United States Department of Agriculture
Office of the Chief Financial Officer
National Finance Center
Government Employees Services Division

Functional Requirements Document (FRD)

Project#	Project Title:	Date Prepared:
42117	Multi-Factor Authentication for EmpowHR	08/12/2022

Version:	As of:
2.3	03/14/2023

Scope:	The Office of Management and Budget (OMB) has instructed USDA to enforce PIV for all applicable information technology systems, applications, and devices. EmpowHR will provide a second alternative authentication, 2-factor authentication solution by implementing SMS (Short Message Service) 2-factor authentication for users without a PIV card or PIV card reader availability. EmpowHR will force authentication by providing a one-time-use pass code to a user's registered mobile phone number or via an authentication application.
Assumptions:	The one-time passcode and SMS generation will be at the NFC application level. The one-time passcode will be valid for 10 minutes. After 10 minutes the user will need to re-authenticate to generate a new passcode. The user will contact NCC if they need to reset the alternative MFA set-up. Opt-out responses (i.e Keywords: cancel, end, quit, stop, stopall, unsubscribe) and help responses (i.e help, info) when the user reply with the key words have been established in project 40494 - PIV EPP Two Factors Authentication.

Functional Requirements

☐ **Payroll Applications Systems Branch (PASB) Requirements**

"Not Applicable"

☐ **Personnel Applications Systems Branch (PESB) Requirements**

"Not Applicable"

☐ **Administrative Applications Systems Branch (AASB) Requirements**

"Not Applicable"

☐ **Payroll Web Systems Branch (PWSB) Requirements**

"Not Applicable"

☐ **Administrative Web Systems Branch (AWSB) Requirements**

"Not Applicable"

☑ **Human Resources Applications Branch (HRAB) Requirements**

EmpowHR shall be modified to allow an alternative 2FA method by implementing Short Message Services (SMS). The alternative 2FA login method will be required to users that are logging in using the user ID and Password and are not PIV enabled.

EmpowHR shall have an edit to enforce user IDs that are PIV enabled to require logging in using the eAuth method.

EMPOWHR shall require initial 2FA configuration. Refer to **appendix A** for mockup examples. The user will be requested to select the verification mode of their choice of the two-step verification method identified below:

- Text Message:
  - EMPOWHR shall prompt the user to enter their mobile phone number for the code to be issued.
  - EmpowHR shall generate the random 6-digit passcode and SMS the passcode to the user's mobile phone number. Upon successful initial confirmation of the passcode shall the user's phone number be successfully registered and stored.
  - Modify the sign-on procedure to allow the capability to enter the generated passcode for user verification. EmpowHR shall limit the user to 5 failed attempts and provide the capability to "Resend Code".
  - The code will be valid for 10 minutes. If the user leaves the page, they will have to logon again for a new code to be generated.
  - Upon successful entry of the passcode received on the requested screen, the user is taken to the EmpowHR main screen.

☑ **Human Resources Applications Branch (HRAB) Requirements**

- Phone Call - Automated Voice response system will be used to call the user when they log into the system with a one-time use code. This code will be entered to verify access to the system. Upon successful initial confirmation of the passcode shall the user's phone number be successfully registered and stored.

- Application Authentication – Authentication apps generate security codes for signing into sites that require a high level of security. EMPOWHR shall allow the user to choose the application from the list for the code to be generated. Upon successful initial confirmation of the passcode shall the authentication application be successfully registered. Some options for authentication apps include:
  - Android: Google Authenticator, Authy, LastPass, 1Password
  - iOS: Google Authenticator, Authy, LastPass, 1Password
  - Windows: Microsoft Authenticator, 1Password, OneLogin OTP
  - Mac: 1Password, OTP Manager

Create records, pages and component and security roles as needed to provide the capability to:

- capture the user's OPRID and mobile phone number.
- allow NCC and Administrators to reset the user's 2FA setup.
- allow users to reset or change their 2FA setup through Employee Self-Service (ESS).
- the user shall be notified via email of any security setting changes.

System accounts shall be excluded from the end user MFA requirements.

Modify the login screen to include specific verbiage and/or hyperlinks to the NFC MFA Mobile Terms of Use.
(https://www.nfc.usda.gov/AdditionalResources/mobile_terms_service.php)

Project#	Project Title:	Date Prepared:
42117	Multi-Factor Authentication for EmpowHR	08/12/2022

☐ **External Vendor Requirements**

"Not Applicable"

Signature of Systems Requirements Branch Chief	Date:
N/A	

Signature of Web Requirements Branch Chief	Date:
/s/ Amanda Nguyen	**03/14/2023**

Appendix A – EmpowHR 2FA Mockup

Opt-in/Set up MFA procedures

1. Select Option

Two-Step Authentication

To help protect your EMPOWHR account from fraudulent activity and add extra security, we are adding two-step authentication which requires you to enter a one-time verification (security) code. You can receive a verification code by text message (SMS) or phone call, or you can enter a security code generated by an authentication application.

