

DEFENSE LOGISTICS AGENCY

Established 1961



New Login.gov, iNAP and FEPMIS User Guide



THE NATION'S LOGISTICS COMBAT SUPPORT AGENCY



1. Setting up LOGIN.GOV user account:

- a. Go to: <https://famauth.wildfire.gov/>

Note: This will be your access point for LESO FEPMIS from now on so you can bookmark this page.

- b. Select Public Partners (Login.gov)

To login to your Wildland Fire Application please select one of the two tiles, Login.gov or eAuthentication.

Public partners LOGIN.GOV

Login.gov is a service that offers secure and private online access to government programs through a Private Non-Federal account.

Government eAuth

eAuthentication is the system that allows users access to Wildland Fire Apps and Services using government clearance.

Upon logging in, you agree to the following information:

Unauthorized access to this United States Government Computer System and software is prohibited by Title 18, United States Code 1030.

This statute states that: Whoever knowingly, or intentionally accesses a computer without authorization or exceeds authorized access, and by means of such conduct, obtains, alters, damages, destroys, or discloses information or prevents authorized use of (data or a computer owned by or operated for) the Government of the United States shall be punished by a fine under this title or imprisonment for not more than 10 years, or both.

All activities on this system and network may be monitored, intercepted, recorded, read, copied, or captured in any manner and disclosed in any manner by authorized personnel. THERE IS NO RIGHT OF PRIVACY ON THIS SYSTEM. System personnel may give to law enforcement officials any potential evidence of crimes found on this USDA computer system.

USE OF THIS SYSTEM BY ANY USER, AUTHORIZED OR UNAUTHORIZED, CONSTITUTES CONSENT TO THIS MONITORING.

User notices

Application
FEMS

FEMS

Provisional Data Sets (8/10/2023)

Provisional data sets are being used, operational decisions should be made with caution.

Note: If you have an existing Login.gov account then sign into your existing account.

New Login.gov, iNAP and FEPMIS User Guide

Login.gov Setup



National Fire & Aviation Management is using Login.gov to allow you to sign in to your account safely and securely.

Email address

Password

Show password

Sign in

Create an account

[Sign in with your government employee ID](#)

[Back to National Fire & Aviation Management](#)

[Forgot your password?](#)

[Security Practices and Privacy Act Statement](#) [↗](#)

[Privacy Act Statement](#) [↗](#)

- c. Create a Login.gov account by selecting Create an Account



A DEMO website of the United States government. [Here's how you know](#)

LOGIN.GOV Government Agency Name Placeholder

Create your account

Enter your email address

Select your email language preference

Login.gov allows you to receive your email communication in English, Spanish or French.

English (default)

Español

Français

Check this box to accept the Login.gov [Rules of Use](#)

Submit

[Cancel](#)

[Security Practices and Privacy Act Statement](#)

[Privacy Act Statement](#)

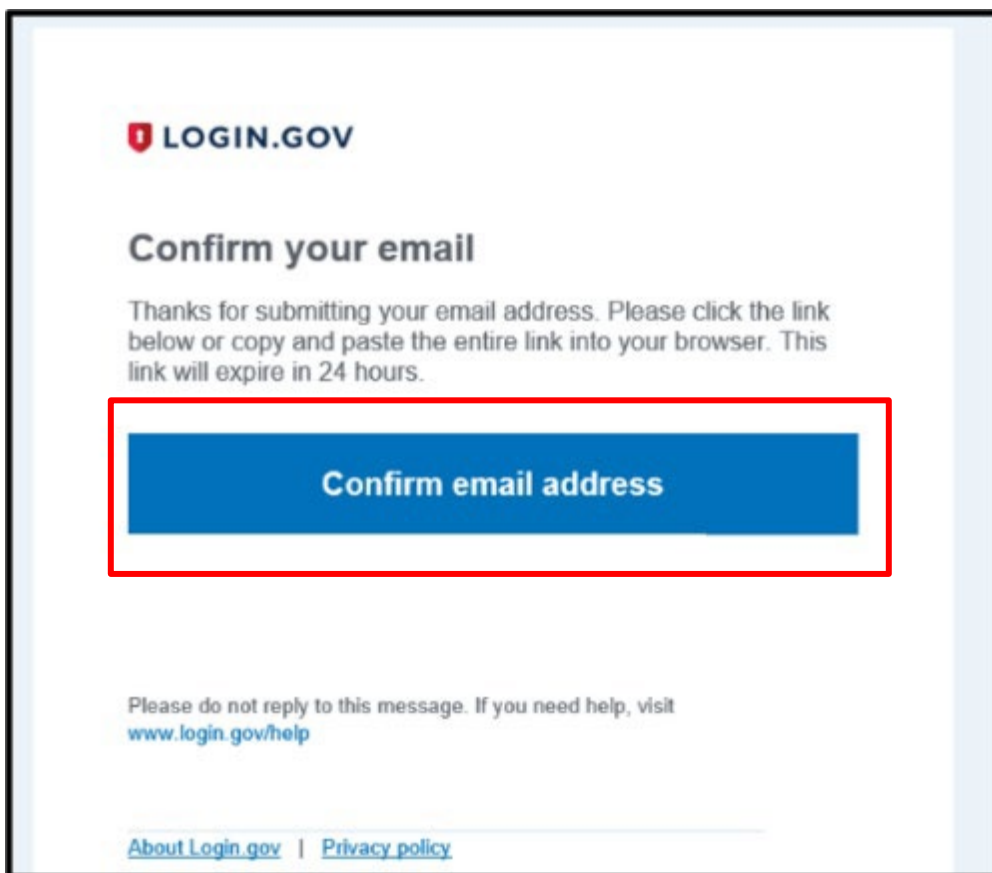
d. Enter your email address.

