of their records should contact their current agency. Former employees should contact the system manager. Individuals must furnish the following information for their records to be located and identified. a. Full name(s). b. Date of birth. c. Social security number. d. Last employing agency (including duty station) and approximate date(s) of employment (for former Federal employees). e. Signature. Individuals requesting amendment must also comply with the Office's Privacy Act regulations on verification of identity and amendment of records (5 CFR part 297).

7.5 Risk Mitigation

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

Paper or microfiche/microfilmed records are located in locked metal file cabinets or in secured rooms with access limited to those personnel whose official duties require access. Access to computerized records is limited, through use of user logins and passwords, access codes, and entry logs, to those whose official duties require access. Computerized records systems are consistent with the requirements of the Federal Information Security Management Act (Pub. L. 107-296), and associated OMB policies, standards and guidance from the National Institute of Standards and Technology.

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 only has privileged users (administrators) at the GSS level. All administrators are privileged users. All privileged users are granted access to the system utilizing multi-factor authentication and decentralized authorization access. They must first gain access utilizing multifactor authentication through the external VPN and once inside, they authenticate separately to each resource, using an individual username and password. Non-privileged users only exist on the application that reside on Fire NESS that are within this boundary. There are no non-privileged users at the GSS level. Non-privileged users must also first gain access utilizing multifactor authentication through the external VPN and once inside, they authenticate separately to each resource that they have permissions to access, using FAM Auth (two factor authentication) or an individual username and password. All Fire NESS GSS users must be explicitly authorized prior to being granted access and must follow the process described in the implementation statement for AC-2. The process for obtaining a Fire NESS GSS account is summarized below. To obtain a Fire NESS GSS account, all users must meet three prerequisites:

1. Take annual security awareness training and privacy training;
2. Sign the Fire Rules of Behavior (ROB) for privileged users; and
3. Complete an appropriate background investigation or be on a waiver letter that has been submitted to the FS CIO.

Concurrent with completing the prerequisites, a Fire NESS user must request access to the Pulse Secure, as well as to the Fire NESS environment. Pulse allows authorized Federal users with HSPD-12 cards to access the Fire NESS environment. To obtain a Pulse account, the FS employee's supervisor, contractor's COTR, or FAM IM PM must request access to the NESS PM via email along with completed account User Access Request (UAR) forms and supporting 6500 for with current ROB. Account requests are reviewed by the NESS PM and submitted to the Fire IT Branch Chief and then to the FAM ISSO. The ISSO then reviews the request; if approved, the Authorized Fire-IT Agency Role Membership Manager (ARRM) creates the Pulse account. The ARRM creates the account, sends an encrypted account-created notification email directly to the user along with instructions for initial access and login. The account is not usable until the next level USDA Pulse Administrator 'provisions' the account and associates the user's HPDS-12 card with the FedID and PersonalGuid.

For DISC and USGS-EROS, all access originates through the Network Access Gateway, a Pulse VPN device unique to each installation. When the user receives the web page, the user is challenged for a username and password, and a selection for the type of multi-factor that user is assigned. For PIV Access, the user's primary credentials and HSPD-12 FED ID number are reviewed to determine if they match the current records in USDA Active Directory; if so, the user is presented with a PIN entry box. If not, the user is presented with an error message.

Once the user is granted access to the VPN, they are presented with a web page with a number of choices. From this web page they may navigate to any system for which they have been granted authorization separately. This access is not managed centrally but is instead individualized to the machine or service they have a need to use. Each environment maintains a Microsoft Active Directory to authenticate Microsoft accounts; some Linux accounts are also managed within the MS AD LDAP. Each machine is accessed by a username and password. This is the same for both the USDA-DISC and USGS-EROS environments.
The Fire NESS Windows machines and all Linux systems are incorporated into an Active Directory management system and they are managed via Microsoft's AD tools.
If the user also requires elevated privileges on Fire NESS (SUDO or DBA access) some Linux machines, he or she must also complete the User Elevated Access Request Form (Appendix B of the Access Control and Account Management document) and provide a justification for requiring elevated access. The Supervisor/COTR, Fire NESS PM, and the ISSO must sign this form. The ISSO then requests that System Administration contractors provide elevated access. The system level accounts are granted levels of permissions or access to the SUDO or DBA groups. SUDO allows an authorized user to execute explicitlyauthorized individual commands as specified by the Fire NESS administrators. All SUDO users must authenticate themselves with their user identifier and user password. This ensures that all actions are traceable to a specific user (e.g., timestamps updated).
ICBS/eISuite: All ICBS, WIMS, eISuite application users must be explicitly authorized via established and formal account management process. All ICBS and eISuite users must first obtain a Fire National Enterprise Support Services (NESS) Application Portal (NAP) account. To obtain a NAP account, users must use the online request form via the NAP (http://nap.nwcg.gov/NAP/).

eISuite: The online request form is routed to a NAP Account Manager, who reviews the request. Accounts for privileged access to the e-ISuite Enterprise Application are validated by the NAP Account Manager by contacting the Approving Official listed on the NAP Account request. Accounts for non-privileged (standard) access to the e-ISuite Enterprise Application are validated by the Incident Interagency (IIA) Helpdesk, who contacts the Approving Official listed on the NAP Account request. Once the account has been validated, the IIA Helpdesk notifies the NAP Account Manager. The NAP Account Manager then creates the user account in NAP and links the user to the e-ISuite Enterprise application (note: this action does not give the user the ability to do anything within the e-ISuite application). The NAP automatically generates the user name, creates the user account, and assigns the account access to the e-ISuite application. The NAP also sends an email to the requesting user notifying them of account creation. An eISuite Application Account Manager then imports the user account into the e-ISuite Enterprise application and assigns roles for access to the application as approved by the user's Home Unit.

ICBS: The online request form is routed to a NAP Account Manager, who reviews the request and contacts the ICBS Cache Manager. The ICBS Cache Manager validates the user's credentials and need to access the ICBS application.

Once creation of the account is approved, the ICBS Cache Manager, notifies the NAP Account Manager, authorizing creation of the requested user account. The NAP Account Manager then creates the user account in NAP and links the user to the ICBS application (note: this action does not give the user the ability to do anything within the ICBS application). The NAP automatically generates the user name, creates the user account, and assigns the account access to the ICBS application. The NAP also sends an email to the requesting user and ICBS Cache Manager notifying them of account creation. The Dispatch Center manager then assigns ICBS application roles.

8.2 Contractor Access

Will Department contractors have access to the system?

Component Applications: Fire NESS contractors have access to 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?

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 has an ATO signed in April 2022.

8.5 Audit and Technical Safeguards

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

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?

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. The passwords are stored encrypted.

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 is a GSS providing primary computing platforms (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-1023?

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

Approval Signature

_____

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

_____

Benjamin Moreau
Assistant Chief Information Security Officer (ACISO) Natural Resources and Environment, Forest Service
United States Department of Agriculture