Multi-Factor Authentication is Coming Soon!
The U.S. Government, as part of its CyberSecurity National Action Plan, has mandated the use of Multi-Factor Authentication (MFA) for all federal government websites. In an effort to comply with these mandates and strengthen the security of our websites, GSA will implement MFA and new password policies on GSA AutoAuctions, GSA Fleet Applications, GSA Advantage, GSA eBuy, and GSA Global Supply.

What is Multi-Factor Authentication?
Multi-factor Authentication (MFA) is a systems access authentication method in which a user is granted access only after successfully presenting two or more pieces of evidence (or factors) to an authentication mechanism. This extra layer of security protects you, your agency or organization, and the government by making it more difficult for someone to gain unauthorized access to your user account.

What will the new login process look like?
Every time you log in to AutoAuctions, you will be required to enter your email address, password, and a one-time verification code. Please note that we will discontinue the use of the User ID login. Your email address will replace your User ID.

Will I be required to update my password?
As an added security feature, GSA has implemented policies requiring stronger passwords that meet National Institute of Standards of Technology (NIST) requirements. The first time you log in after the implementation of MFA, you will immediately be asked to change your password to meet the new length and complexity requirements. Additionally, you will be required to change your password every 90 days.

What are the new steps for logging in?
1. Enter the email address and password associated with your account.
2. You will be prompted to receive a system-generated verification code either via email or SMS (text).
3. AutoAuctions will send you a single-use verification code via the method you elected.
4. Enter the verification code into the field displayed on the AutoAuctions login screen. Note that the verification code is valid for only 5 minutes.

What forms of Multi-Factor Authentication will be supported?
Email and SMS (text) are currently the only two means of receiving the two-factor verification code. Planned future enhancements include support for Voice, Smartphone Authenticator and CAC/PIV as approved options for receiving the MFA code.