Note: We recommend using your personal email address to avoid issues with your organization blocking emails from login.gov.

e. Select your language.

f. Check the 'Rules of Use' box.

g. Select 'Submit'



Note: An email will be sent to the email address entered in step 4. Note: Ensure all your browsers are closed before proceeding.

h. Confirm Email

- i. Go to your email account.
- ii. Find the email from login.gov.
- iii. Click on the 'Confirm email address' link within the email that you received.



- i. Create a strong password.

Note: Password must contain at least 12 characters with a good or better strength rating (3 green bars) in order to continue. REMEMBER YOUR PASSWORD

Note: Your password will not expire unless you change it. If you email address is invalid or not working any more than it would affect your account with login.gov because you wouldn't have a valid email.

- j. Select 'Continue'



Authentication method setup

Add a second layer of security so only you can sign in to your account.

Keep this information safe. You will be locked out and have to create a new account if you lose your authentication method.

Select an option to secure your account:

- Security key
Use a security key (you have a physical device that you plug in to your computer or phone (it often looks like a USB drive). Recommended for users who are security resistant. **MORE SECURE**
- Government ID card
Insert your government ID card (CAC or CAC card) and enter your PIN. **MORE SECURE**
- Authentication app
Get codes from an app on your computer, or tablet. Recommended for users who want to manage. **MORE SECURE**
- Text or Voice Message
Get security codes by text message (SMS) or phone call. Please do not use web-based (VOIP) phone services. **LESS SECURE**
- Smart card
Use a smart card (you have a physical card that you insert into a reader). Recommended for users who are security resistant. **MORE SECURE**

Continue

k. Select your 2nd level authentication method: 'TEXT or VOICE MESSAGE'

- We recommend using TEXT if possible.
- Do not use web based VOIP phones.

Note: If you choose to use a different authentication method, we cannot provide any further guidance for you.


- You will be required to use this 2nd level of authentication each time you log into LESO FEPMIS.

l. Select 'Continue'



A DEMO website of the United States government. [Here's how you know](#)

LOGIN.GOV Government Agency Name Placeholder



Send your security code via text message (SMS) or phone call

We'll send you a security code **each time you sign in.**

Message and data rates may apply. Please do not use web-based (VOIP) phone services.

Phone number
Example: (201) 555-0123

How should we send you a code?

You can change this selection the next time you sign in. If you entered a landline, please select "Phone call" below.

Text message (SMS) Phone call

[Mobile terms of service](#)

[Choose another option](#)

m. Phone Authentication

- i. Login.gov will send you a security code each time you sign in, so ensure you use a phone number you have access to
- ii. Message and data rates may apply. Do Not use a web based VOIP phone service.

n. Enter your phone number.

o. Select Text Message or Phone Call 'We recommend text.'

p. Select send code.

Note: The Code Will Expire in 10 Minutes.



Enter your security code

We sent a security code to + [REDACTED] This code will expire in 10 minutes.

One-time security code

M5YVE3

Remember this browser

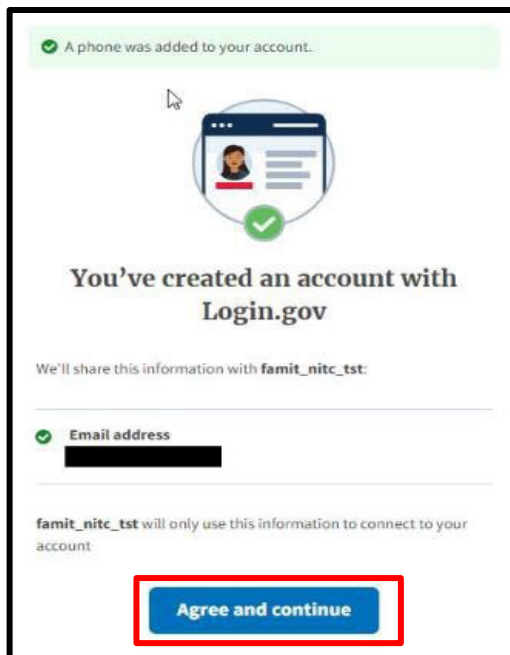
Submit

[Get another code](#)

Entered the wrong phone number? [Use another phone number](#)

[Choose another option](#)

- q. Enter your one-time security code that you received either text or call (**this security code will be sent to your phone each time you log in**)
- r. Uncheck 'Remember this Browser.'
- s. Select Submit



Note: You should see a confirmation from login.gov like this 'A phone was added to your account' and the email address associated with your login.gov account.

t. Select Agree and Continue

Note: You have successfully created a login.gov account and you will be returned to Wildland Fire Application Portal.

Note: You must now create an iNAP account. Please Continue.



Wildland Fire Application Portal

FAMAUTH QA VERSION, USE ONLY FOR TESTING
Production link: <https://famauth.wildfire.gov/>

To login to your Wildland Fire Application please select one of the two tiles, Login.gov or eAuthentication:

Public partners **LOGIN.GOV**
Login.gov is a service that offers secure and private online access to government programs through a Private Non-Federal account.

Government **eAuth**
eAuthentication is the system that allows users access to Wildland Fire Apps and Services using government clearance.

⚠ Upon logging in, you agree to the following information:
Unauthorized access to this United States Government Computer System and software is prohibited by Title 18, United States Code 1030.
This statute states that: Whoever knowingly, or intentionally accesses a computer without authorization or exceeds authorized access, and by means of such conduct, obtains, alters, damages, destroys, or discloses information or prevents authorized use of (data or a computer owned by or operated for) the Government of the United States shall be punished by a fine under this title or imprisonment for not more than 10 years, or both.
All activities on this system and network may be monitored, intercepted, recorded, read, copied, or captured in any manner and disclosed in any manner by authorized personnel. THERE IS NO RIGHT OF PRIVACY ON THIS SYSTEM. System personnel may give to law enforcement officials any potential evidence of crimes found on this USDA computer system.

