National Firefighter Registry

Requirements Engineering Review

August 2021

NIOSH®

ODDM DIT Office of Deputy Director for Management
Office of Information Technology and Informatics Services

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

FedRAMP System Categorization	Identity Assurance Level (IAL)	Authenticator Assurance Level (AAL)	Federation Assurance Level (FAL)
High	IAL3: In-person, or supervised remote identity proofing	AAL3: Multi-factor required based on hardware-based cryptographic authenticator and approved cryptographic techniques	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
Moderate	IAL2: In-person or remote, potentially involving a "trusted referee"	AAL2: Multi-factor required, using approved cryptographic techniques	FAL2: Assertion is signed and encrypted by the identity provider, such that only the relying party can decrypt it
Low	IAL1: Self-asserted	AAL1: Single-factor or multi-factor	FAL1: Assertion is digitally signed by the identity provider

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

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

- *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

NFR Account Creation via Login.gov

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.
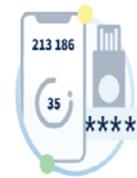
3. One or more authentication methods such as:

- **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

LOGIN.GOV

📧 Check your email

We sent an email to XXXXXXXXXX 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

LOGIN.GOV

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

---

✓ You have confirmed your email address

Create a strong password

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

Password   ☐ Show 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.

MORE SECURE

○ **Government employee ID**

Insert your government or military PIV or CAC card and enter your PIN.

MORE SECURE

○ **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.

SECURE

○ **Phone**

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

LESS SECURE

○ **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 notes can get lost. Keep them in a safe place.

LEAST SECURE

Continue

SMS Text Message is Popular 2ⁿᵈ Factor

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

🇺🇸 ▾

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
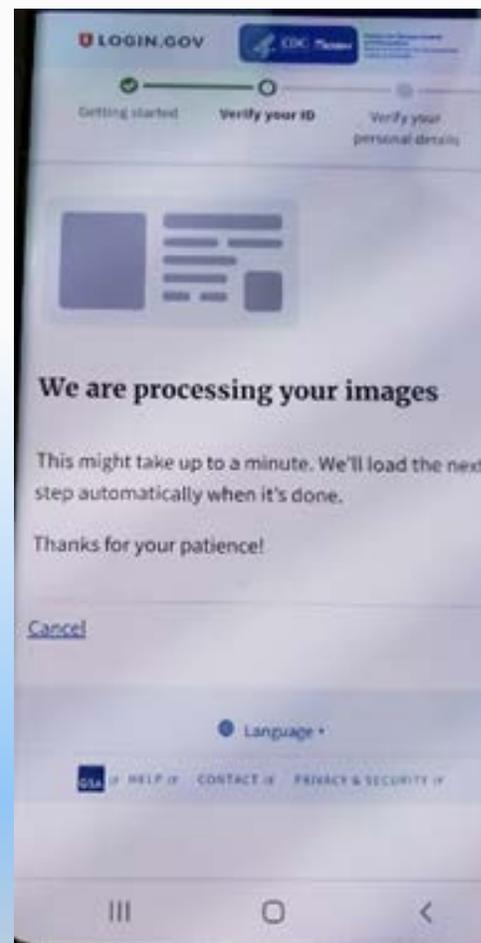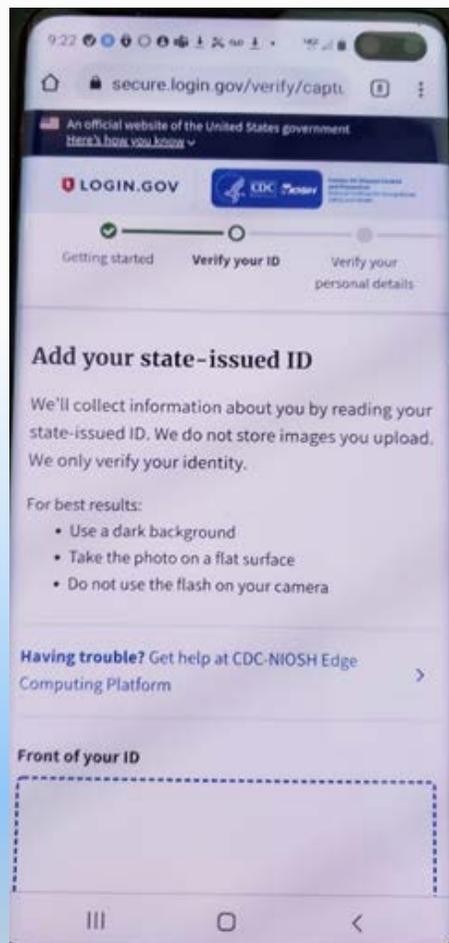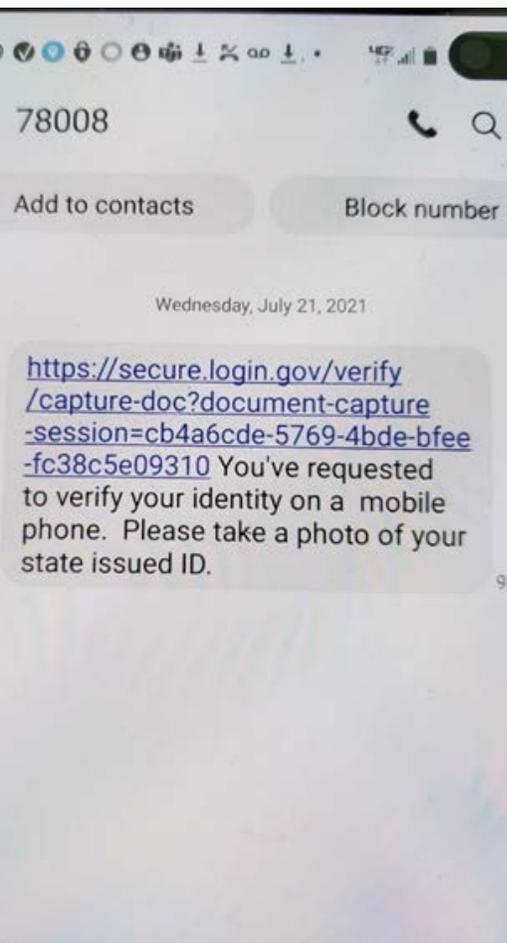
Login.gov Identity Proofing
- additional verification steps

