National Firefighter Registry

Requirements Engineering Review

August 2021
Agenda

• Identity Management & Privacy Compliance
• Participant Account Considerations
• Account Creation Walkthrough
• Example NFR Participant Profiles
• Project Planning & Timing
Federal System Compliance Requirements

- Protecting participants and their information
  - Basic Identity Theft
  - First Responder Status
  - Personal Information
  - Health Status
  - Employment History
  - Questionnaire Details

- Compliance exists to mitigate risk to participants

<table>
<thead>
<tr>
<th>FedRAMP System Categorization</th>
<th>Identity Assurance Level (IAL)</th>
<th>Authenticator Assurance Level (AAL)</th>
<th>Federation Assurance Level (FAL)</th>
</tr>
</thead>
<tbody>
<tr>
<td>High</td>
<td>IAL3: In-person, or supervised remote identity proofing</td>
<td>AAL3: Multi-factor required based on hardware-based cryptographic authenticator and approved cryptographic techniques</td>
<td>FAL3: The subscriber (user) must provide proof of possession of a cryptographic key, which is referenced by the assertion. The assertion is signed and encrypted by the identity provider, such that only the relying party can decrypt it</td>
</tr>
<tr>
<td>Moderate</td>
<td>IAL2: In-person or remote, potentially involving a “trusted referee”</td>
<td>AAL2: Multi-factor required, using approved cryptographic techniques</td>
<td>FAL2: Assertion is signed and encrypted by the identity provider, such that only the relying party can decrypt it</td>
</tr>
<tr>
<td>Low</td>
<td>IAL1: Self-asserted</td>
<td>AAL1: Single-factor or multi-factor</td>
<td>FAL1: Assertion is digitally signed by the identity provider</td>
</tr>
</tbody>
</table>
Protecting Identities and Information

- Protecting data is less burdensome to users than protecting identities and access
  - Data collected from responders can be protected with elaborate measures through hidden background technology
  - One-way data (like survey data) can be collected via secure interface and pushed into a highly secure database
  - Data within a registry that can re-accessed over time by identities (accounts) through authentication (secure login) presents additional risk to be mitigated
Balancing NFR Functionality & Compliance

• When designing systems like NFR, features that improve research and overall value often require enhanced controls to mitigate risk.

• Content shared today is intended to drive analysis and input for the best “balance” of functionality and associated controls.

• Analysis of benefits vs burden (perceived complexities) should be based on typical firefighter perspective and potential difficulties in communicating security measures.
NFR Account Functionality & Design Considerations

• Functionality of the NFR system to offer participant profiles and retrieve sensitive data increase compliance controls

• Long-term functionality should be considered when determining the best approach for participant account management

• To better facilitate updating of data over time, priority should be given to implementing hierarchical, directly accessible profile and survey data that can be easily retrieved, reviewed and updated

• Modular, categorized and directly accessible surveys in an easy-to-use library will provide long-term flexibility to refine and enhance data capture needs
NFR Participation & Account Design Options

1. Full Registration – No Limits on Data Retrieval/Update
   - Robust participant profile includes employment and health history
   - Participant can view and update previously submitted survey data
   - Requires account creation & identity proofing

2. Light Registration – No Sensitive Health Information
   - Profile only includes less-sensitive health identifiers
   - No ability of participant to recall survey response (sensitive health information)
   - Requires account creation

3. No Registration or Profile
   - Functions like a web-based survey
   - No persistent data – each survey is a stand-alone transaction
   - No participant account
Overview of Identity Proofing

• Identity proofing is used to establish uniqueness and validity of an individual’s identity

• This is accomplished through automated, digital validation of a participant’s state issued ID and personal records

• Federal systems rated moderate that enable retrieval of sensitive information require Identity Assurance (IAL2)

• Identity proofing mitigates risk of account compromise, spoofing or hijacking that would expose sensitive data
Examples of Data and Requirement for Identity Proofing