User notices
No notices today.

u. Select 'Login.gov'



Portal FAMAuth admin

▼	▼	WFMI	▼
ICBS Interagency Cache Business System	IETDSS/FTEM Interagency Fuel Treatment Decision Support System/Fuel Treatment...	IgPoint Fire Ignition Points Website	InciWeb InciWeb Incident Information System
IQCS Incident Qualifications and Certification System	IROC IROC Interagency Resource Ordering Capability	LESO FEPMIS Law Enforcement Support Office Federal Excess Property Management...	NIFCSSO NIFC Single Sign-On
NIROPS National Infrared Operations Website	NPSG National 7-Day Significant Fire Potential	OIS Organization Information System	OLMS Operational Loads Monitoring System

- v. On the Wildland Fire Application Portal Dashboard page, find the LESO FEPMIS Tile and select 'Access'.



w. Select 'Request access'

An official website of the United States government [Here's how you know](#) ▼

USDA U.S. FOREST SERVICE
FIRE AND AVIATION MANAGEMENT -
INFORMATION MANAGEMENT (FAM-IM) Wildland Fire Application Portal – FAMAAuth

Link user

ⓘ We are unable to find a FAMAAuth user linked with your Login.gov account.
If you have a FAMAAuth user (previously known as iNAP profile) already, enter the primary or an alternate e-mail address associated with your user.
If you are a new user, you may **request access**.

E-mail address

Next



- x. Enter user information, All Fields are required unless noted as “Optional.”

Note: Ensure your email address matches in both E-Mail boxes (E-Mail box and the E-Mail Confirm box).

- y. Enter Primary Affiliation ‘DoD Government’
- z. Enter ‘Other’ and ‘LESO’ for Organizational Unit
- aa. Enter ‘Other’ and your current agency for Agency.
- bb. Select ‘Next’

An official website of the United States government. Here's how you know

USDA U.S. FOREST SERVICE TREE HEALTH ACTION MANAGEMENT INFORMATION MANAGEMENT (TAM-IM)

iNAP Integrated National Application Portal

Request access

Enter user information

Please enter your full name as it appears on your Government ID.

First name Middle name (optional) Last name

Job title (optional)

E-Mail

E-Mail confirm New Field

Office number Ext (optional) Mobile (optional) Fax (optional)

Primary affiliation

Part-time/seasonal

Next Cancel

Primary affiliation

DOD Government

Part-time/seasonal

Organizational unit

Search Organizations Enter the organizational unit you are employed by. You may enter all or part of the name. For example: Pacific Ranger District or Pacific or Ranger District.

Other (not listed)

Other organizational unit

LESO

Agency

Agency in this context is a general term for agency, department, interagency, state, county, city or tribe

Other (not listed)

Other agency

Your Agency

Next Cancel

New Login.gov, iNAP and FEPMIS User Guide

iNAP Setup



U.S. FOREST SERVICE
FIRE AND APPOINTMENT MANAGEMENT
INFORMATION MANAGEMENT SYSTEM

iNAP Integrated National Application Portal

Review and accept rules of behavior

In compliance with USDA and federal security policies, you must accept the following rules of behavior annually, prior to being granted access to iNAP/FAH applications. Please read and confirm your acceptance before proceeding.

Statement of Information Security Responsibilities for Associate Forest Service Users of FS Systems

I acknowledge that I understand and agree to comply with Forest Service (FS) and USDA information security policies and procedures, as well as with federal, state, and local laws. I understand that as an FS associate, I may not be entitled to the same limited personal use privileges as FS employees, and that my use of FS information systems and equipment is limited to that which is specifically described in my contract or other agreement with the FS.

I understand that my contract or other agreement may specify additional information security responsibilities or requirements, such as the need for a signed confidentiality statement. Key statements of Forest Service Manual (FSM) Chapter 6680, Security of Information, Information Systems, and Information Technology (both 6680-6682 and 6680-6683), for which I am responsible, are summarized below. I understand and agree that I must periodically review the FSM Chapter 6680 for changes.

I am also responsible to:

- Take appropriate measures to protect information from unauthorized access, including seeking out and applying security measures to protect sensitive information stored on my computer, on other electronic devices, or on other media such as CDs, DVDs, magnetic tape, and paper.
- Not store any classified information on any computer.
- Encrypt, using agency authorized encryption methods, any government sensitive or confidential information or information subject to the Privacy Act that is stored on any personal electronic device or removable storage medium.
- Sign off or electronically lock the computer before leaving it unattended.
- Comply with physical security standards and procedures, including taking appropriate measures to protect computer equipment and other electronic devices from theft, damage, or unauthorized use.
- Comply with password standards and procedures specified in the FSM and USDA's password policy.
- Verify that automatic virus protection is enabled on the computer in use (e.g., Symantec).
- Ensure if I am working remotely (those who operate portable computer systems in an alternate workplace, e.g., cell phone, PDA (BlackBerry), or home computers), I take the same precautions as required of users of stationary systems located at FS facilities to protect the FS system's hardware, software, and information.
- Ensure that Agency sensitive information to which I have access is securely maintained, disseminated, and protected from disclosure, release, or extraction to unauthorized individuals or groups. In the instance of information protected by specific laws, such as the Privacy Act or the Health Insurance Privacy and Portability Act (HIPPIA), users must be aware of the confidentiality protection procedures required of them in their handling of Agency sensitive data as required by law.
- Being aware of retention and disposal requirements of data to which I have access privileges.
- Promptly report all suspected security incidents to the FS Computer Incident Response Team (CIRT@fs.fed.us) and/or my supervisor or other appropriate management officials.