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

Example NFR Respondent Profiles

Example NFR Respondent Profiles

Microsoft - Official Home

https://NationalFireFightersWebsite.com/

Create Profile: Personal Info

Dashboard

Informed Consent

User Profile
1. Personal Info
2. Employment Info
3. Health Info

Enrollment Questionnaire

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 you mobile number below

(xxx)xxx-xxxx

Save & Continue:
Create Profile

Example NFR Respondent Profiles

Example NFR Respondent Profiles

Example NFR Respondent Profiles

Example NFR Respondent Profiles

Example NFR Respondent Profiles

Example NFR Respondent Profiles

Create Profile: Health Info

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

In the United States, each state has a cancer registry that collects and combines information on all cancer diagnoses from all hospitals 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 risk. 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?

[Pop-up box if user clicks "why are we asking this"]
Why are we asking for this?
We need to track firefighters' health over time to truly understand their cancer risks and improve their protections. Your social security number will let us do this by linking your information to state cancer registries. With this information we can see any potential future cancer diagnosis without any further action from you. Each firefighter that shares 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, which is the highest level of protection available for identifiable information. Under this formal protection, we are not allowed to share your identifiable information without your written permission. This means we will not share your social security number, contact information, or identifiable questionnaire responses with outside groups like your employer, insurance company, or even for a lawsuit. Your privacy is as important to us as your participation.

Save & Continue: Create Profile

Begin Survey

Detailed attributes collected for either of the 3 Account Design Options

---

Microsoft - Official Home

https://NationalFireFightersWebsite.com/

John Public

Dashboard
Informed Consent
User Profile
Enrollment Questionnaire

1. Demographics

2. Work & Exposure History

3. Lifestyle

4. Health History

5. Submit

CDC estimates the average reporting burden for this collection of information as 30 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 this burden estimate or any other aspect of this collection of information including suggestion for reducing the burden to CDC/ATSDR Information Collection Review Office, 1500 Clifton Road NE, MS D-74, Atlanta, Georgia 30333; ATTN: PRA (0920-XXXX).

Enrollment Questionnaire

1. First Name* `John`
2. Middle Name `Quinton`
3. Last Name* `Public`

4. Employee ID/Departmental Identification for current of most recent position

5. Date of Birth:
Month `January`
Day `01`
Year `1950`

6. Country of Birth
City of Birth
US State/ Territory of Birth

7. Current residential address:
Street
City
State or Territory Code
Zip Code

Fields 1 through 7 are to be auto populated from the user profile

8. What sex were you assigned at birth, on your original birth certificate? ○ Male   ○ Female   Clear

9. Ethnicity – Are you Hispanic or Latino?
○ Yes, I am Hispanic or Latino
○ No, I am not Hispanic or Latino

10. Race (select one or more):
☐ American Indian or Alaska Native
☐ Asian
☐ Black or African American
☐ Native Hawaiian or Other Pacific Islander
☐ White

11. Marital status: ○ Married   ○ Living with a partner As an unmarried couple   ○ Never married   ○ Separated   ○ Widowed   ○ Other – Please specify: ○ Prefer not to answer   Clear

12. What is your height? ___ feet ___ inches

(if pregnant, please report pre-pregnancy weight)

13. What is your current weight? ___ pounds

Pregnancy note only displayed if user selected female

Save & Continue >>

Project Planning & Timing

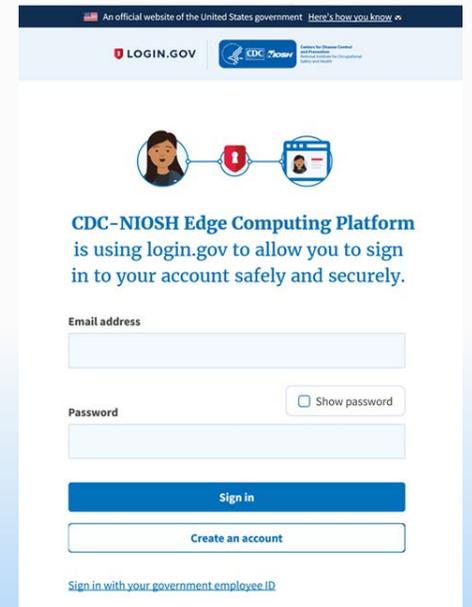## NFR PLANNING SERVICES

- 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