<table>
<thead>
<tr>
<th>Data</th>
<th>ID Proofing Required</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>NO</td>
</tr>
<tr>
<td>Residential Address</td>
<td>NO</td>
</tr>
<tr>
<td>Email Address</td>
<td>NO</td>
</tr>
<tr>
<td>Phone Number</td>
<td>NO</td>
</tr>
<tr>
<td>Work Status</td>
<td>NO</td>
</tr>
<tr>
<td>Current Department</td>
<td>YES</td>
</tr>
<tr>
<td>EmployeeID</td>
<td>YES</td>
</tr>
<tr>
<td>Year Start/Stop working</td>
<td>YES</td>
</tr>
<tr>
<td>Job Title</td>
<td>YES</td>
</tr>
<tr>
<td>Cancer Diagnosis</td>
<td>YES</td>
</tr>
<tr>
<td>Date of Birth</td>
<td>YES</td>
</tr>
<tr>
<td>Country/City/State of Birth</td>
<td>YES</td>
</tr>
<tr>
<td>SSN</td>
<td>YES</td>
</tr>
</tbody>
</table>

- **Option 1**
  - would allow participants to retrieve any previously submitted data, including basic registration (green) and sensitive data (red)
  - requires identity proofing to protect a participant’s sensitive data (red) because it can be retrieved and is exposed to the public.

- **Option 2**
  - does not require identity proofing because sensitive data (red) cannot be retrieved.
  - would allow participants to retrieve only basic registration data (green) because retrieval is limited to less sensitive data.

- **Option 3**
  - would not allow participants to retrieve any information. Identity proofing is not required because none of the data can be retrieved.
When you're ready to create your secure Login.gov account, you'll need to provide a few pieces of information:

1. **Email address**
   - We recommend a personal email address that you'll always be able to access rather than a work email address.
   - If you already have an account with Login.gov with that email address, we’ll send you an email to let you know how you can reset your password and access the account.

2. **Secure password**
   - Passwords must be at least 12 characters and should not include commonly used words or phrases.

3. **One or more authentication methods such as:**
   - More secure
     - Security Key
     - Authentication application
     - Federal government employee or military identification (PIV/CAC)
   - Less secure
     - SMS/Text messages
     - Backup codes

Your one account for government

Create an account
Creating login.gov 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

Check your email

We sent an email to XXXXXXXXXXXXX with a link to confirm your email address. Follow the link to continue creating your account.

Didn't receive an email? Resend

Or, use a different email address

You can close this window if you’re done.
Creating login.gov Account

Confirm your email

Thanks for submitting your email address. Please click the link below or copy and paste the entire link into your browser. This link will expire in 24 hours.

Confirm email address

https://secure.login.gov/sign_up/email/confirm?_request_id=&confirmation_token=t6sMMkeoVZRpyugzddUQ

Please do not reply to this message. If you need help, visit www.login.gov/help

Create a strong password

It must be at least 12 characters long and not be a commonly used password. That’s it!

Password

************

Password strength: So-so
Common names and surnames are easy to guess

Continue

Password safety tips

+ Cancel account creation
Selecting a 2-factor Authentication Method

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 that you have. It's a physical device that you plug in or that is built in to your computer or phone (it often looks like a USB flash drive). Recommended because it is more phishing resistant.

- **Authentication application**
  Get codes from an app on your phone, computer, or tablet. Recommended because it is harder to intercept than texts or phone calls.

- **Phone**
  Get security codes by text message (SMS) or phone call. Please do not use web-based (VOIP) phone services.

- **Backup codes**
  We'll give you 10 codes. You can use backup codes as your only authentication method, but it is the least recommended method since codes can get lost. Keep them in a safe place.

Continue
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

Send code

Choose another option
Login.gov Identity Proofing
- required if re-accessing sensitive health information
Login.gov Identity Proofing
- submit photo of state issued ID via cell phone
Login.gov Identity Proofing
- additional verification steps

Please verify your information

First Name: Jane
Last Name: Doe
Date of Birth: 01/01/1990
Address: 123 Apple Street
City: Nashville
State: TN
Zip Code: 12345
Social Security Number

Enter a phone number with your name on the plan

We'll check this number with phone bill records. This is to help verify your identity, we won't use it to sell or test you.

This phone number must:
- be a phone plan associated with your name (you do not need to be the primary account holder)
- not be a virtual phone (such as GoogleVoice or Skype)
- be a U.S. number

If you setup a phone for two-factor authentication, this can be a different number.