Text message (SMS) and phone call are available in the US only. If you are outside of the US, you must use the Authentication application option.

Choose an option to verify your access:

O Text Message (SMS)

NFC MFA. Message and data rates apply. Reply HELP for help, STOP to cancel. See our Terms of Service, Privacy Act Notice (below).

O Phone Call

O Authentication Application

Continue

What is a text message (SMS)?

Each time you log into your account with your password, we will send a one-time verification code via text message (SMS) to your registered phone number. You will then enter that code to verify your account access.

What is an Authentication App?

Authentication apps generate security codes for signing into sites that require a high level of security. You can use these apps to get security codes even if you don't have an internet connection or mobile service. A mobile phone app is the typical example of an authentication app, but other forms exist, including applications for desktops, browser extensions, and physical hardware.

Any application that implements the time-based one-time password (TOTP) standard and can use a QR code or accept a manually entered key will also work. After installing and configuring the application to work with the registrar, you will be able to generate security codes for your account.

Please note that some authentication apps have a cost.

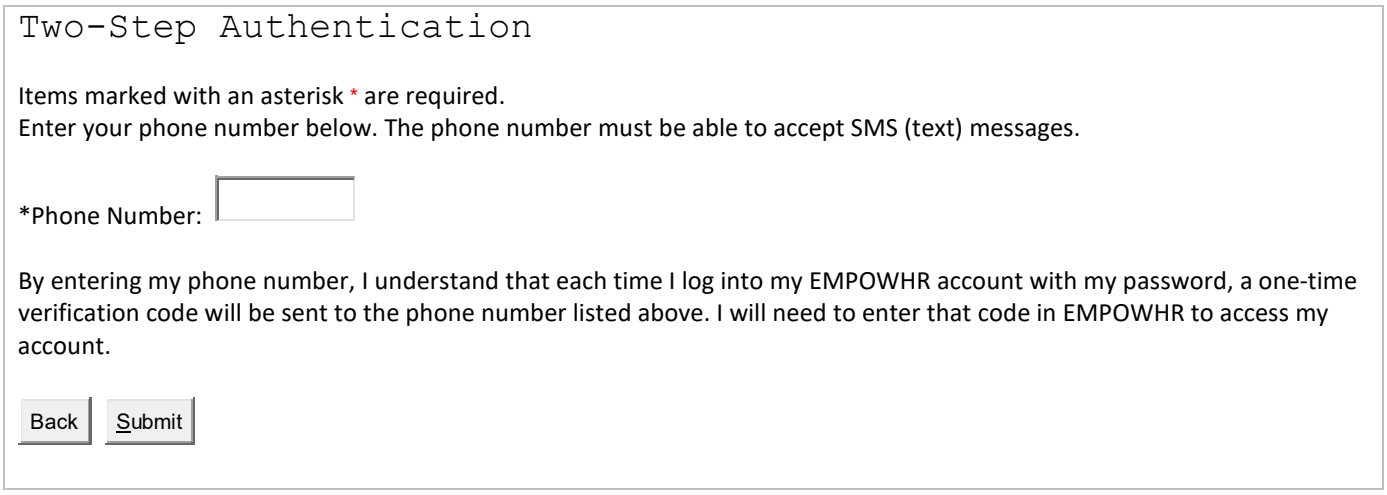
What is phone call?

Each time you log into your account with your password, we will send a one-time verification code via a phone call to your registered phone number. You will then enter that code to verify your account access.

Privacy Act Notice

We are asking for your personal contact information, including your phone number and email address, to send confirmation notices to you about online transactions. We use and retain your personal information only for this purpose and only as long as needed, as authorized by law. We will not share the information you provide to us other than as provided by law.

