The BHE JAGGAER Advantage platform requires multi-factor authentication (MFA) to access the system.

Two available options:

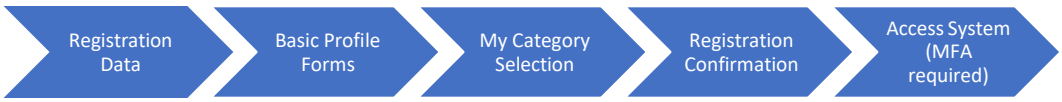
Option 1: Install Google Authenticator (MFA) on Smartphone:

a. Installing Google Authenticator
b. Install Google Authenticator (official Google Authenticator app only available on iOS and Android; third party alternatives exist for Blackberry and Windows Phones)
    i. iOS – install from the Apple App Store
    ii. Android – install from the Android App Store
c. Open Google Authenticator app and scan the barcode (NOT the barcode below; this is a sample) presented during the registration process to register your smartphone. You will receive a 6-digit code – input the **Code/Token Number** (with no spaces) and **Submit**

Option 2: Install Google Chrome add-on Authenticator (MFA) on Computer:
Install this Chrome add-on and use Google Authenticator codes straight from your computer browser.

https://chrome.google.com/webstore/detail/authenticator/bhghoamapcdpbohphigoooaddinpkbai

Next access the BHE JAGGAER Advantage Platform:



1. Enter username and temporary password
    a. Note: if self-registering (those that initiated the supplier registration process by clicking the "Register" button on the home page), you will receive your temporary password after the completion of the registration process (steps 4 – 7; see process flow above).
2. Accept User Agreement
3. Change Temporary Password
4. Complete Registration Data
5. Complete Basic Profile
6. Category Selection (this completes registration)
7. Login as Supplier to access the Main Dashboard
    a. Your Google Authenticator App will generate a new **Code/Token Number.** Input the 6-digit code (with no spaces) and **Submit** to access the system.

Reasons why BHE requires MFA:

- Berkshire Hathaway Energy is very serious about cyber security.

- The controls currently in place with the BHE legacy system are less stringent. However, since the legacy system was implemented, the world has changed and BHE cyber security policies have become significantly more stringent.

- The majority of cyber-attacks (85% – 90%) are authentication attacks.
    - Once malware is installed, login credentials are often stolen.

- The goal of MFA is to ensure the credentials being used actually belong to the person logging in, by requiring an additional – different factor.

- To be effective, controls need to be applied consistently.

- The goal of using strong controls, including security controls, is to assure the integrity of any process.
    - In this case the RFX process, which in the near future will include the contract process.

- A breach could allow improper access to company information
    - RFx event or Contract
    - Potential CIP Information
    - Even if only a few RFX events contain info that should be protected, you have to protect all. There is no way to effectively manage access vetting on a case by case basis.
    - With security, you have to set the bar high, not at the lowest point.