I understand findings of culpability will result in disciplinary action consistent with the provisions of FSM 6170 and USDA's DPM 751, which may include the loss of use or limitations on use of equipment, disciplinary or adverse action, criminal penalties, and/or financial liability for the cost of improper use. If I have an FS issued computer, I am also responsible to:

- Store corporate data within the corporate filing system, where it is backed up routinely. The FS defines corporate data as information owned, collected, maintained, or generated by the enterprise that has inherent value to and is intended for consistent, shared use within the enterprise.
- Install only that software for which I have obtained authorization, and when my privileges are elevated to allow installation of authorized software to perform only those activities that are specifically authorized.
- Refrain from installing on FS computer equipment any software, including "freeware" and "shareware," that does not have technical approval from the Chief Information Office.
- Verify that the automatic virus definition file updates to the enterprise antivirus tool (currently, Symantec AntiVirus) occur as scheduled.
- Be aware of the proper procedures for the sanitization and disposal of Agency information and data. Users shall be aware that data can be retrieved from media (diskettes, tapes, hard drives, or other memory devices) even after being erased or deleted. To properly sanitize media of residual data, users must contact the Forest Service Help Desk for assistance in degaussing, overwriting, or otherwise erasing media as pruned prior to disposal.
- Not remove hardware containing Agency sensitive information from FS without following appropriate media protection (encryption) or sanitization and disposal (overwriting, degaussing) procedures.
- Take FS computer equipment from an FS facility only for official business purposes.
- Only use computer equipment for which I have authorization.
- Not install computer equipment unless I am an authorized technician and the action has been approved by the appropriate IT System Owner or supervisor.
- Ensure if I am working remotely to follow the remote access requirements, which may include two-factor authentication and additional restrictions on portable computer systems to ensure these devices do not compromise the integrity or confidentiality of FS information or data.
- Not change the configuration settings or attempt to modify or disable any of the security programs installed on their FS information system, including virus protection software and the password protected screen saver.
- Ensure all software in use by a user on FS equipment must have a valid license on file with purchasing.

Personally Identifiable Information (PII) is any piece of information that can potentially be used to uniquely identify, contact, locate, or impersonate a single person. If I have access to PII, I am responsible to:

- Never access PII unless absolutely necessary to perform my job.
- Never disclose PII to another person within FS unless they have verified that the other person is entitled to the information.
- Never remove PII from FS premises unless it is encrypted using a FS approved method unless they have a copy of a memorandum waiving the encryption requirement that has been signed by a Business Unit Manager and that applies to this circumstance.
- Verify that any time I extract any PII from an IT system into a computer readable form, e.g., into a spreadsheet or report, that this act has been properly logged so that the location of the PII may be tracked.
- Ensure that after having finished using any extracted PII, or after 90 days, whichever comes first, I will erase the PII or receive written permission from my supervisor to retain it for longer.
- Ensure when erasing PII, that this act is properly logged so that the location of the PII will no longer be tracked.
- Never access PII from computers or devices outside of FS premises without advance authorization for remote access.
- Never attempt remote access without using approved FS access methods, which generally require the use of a SecurID device (called a "token").
- Never show their token with or near a laptop or other portable computer that contains PII or is used for PII access.
- Never mark their token with any information such as name or password.
- Promptly report any possible, suspected, or actual loss of PII or any device containing PII to the appropriate point of contact. Hence, I must ensure that I know how to make a report, and that I keep a record of the reporting point of contact separately from any device, so that a report is made if the device is missing.
- Report any possible, suspected, or actual loss of PII or any device containing PII within 15 minutes of discovery of the incident, regardless of the time of day.
- Physically secure all portable devices containing PII. I will lock up laptops using a cable lock when they are not in use, including when they are within their home, vehicle, or motor home. I will lock small devices into secure containers when they are not in their possession.
- Encrypt PII when it is placed onto removable media such as CDs, "thumb drives," or memory sticks, and when it is removed from agency premises.
- Ensure that if PII is lost or stolen, it is reported to the Forest Service Help Desk within 24 hours.

I understand that any use of FS communications resources generally is not secure, that it is not private, and that it is not anonymous, and that system managers do employ monitoring tools to detect improper use. I understand that there is no right to privacy when using government information systems (often wearing "cameras").

[Return to top](#)

Wildland Fire NIFC NWCG Privacy Disclaimer Accessibility IAA Helpdesk 866-224-7677

cc. Review/Read and Accept Rules of Behavior (RoB) and select Accept

NOTE: RoB must be accepted to submit a request for access. If you decline the RoB you will not be allowed to proceed.



dd. Verify the requested application access and roles.

- i. Application Access: LESO-Law Enforcement Support Office
- ii. Instance: PRODUCTION
- iii. Request application role for LESO-PROD (Standard)
- iv. LESO Report Reader (default) is checked.

Request application access and roles

ⓘ Requesting application access will result in a request to iNAP. To request access to more than 1 application, please click the plus button below. Once your request is reviewed, you will receive an e-mail. Please do not submit further requests until you receive this e-mail.

Application access	Instance(s)
LESO-Law Enforcement Support Office	PRODUCTION

Request application roles for LESO - PROD (Standard)

<input checked="" type="checkbox"/> LESO Report Reader (default)
<input type="checkbox"/> LESO Report Writer



① Enter the contact who can validate your need to access this application.

- You CAN NOT validate yourself.
- Agency employees: enter manager or supervisor.
- Contractors: enter your government contracting office personnel.

Contact's first name

Contact's last name

Job title

Phone number

Ext (optional)

E-Mail

Submit

Cancel

ee. Enter contact information.