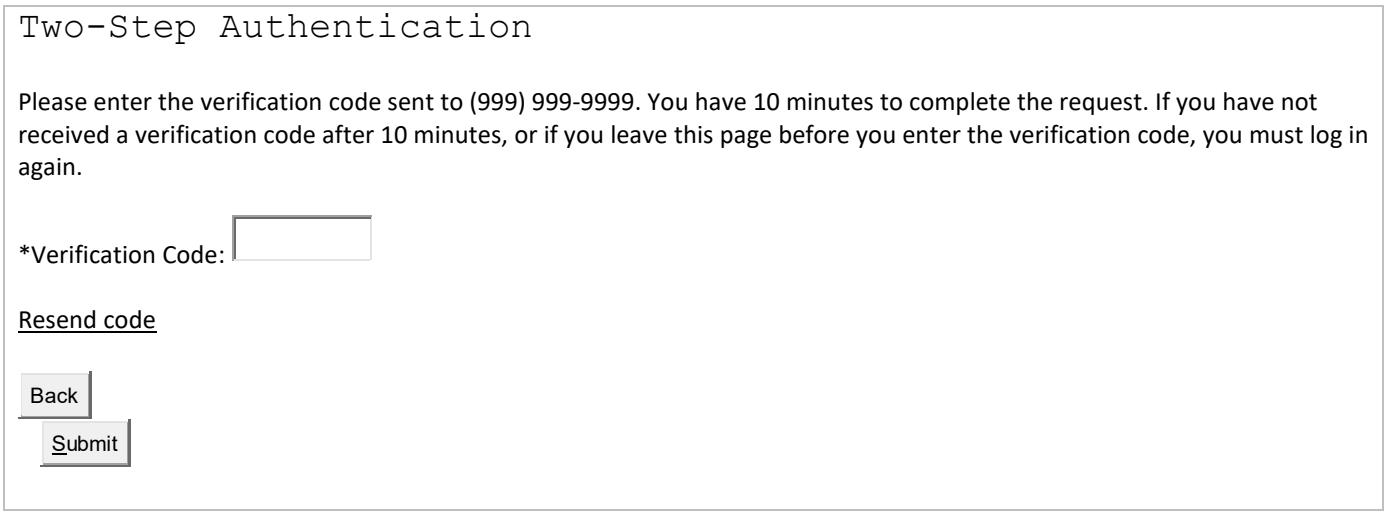
2. Enter Phone Number



3. Receive Code via message

"NFC MFA. Your EMPOWHR verification code is 999999. This code is valid for 10 minutes."

4. Enter Verification Code



5. Receive confirmation via message

"Welcome to NFC MFA. Msg&data rates may apply. 1 message per login. Reply HELP for help, STOP to cancel."

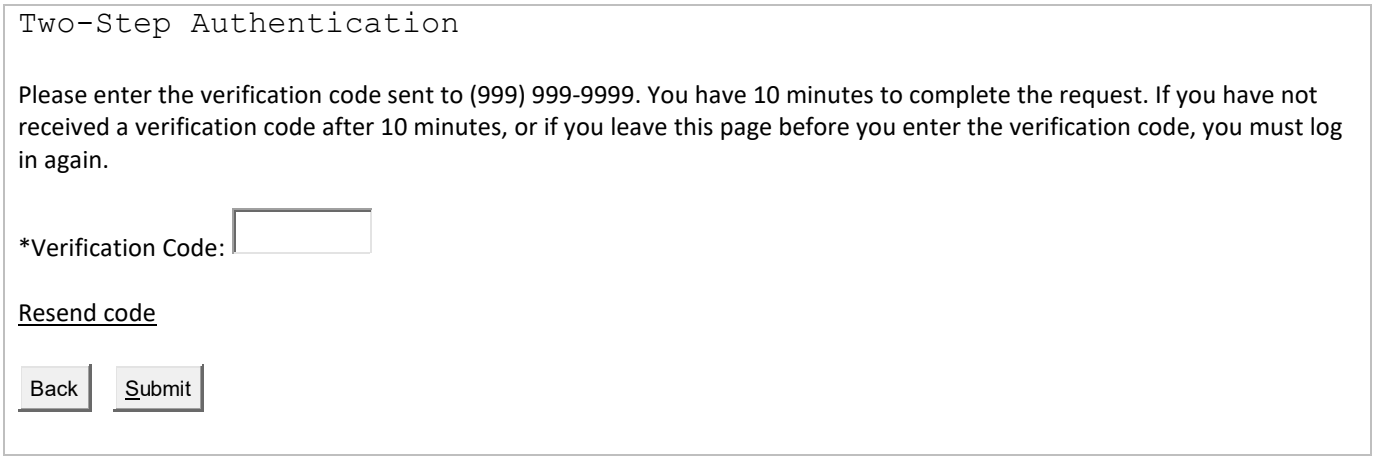
Log-in procedures

1. Enter Credentials

2. Receive code via message

   "NFC MFA. Your EMPOWHR verification code is 999999. This code is valid for 10 minutes."

3. Enter Verification Code



Opt-Out Responses

Message: NFC MFA: To unsubscribe, call (800) 767-9641, Weekdays 6:30 AM to 5:00 PM CT, except Federal Holidays. Msg&data rates may apply. 1 message per login.

Help Responses

Message: NFC MFA: Help at (800) 767-9641, Weekdays 6:30 AM to 5:00 PM CT, except Federal Holidays. Msg&data rates may apply. 1 message per login. Reply STOP to cancel.