Phone Number: +1 555-555-5555

Verify your address by mail instead. We'll mail you a letter with a code in it.

Save your personal key

You'll need this personal key if you forget your password. If you reset your password and don't have this key, you'll have to verify your identity again.

Your personal key: ABCD:EFGH:HIJK:LMNO

Generated on July 23, 2023

Save it. Keep it safe. Don't lose your personal key or share it with others. We'll ask for it if you reset your password.
Example NFR Participant Profiles

• Segmented Profile Content for Ease of Use
  • Personal Information
  • Employment Information
  • Health Information

• Orange highlighted content would require identity proofed accounts – or must be moved to survey as non-retrievable attributes
Create Profile: Personal Info

CDC estimates the average time burden for this collection of information as 5 minutes per response, including the time for reviewing instructions, searching existing data/information sources, gathering and maintaining the data/information needed, and completing and reviewing the collection of information. An agency may not conduct or sponsor, and a person is not required to respond to a collection of information unless it displays a currently valid OMB control number. Send comments regarding the burden estimate or any other aspect of this collection of information including suggestions for reducing the burden to CDC/ATSDR Information Collection Review Office, 1600 Clifton Road NE, MS D-14, Atlanta, Georgia 30333, ATSDR-PR (9083-XXXX).

* Required Fields

First Name*  Middle Name  Last Name*

Have you been known by any other name (example, maiden name)?

- No
- Yes

What name?

First  Last

Date of Birth:

Month  Day  Year

Country of Birth  City of Birth  State/Territory of Birth

What is your current residential address?

Street  City  State or Territory Code  Zip Code

Save & Continue  Create Profile
Example NFR Respondent Profiles

Create Profile: Personal Info

We would like to keep you updated on the progress of the NFR. We have the following email address on file for you:

Would you like to provide another email address? A personal email address is preferred for communications because you should have access to this email even outside of work.

If you would also like to receive updates via text messages, please provide your mobile number below:

(XXX)XXX-XXXX
Example NFR Respondent Profiles

Create Profile: Employment Info

What is your current work status in the fire service (select all that apply)?

- [ ] Full time, paid
- [ ] Part time, paid
- [ ] Volunteer (full or part time)
- [ ] Seasonal
- [ ] Paid on call or paid per call
- [ ] Retired in what year did you retire: 2021
- [ ] No longer working in the fire service
- [ ] Out on long-term disability
- [ ] Other Please specify Enter Text
Example NFR Respondent Profiles

Create Profile: Employment Info

Where is your current, or most recent fire department, agency, or organization located?

What is your current, or most recent fire department, agency, or organizational affiliation?

If not listed, please list department name:

What jurisdiction do/did you serve at this department/agency/organization?

Employee ID/Departmental Identification for current or most recent position

Approximately what did you start working at <department/agency/organization> (auto populated)?

Approximately when did you stop working at <department/agency/organization> (auto populated)?

What job titles do/did you hold at this department/agency/organization? Select all that apply:

- Structural or Industrial Engineer
- As a structural firefighter, which roles most closely apply/applicable to you? (select all that apply)
  - Firefighter
  - Firefighter Medic
  - Firefighter EMT
  - Firefighter AEMT
  - Firefighter Paramedic
  - Driver/Engineer/Operator

- Wildland Firefighter
- As a wildland firefighter, which roles most closely apply/applicable to you? (select all that apply)
  - Engine crew
  - Hand crew
  - Line medic
  - Base camp support staff
  - Smokejumper

This section would be moved to the Enrollment Questionnaire with Option 2

If manually entered, the Jurisdiction pull down will be displayed.
Create Profile: Employment Info

(continued) What job titles do/did you hold at this department/agency/organization? Select all that apply:

- Company Officer (Lt, Cpt, Sgl)
- Wildland Supervisor or Overhead
- Chief
  - Fire Chief
  - Battalion/District Chief
  - Assistant Chief
  - Deputy Chief
  - Division Chief
- Fire Investigator, where this is your primary job assignment
- Instructor, where this is your primary job assignment
- Superintendent/Crew Boss
- BMT/Paramedic, where this is your primary job assignment
- Fire Marshal
- Other
This section would be moved to the Enrollment Questionnaire with Option 2

Create Profile: Health Info

Please specify: Have you ever been diagnosed with cancer?
- No
- Yes

If "yes" is selected then the user will be asked about a cancer diagnosis. If "no" is selected the cancer question will not be presented.