- State Coordinators enter your LESO East/West Lead
- Law Enforcement Agencies enter your State Point of Contact information.

ff. Select 'Submit'



An official website of the United States government [Here's how you know](#)

USDA U.S. FOREST SERVICE
FIRE AND AVIATION MANAGEMENT -
INFORMATION MANAGEMENT (FAM-IM) **iNAP** Integrated National Application Portal

Confirm additional access

Do you want to request access to another application?

If so, select Yes to return to the request form and use the + button to request additional application(s).

Yes No, submit my request

gg. Select 'No, Submit my request.'

Leaving iNAP

✓ Your application access request(s) have been submitted to iNAP. You will receive an e-mail when your application access request(s) is processed.

⚠ For increased security, please close your browser window.

Note: You will see this page display. You have successfully connected your new login.gov account to your new iNAP account.

Note: STOP HERE, close your browser, and wait until the LESO HQ approves your account. Once approved you will receive 2 emails. After you receive the emails, you will be able to proceed.



From: donotreply@mail.nwcg.gov <donotreply@mail.nwcg.gov>

Sent: Thursday, November 19, 2020 12:32:59 PM

To: [REDACTED]

Subject: iNAP User Account Information

The user name for your standard iNAP User Account has been set to: flast

After you receive your user name and password, you may need to contact the application steward for the specific application you need access to. The Steward will establish your user roles for that application if required.

This is an automatically generated message. Please do not reply to this message.

<https://nap.nwcg.gov/NAP/>

From: donotreply@mail.nwcg.gov <donotreply@mail.nwcg.gov>

Sent: Thursday, November 19, 2020 12:32:59 PM

To: [REDACTED]

Subject: Application Access for LESO-TEST Approved

Your access request for LESO-TEST is approved.

This is an automatically generated message. Please do not reply to this message.

<https://nap.nwcg.gov/NAP/>

- hh. Upon confirmation and approval of your iNAP request by the approving official you will receive multiple email messages from donotreply@nwcg.gov
 - ii. Up to 2 emails could be sent.
 - i. iNAP User Account Information.
 - ii. Application Access for LESO-PROD Approved.

You have successfully connected your iNAP and LOGIN.gov accounts. This is a onetime process.

You must wait to receive email confirmation that your iNAP account has been approved to proceed.

The next time you attempt to login to LESO FEPMIS you will be Authenticated by login.gov two level authentication and authorized by iNAP and then be redirected into LESO FEPMIS.

Note: You must completely CLOSE YOUR BROWSER down. To access LESO FEPMIS on your next login attempt go to <https://famauth.wildfire.gov/>.



- a. Go to: <https://famauth.wildfire.gov/>
- b. Select Public Partners 'Login.gov'

The screenshot shows the Wildland Fire Application Portal login page. At the top, there is a navigation bar with the USDA and U.S. Forest Service logos, and the text "Wildland Fire Application Portal". Below the navigation bar, there is a banner image of a wildfire. The main content area contains a message: "To login to your Wildland Fire Application please select one of the two tiles, Login.gov or eAuthentication:". There are two tiles: "Public partners LOGIN.GOV" and "Government eAuth". The "Public partners LOGIN.GOV" tile is highlighted with a red border. Below the tiles, there is a yellow box with a warning icon and the text: "Upon logging in, you agree to the following information:". To the right, there is a "User notices" section with a dropdown menu for "Application" set to "FEMS" and a section for "Provisional Data Sets (8/10/2023)".



An official website of the United States government [Here's how you know](#)

LOGIN.GOV

National Fire & Aviation Management is using Login.gov to allow you to sign in to your account safely and securely.

Email address

Password Show password

[Sign in with your government employee ID](#)

[Back to National Fire & Aviation Management](#)

[Forgot your password?](#)

[Security Practices and Privacy Act Statement](#)

[Privacy Act Statement](#)

Note: If you have not created a login.gov account yet stop and go to step 1 to create an account.

c. Enter your login.gov email address.

d. Enter your login.gov password.

e. Select 'Sign in'

Note: A new one-time security code will be sent to your phone, this is your 2nd level of authentication.



Enter your security code

We sent a security code to [REDACTED]. This code will expire in 10 minutes.

One-time security code

ZSNH4J

remember this browser

Submit

[Get another code](#)

Don't have access to your phone right now?

[Choose another authentication method](#)

[Cancel](#)

- f. Enter one-time security code sent to your phone **(this security code will be sent to your phone each time you log in)**
- g. Uncheck 'Remember this browser.'
- h. Select 'Submit'




- i. On the Wildland Fire Application Portal page, Find the LESO FEPMIS Tile and select 'Access'.

To access your Wildland Fire Application select one of the tiles below:

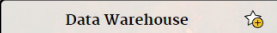

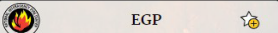
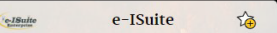
View as Logos Tiles

My production applications

 LESO FEPMIS

My training applications

Wildland fire applications

 Data Warehouse	 DRONESIM	 EGP	 e-ISuite
Data Warehouse	UAS Training, Flight Simulator	Enterprise Geospatial Portal	e-ISuite Enterprise

User

Applica
FEMS

FEMS

Provis

Provis
shoul



location of the PII may be tracked.

- Ensure that after having finished using any extracted PII, or after 90 days, whichever comes first, I will erase the PII or receive written permission from my supervisor to retain it for longer.
- Ensure when erasing PII, that this act is properly logged so that the location of the PII will no longer be tracked.
- Never access PII from computers or devices outside of FS premises without advance authorization for remote access.
- Never attempt remote access without using approved FS access methods, which generally require the use of a SecurID device (called a "token").
- Never store their token with or near a laptop or other portable computer that contains PII or is used for PII access.
- Never mark their token with any information such as name or password.
- Promptly report any possible, suspected, or actual loss of PII or any device containing PII to the appropriate point of contact. Hence, I must ensure that I know how to make a report, and that I keep a record of the reporting point of contact separately from any device, so that a report is made if the device is missing.
- Report any possible, suspected, or actual loss of PII or any device containing PII within 15 minutes of discovery of the incident, regardless of the time of day.
- Physically secure all portable devices containing PII. I will lock up laptops using a cable lock when they are not in use, including when they are within their home, vehicle, or hotel room. I will lock small devices into secure containers when they are not in their possession.
- Encrypt PII when it is placed onto removable media such as CDs, "thumb drives," or memory sticks, and when it is removed from agency premises.
- Ensure that if PII is lost or stolen, it is reported to the Forest Service Help Desk within 24 hours.

I understand that any use of FS communications resources generally is not secure, that it is not private, and that it is not anonymous, and that system managers do employ monitoring tools to detect improper use. I understand that there is no right to privacy when using government information systems (login warning banner)

Note: If the Rules of Behavior screen does not show go to step (t.)

j. Read and Select 'Accept' the Rules of Behavior.

Note: You will receive a message on the screen that you are leaving iNAP.

Note: Unfortunately, due to security issues you will have to log back in after accepting the Rules of Behavior. Close your Browser and go to the next slide.

in Portal

Leaving iNAP

✓ Rules of Behavior Accepted. Please return to FAMAuth to continue.

⚠ For increased security, please close your browser window.



- k. Go to: <https://famauth.wildfire.gov/>
- l. Select Public Partners 'Login.gov'

Wildland Fire Application Portal

FAMAUTH QA VERSION, USE ONLY FOR TESTING
Production link: <https://famauth.wildfire.gov/>

To login to your Wildland Fire Application please select one of the two tiles, Login.gov or eAuthentication:

Public partners **LOGIN.GOV**

Login.gov is a service that offers secure and private online access to government programs through a Private Non-Federal account.

Government **eAuth**

eAuthentication is the system that allows users access to Wildland Fire Apps and Services using government clearance.

⚠ Upon logging in, you agree to the following information:

Unauthorized access to this United States Government Computer System and software is prohibited by Title 18, United States Code 1030.

This statute states that: Whoever knowingly, or intentionally accesses a computer without authorization or exceeds authorized access, and by means of such conduct, obtains, alters, damages, destroys, or discloses information or prevents authorized use of (data or a computer owned by or operated for) the Government of the United States shall be punished by a fine under this title or imprisonment for not more than 10 years, or both.




All activities on this system and network may be monitored, intercepted, recorded, read, copied, or captured in any manner and disclosed in any manner by authorized personnel. THERE IS NO RIGHT OF PRIVACY ON THIS SYSTEM. System personnel may give to law enforcement officials any potential evidence of crimes found on this USDA computer system.

User notices
No notices today.



An official website of the United States government [Here's how you know](#)

LOGIN.GOV

National Fire & Aviation Management is using Login.gov to allow you to sign in to your account safely and securely.

Email address

Password Show password

Sign in

Create an account

[Sign in with your government employee ID](#)

[Back to National Fire & Aviation Management](#)

[Forgot your password?](#)

[Security Practices and Privacy Act Statement](#)

[Privacy Act Statement](#)

m. Enter your login.gov Email address.

n. Enter your login.gov Password.

o. Select 'Sign in



Enter your security code

We sent a security code to [REDACTED]. This code will expire in 10 minutes.

One-time security code

ZSNH4J

Remember this browser

Submit

[Get another code](#)

Don't have access to your phone right now?

[Choose another authentication method](#)

[Cancel](#)

- p. Enter One-time security code sent to your phone **(this security code will be sent to your phone each time you log in)**
- q. Uncheck 'Remember this browser.'
- r. Select 'Submit'




- s. On the Wildland Fire Application Portal page, Find the LESO FEPMIS Tile at the top of the page under 'My Applications' and select 'Access'.

To access your Wildland Fire Application select one of the tiles below:











View as Logos Tiles

▼ My production applications

 LESO FEPMIS

▼ My training applications

▼ Wildland fire applications Filter

<p>Data Warehouse </p> <p>Data Warehouse</p> <p>▼ </p>	<p>DRONESIM </p> <p>UAS Training, Flight Simulator</p> <p>▼ </p>	<p> EGP </p> <p>Enterprise Geospatial Portal</p> <p>▼ </p>	<p> e-ISuite </p> <p>e-ISuite Enterprise</p> <p>▼ </p>
--	--	---	---

User
Applica
FEMS
FEMS
Provi
Provis
shoul



t. On the LESO FEPMIS: Initial login Select 'NEW USER'

LESO FEPMIS: Initial Login User ID: Not Logged In

Welcome to the LESO FEPMIS Initial iNAP login screen. After either linking your current LESO FEPMIS account to iNAP or creating your new LESO FEPMIS account you will no longer see this screen when logging in.

If you are an existing LESO FEPMIS user you must link your iNAP account to your LESO FEPMIS account for historical and audit purposes. Please select 'CURRENT USER'


If you are new LESO FEPMIS user you must create a new LESO FEPMIS account. Only create a new account if you have never used LESO FEPMIS before.

NEW USER

LESO FEPMIS Menu

Email: LESO@DLA.MIL
Phone: 800.332.9946
Fax: 269.961.4431
IIA Helodesk
(866) 224-7677





LESO FEPMIS
Menu

LESO FEPMIS: Create LESO FEPMIS Account User ID: Not Logged In

Please enter your information

Error/Info Messages:

User First Name:

User Last Name:

Title:

Address: *

Address 2:

City:

State:

Zip Code:

Telephone Number:

Telephone Number Extension:

Cell Number:

Email Address: *

Fields marked with '*' are required

Create
Back


Note: If you are not a NEW FEPMIS User then stop and go to the existing user guide.

u. Enter user information.

v. Select 'Create'

Note: all fields with an * are required.