What type(s) of cancer were you diagnosed with? Please select where the cancer(s) started (primary site):

- Bladder
- Brain or Central Nervous System
- Breast
- Cervix
- Colon or Rectum
- Esophagus
- Hodgkin's Lymphoma
- Kidney
- Leukemia
- Liver
- Lung
- Mesothelioma
- Multiple Myeloma
- Non-Hodgkin's Lymphoma
- Oral Cavity or Pharynx (e.g. lip, tongue, palate, tonsil, other parts of the mouth)

- Ovary
- Pancreas
- Prostate
- Skin: Melanoma
- Skin: Non-Melanoma (e.g. basil cell carcinoma, squamous cell carcinoma) or Unknown
- Small Intestine
- Stomach
- Testis
- Thyroid
- Uterus/Endometrium
- Unsure
- Other
Create Profile: Health Info

For each cancer selected, except for Leukemia, the following questions will be displayed

For each cancer selected, except for Leukemia, the following questions will be displayed

- Cancer name:
  - What was your age when first diagnosed? [Age]
  - In what US state/territory were you living when first diagnosed? [State/Territory]

If Leukemia was selected, display the following:

What type of Leukemia were you diagnosed with?

- Acute myeloid (or myelogenous) leukemia (AML)
- Chronic myeloid (or myelogenous) leukemia (CML)
- Acute lymphocytic (or lymphoblastic) leukemia (ALL)
- Chronic lymphocytic leukemia (CLL)
- Other or Unsure

Leukemia:
- What was your age when first diagnosed? [Age]

- In what US state/territory were you living when first diagnosed? [State/Territory]
Create Profile: Health Info

In the United States, each state has a cancer registry that collects and combines information on all cancer diagnoses from all hospital in that state. Providing your social security number (SSN) is the only way to guarantee the information you provide in your user profile and questionnaire matches any past or potentially future cancer diagnosis reported to a state. This information is necessary to meet the statutory requirements of the Firefighter Cancer Registry Act of 2018. You can choose to provide this information or not. However, without this information, your data may not be included in the analysis of firefighters’ cancer risks. As noted on the informed consent, all your private information will be encrypted, secured, and protected to the fullest extent allowed by law.

SSN: ________________

Confirm SSN: ___________

Why are we asking this?

This question is not about data breaches. It is about understanding the risks and potential treatments for firefighters with cancer.

We need to know your social security number to help us understand the risks and potential treatments for firefighters with cancer.

Information we can use any potential future cancer diagnosis without any further action from you. Each Firefighter Must share this information will increase the accuracy of our findings, which could potentially lead to greater protections for all firefighters. Sharing your social security number will ensure your participation has the maximum impact.

We will protect your information to the fullest extent allowed by law. The National Firefighter Registry is covered by an assurance of confidentiality, whether the highest level of protection mandated by your state’s law. Under this framework, we are not allowed to share your identifiable information without your written permission. We never will share your social security number, contact information, or identifiable questionnaires to companies and insurance companies. Your privacy is as important to us as your participation.
Detailed attributes collected for either of the 3 Account Design Options
Project Planning & Timing

NFR PLANNING SERVICES

- Business Needs Analysis 6/2021
- Requirements Engineering 9/2021
- Solution Engineering 2/2022
- Implementation 7/2022

Estimated timeline
NFR Participation & Account Design Options

1. Full Registration – No Limits on Data Retrieval/Update
   • Robust participant profile includes employment and health history
   • Participant can view and update previously submitted survey data
   • Requires account creation & identity proofing

2. Light Registration – No Sensitive Health Information
   • Profile only includes less-sensitive health identifiers
   • No ability of participant to recall survey response (sensitive health information)
   • Requires account creation

3. No Registration or Profile
   • Functions like a web-based survey
   • No persistent data – each survey is a stand-alone transaction
   • No participant account