LESOFEPMIS
Menu

Email: LESO@DLA.ML
Phone: 800.532.9946
Fax: 269.961.4431
JJA Helpdesk:
(866) 224-7677

LESOFEPMIS: Rules of Behavior (RoB) User ID: Not Logged In

***** User ID 'N7018' was successfully connected to your iNAP account. Please make note of your User ID 'N7018' and notify your State Contact that you have successfully created a new FEPMIS account so your FEPMIS roles can be assigned. *****

GOVERNMENT WARNING

The Rules of Behavior (RoB) for Use of a U.S. Government (USG) Information System (IS) provides the rules that govern the appropriate use of information resources for Department users, including federal employees, contractors, and other system users. All users of USG information resources must read and accept the RoB before accessing data or other information, systems, and/or networks. This acknowledgement must be completed annually thereafter. By accepting the RoB users reaffirm their knowledge of, and agreement to adhere to, the USG RoB. The USG RoB cannot account for every possible situation. Therefore, where the USG RoB does not provide explicit guidance, personnel must use their best judgment to apply the principles set forth in the standards for ethical conduct to guide their actions.

You are accessing a USG IS that is provided for USG-authorized use only.

All USG IS may be monitored for all lawful purposes, including but not limited to, ensuring that use is authorized, for management of the system, to facilitate protection against unauthorized access, and to verify security procedures, survivability and operational security. Any information on this computer system may be examined, recorded and copied and used for authorized purposes at any time.

All information, including personal information, placed or sent over this system may be monitored, and users of this system are reminded that such monitoring does occur. Therefore, there should be no expectation of privacy with respect to use of this system.

By logging into this Information System, you acknowledge and consent to monitoring of this system. Evidence of your use, authorized and unauthorized, collected during monitoring may be used for civil, criminal, administrative, or other adverse action. Unauthorized or illegal use may subject you to prosecution.

By using this IS (which includes any device attached to this IS), you consent to the following conditions:

- USG may intercept and monitor communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.
- Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose.
- This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.

As a User:

1. I will NOT attempt to access information or information systems for which access has not been authorized;
2. I will NOT share passwords;
3. I will NOT provide my password to anyone, including system administrators;
4. I will NOT use another person's account, identity, password/passcode/PIH, or PIV card;
5. I will protect passwords and access numbers from disclosure;
6. I will promptly change a password whenever its compromise is known or suspected to have occurred;
7. I will NOT attempt to bypass access control measures;
8. I will protect sensitive information from disclosure to unauthorized persons or groups;

I understand that failure to comply with the Rules of Behavior could result in verbal or written warning, removal of system access, reassignment to other duties, criminal or civil prosecution, or termination.

w. Check the box to Acknowledge the Rules of Behavior (RoB)

x. Select 'Acknowledge'

You have successfully created a LESO FEPMIS account and your login.gov, iNAP and LESO FEPMIS accounts are all linked together. The next time you login you will go directly into the LESO FEPMIS application from login.gov.



 <p>LESO FEPMIS Menu</p> <hr/> <p>Email: LESO@DLA.MIL Phone: 800.532.9946 Fax: 269.961.4431 IIA Helpdesk (866) 224-7677</p>	<p>LESO FEPMIS: Initial Login User ID: Not Logged In</p> <hr/> <p>Your account has been updated and you have been logged off. You MUST CLOSE your browser down completely and reconnect through iNAP.</p>
---	--

You Must now....

Close your browser completely or you might have browser cache issues.

Contact your State Point of Contact to assign you to a Station and new user roles.



3. Logging into FEPMIS account for first time after setup.

Note: This will be your access point for a LESO FEPMIS from now on so you can bookmark this page.

a. Go to: <https://famauth.wildfire.gov/>

b. Select Public Partners 'Login.gov'

An official website of the United States government. Here's how you know

USDA U.S. FOREST SERVICE CARING FOR THE LAND AND SERVING PEOPLE Wildland Fire Application Portal

To login to your Wildland Fire Application please select one of the two tiles, Login.gov or eAuthentication:

Public partners LOGIN.GOV

Login.gov is a service that offers secure and private online access to government programs through a Private Non-Federal account.

Government eAuth

eAuthentication is the system that allows users access to Wildland Fire Apps and Services using government clearance.

⚠ Upon logging in, you agree to the following information:

Unauthorized access to this United States Government Computer System and software is prohibited by Title 18, United States Code 1030.

This statute states that: Whoever knowingly, or intentionally accesses a computer without authorization or exceeds authorized access, and by means of such conduct, obtains, alters, damages, destroys, or discloses information or prevents authorized use of (data or a computer owned by or operated for) the Government of the United States shall be punished by a fine under this title or imprisonment for not more than 10 years, or both.

All activities on this system and network may be monitored, intercepted, recorded, read, copied, or captured in any manner and disclosed in any manner by authorized personnel. THERE IS NO RIGHT OF PRIVACY ON THIS SYSTEM.

User notices

Application
FEMS


FEMS


Provisional Data Sets (8/10/2023)

Provisional data sets are being used, operational decisions should be made with caution.



An official website of the United States government [Here's how you know](#)

LOGIN.GOV 



National Fire & Aviation Management is using Login.gov to allow you to sign in to your account safely and securely.



Email address

Password Show password

Sign in

Create an account

[Sign in with your government employee ID](#)

[Back to National Fire & Aviation Management](#)
[Forgot your password?](#)
[Security Practices and Privacy Act Statement](#) 
[Privacy Act Statement](#) 

Note: If you have not created a login.gov account yet stop and go to step 1 to create an account.

- c. Enter your login.gov Email address.
- d. Enter your login.gov Password.
- e. Select 'Sign in'



Note: A new one-time security code will be sent to your phone, this is your 2nd level of authentication.

Enter your security code

We sent a security code to [REDACTED]. This code will expire in 10 minutes.

One-time security code

ZSNH4J

Remember this browser

Submit

[Get another code](#)

Don't have access to your phone right now?
[Choose another authentication method](#)

[Cancel](#)

- f. Enter one-time security code sent to your phone (**this security code will be sent to your phone each time you log in**)
- g. Uncheck 'Remember this browser.'
- h. Select 'Submit'




- i. On the Wildland Fire Application Portal page, Find the LESO FEPMIS Tile at the top of the page under 'My Applications' and select 'Access'.

To access your Wildland Fire Application select one of the tiles below:





View as Logos Tiles

▼ My production applications

 LESO FEPMIS


▼ My training applications

▼ Wildland fire applications Filter tiles

 Data Warehouse	 DRONESIM	 EGP	 e-ISuite
Data Warehouse	UAS Training, Flight Simulator	Enterprise Geospatial Portal	e-ISuite Enterprise



j. Once you click Access you will be directed to LESO FEPMIS

 <p>LESO FEPMIS</p> <p>Menu</p> <ul style="list-style-type: none"> Home Manage Account Receive Receipts Access CCS Inventory Worksheets LESO Inventory Station Item Liability User Management Query Property Queries and Reports <p>Logout</p> <p>Email: LESO@DLA.MIL Phone: 800.532.9946 Fax: 269.961.4431 TIA Helpline: (866) 224-7677</p>	<p>Welcome to LESO FEPMIS</p> <p>LESO FEPMIS</p> <p>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.</p>		<p>DSF0000</p> <p>Your last login was on: 02/16/2022 05:34:20</p>
	<p>**ATTENTION LESO FEPMIS USERS**</p> <p>NOTE: IIA Helpline should be contacted for account access issues. All other LESO FEPMIS issues should be directed to your State Coordinator. If the State Coordinator cannot resolve your issue then the State Coordinator should contact the LESO HQ.</p> <p>NOTE: All DLA access questions (ie DLA Enterprise External Business Portal, DLA AMPS) should be directed to the DLA Enterprise help desk Toll Free: 855.332.6903.</p> <p>DOD DLA Disposition Services LESO Training Material: Find Your State Coordinator and Other Helpful Information</p> <p>DLA Enterprise External Business Portal</p> <p>DLA AMPS</p> <p>NOTE: THE USDA IS NOT RESPONSIBLE FOR THE ABOVE LINKS. DO NOT CONTACT THE LESO FEPMIS IIA HELPLINES WITH ANY ISSUES WITH THE ABOVE LINKS. PLEASE CONTACT YOUR STATE COORDINATOR.</p> <p>Email: LESO@DLA.MIL Phone: 800.532.9946 Fax: 269.961.4431 Password Reset: 866.224.7677 opt #1 LESO FEPMIS - IIA Helpline Online</p> <p>Providing Support To America's Law Enforcement Community Since 1997</p> <p>FAMIVER</p>		<p>**ATTENTION LESO FEPMIS USERS**</p> <p>**Commerce Control List (CCL) Items**</p> <p>Upon title transfer of property, LEAs will consult with Departments of State and Department of Commerce Export Control Regulators about the type of export controls that apply to the item, regardless of DENTL code. LEAs may request a formal Commodity Classification from the Department of Commerce, Bureau of Industry and Security, or submit a General Correspondence request to the Department of State, Directorate of Defense Trade Controls. Information on managing exports of Commerce Control List (CCL) items can be found at the Bureau of Industry and Security (BIS) website.</p> <p>- WARNING - DEATH OR SERIOUS INJURY COULD OCCUR</p> <p>*** ALERT *** DEATH OR SERIOUS INJURY OR DAMAGE TO EQUIPMENT COULD OCCUR</p> <p>PREMATURE SIDEWALL BLOW-OUTS IN GOODYEAR WRANGLER MTR/TIRES ON THE H9MWV AND M1101, M1102, HEAVY CHASSIS TRAILERS.</p> <p>Only the Goodyear Wrangler MTR is affected by this message: 37x12.50R16.SLT Goodyear Wrangler MTR (Load Range E Tire NSN 2610-01-541-4899 used on Tire/Wheel Assembly NSN 2530-01-558-9338) and (Load Range E Tire NSN 2610-01-563-8328 used on Tire/Wheel Assembly NSN 2530-01-563-8628).</p> <p>*** ALERT ***</p> <p>- ATTENTION - ALL USERS REQUIRE TWO-FACTOR AUTHENTICATION USING LOGIN.GOV FOR CONTINUED ACCESS</p> <p>*** ATTENTION *** ALL USERS REQUIRE TWO-FACTOR AUTHENTICATION USING LOGIN.GOV FOR CONTINUED ACCESS</p> <p>### 07-Mar-2022 is a target date and subject to change##</p> <p>ATTENTION: On 07-March-2022 LESO FEPMIS will go to a two-factor authentication application called login.gov. You will be required to create an account in login.gov and link your iNAP and LESO FEPMIS accounts to your new login.gov account. Your State POC should be providing guidance to you by the end of the month. If you have not received guidance by the first week in March please reach out to your State POC via the helpline. Only reach out to the help desk if you have access during your switch to the new application.</p> <p>Contact your State Point of Contact for more details.</p>

You have completed the login process for FEPMIS.

