GSA U.S. General Services Administration

SAM Update - Updated July 11, 2018

NEW LOGIN PROCESS FOR SAM.GOV

What is the new login process for SAM.gov?

The first time you log in to SAM.gov after June 29, 2018, you'll be asked to create a login.gov user account (if you don't already have one). Going forward, you will use your login.gov username and password every time you log in to SAM.gov. Your current SAM.gov username and password will no longer work.

Login.gov is a service that offers secure and private online access to government programs, such as federal benefits, services, and applications. With a login.gov account, you can sign into multiple government websites (including SAM.gov) with the same username and password.

If you already have a login.gov account check the email address associated with it. If your current login.gov account matches the email address associated with your SAM.gov account, you are ready for the new login process. Otherwise, you will need to create a new login.gov account the first time you log in to SAM.gov after June 29, 2018.

Why do I need my current SAM.gov user account email address?

If you use any other email address to create your account at login.gov other than the one associated with your SAM.gov account, your SAM.gov roles will need to be reassigned. This could cause delays in updating your existing registrations.

How do I find the email address for my SAM.gov user account?

- If you don't know which email is associated with your SAM.gov user account, contact the supporting Federal Service Desk at www.fsd.gov, or by telephone at 866-606-8220 (toll free) or 334-206-7828 (internationally) Monday through Friday from 8 a.m. to 8 p.m. (ET), for FREE assistance.

What do I need to create my Login.gov user account?

Through SAM.gov, create a login.gov account (if you don't already have one). Your old SAM.gov username and password won't work anymore. You'll need to:

- **Create a login.gov account if you don't have one.** You only need to do this once.
- **If you have a login.gov account, check the email address.** - If you already have a login.gov account, the associated email address must match the email address associated with your SAM.gov account in order to migrate your roles. If the email addresses don't match, you'll need to create a new login.gov account.
- **If you don't have a login.gov account, enter an email address.** Use the same email address you use for SAM.gov. If you don't currently have a SAM.gov account (are a brand new user, for example), you may use any email address you have access to.
- **Create a new password.**

- **Pick how you want to receive security codes.** You need a working phone number (mobile or landline) or an authentication app (installed on your mobile or on your computer). Login.gov will use your phone or your authentication app to send you a one-time security code for authentication.

How do I sign into SAM.gov after I create my Login.gov account?

Every time you select "Log In" on SAM.gov, you'll go to the login.gov sign-in page. You need to enter your login.gov email address, password, and the one-time security code that you receive. You can tell login.gov to remember your browser which stores your security code for 30 days.

Why did SAM.gov make these user account changes?

- To further increase security and deter fraud, SAM.gov is partnering with login.gov to implement multi-factor authentication for registered SAM.gov users.

Does this change impact public users who do not log in to SAM.gov?

- No. There is no change for users who search and view public data on SAM.gov without logging in to the system.

Can I get help for this new login process?

- Yes. SAM.gov has additional instructions, the Federal Service Desk will be available to support, and you can go to login.gov to learn more about creating an account.

Alleged Fraudulent Activity in SAM

GSA has taken action to address alleged fraudulent activity in the System for Award Management (SAM). The measures GSA already put in place to help prevent improper activity in SAM include masking specific data elements in the entity registration even for authorized entity users; requiring "parent" approval of new registrations for their "child" entities; and requiring the formal appointment of the Entity Administrator by original, signed notarized letter.

Additional enhanced controls have been deployed. These controls include implementing multi-factor authentication using login.gov and notifying Entity Administrators when there is a change in the entity's bank account information.

NOTARIZED LETTER PROCESS CHANGES

How has the notarized letter review process changed?

All non-Federal entities who create or update their registration in SAM.gov will **no longer** need to have an approved Entity Administrator notarized letter on file before their registration is activated.

- *Hint*: This applies to you if your SAM.gov Purpose of Registration is either Federal Assistance or All Awards. Check SAM.gov to find your Purpose of Registration.
- All non-Federal entities still must mail the original, signed copy of the notarized letter to the Federal Service Desk.

Where can I find the notarized letter templates?

Read the instructions for domestic entities or instructions for international entities posted at the Federal Service Desk.

Where do I send the notarized letter?

You must mail the original, notarized letter to:

FEDERAL SERVICE DESK
ATTN: SAM.GOV REGISTRATION PROCESSING
460 INDUSTRIAL BLVD
LONDON, KY 40741-7285

Does the notarized letter requirement apply to U.S. Federal Government entities registering in SAM?

- No.

BACKGROUND

GSA's System for Award Management (SAM) continues to support an active investigation by the GSA Office of Inspector General (OIG) into alleged, third-party fraudulent activity in SAM. Only a limited number of entities registered in SAM were suspected of being impacted by this alleged fraudulent activity. In March 2018, GSA took steps to address this issue and notified affected entities. GSA continues to work with the OIG and law enforcement agencies to take additional action, as appropriate.

What has GSA been doing to address the problem?

GSA took a number of proactive steps to address this issue, including system modifications, to prevent improper activity going forward. In addition, GSA expired, then deactivated any entity registrations that appeared to have been affected. These entities were advised to validate their registration information in SAM, particularly their financial information and points of contact, before reactivating the entity registrations. Further, GSA has begun implementing additional reviews during the registration process to prevent future issues.

What interim changes were made to the SAM registration process?

These proactive steps include requiring submission of an original, signed notarized letter identifying the authorized Entity Administrator for the entity associated with the Data Universal Numbering System (DUNS) number. GSA posted instructions for domestic entities and instructions for international entities for easy reference. This requirement went into effect on March 22, 2018, for new entities registering in SAM and went into effect on April 27, 2018, for existing registrations being updated or renewed in SAM. For Federal Assistance only entities, changes went into effect on June 11, 2018 and for all entities on June 29, 2018.

Who was impacted?

Entities with registrations that appeared to be impacted were notified. Instructions were provided explaining how to validate registration information and how to reactivate the registration. In addition, entities whose bank account information for Electronic Fund Transfer (EFT) changed within the 12 months prior to March 2018 were notified. Although not associated with suspicious activity, these entities are required to validate their registration information, particularly their EFT information.

What is an entity?

In SAM, you, your company, business, or organization is referred to as an "entity." Individuals register themselves or their entity to do business with the U.S. Federal Government by completing the registration process in SAM.

What should entities registered in SAM do to protect themselves and confirm that their bank account information has not been changed?

Entities registered in SAM are advised to log into SAM and review their registration information, particularly their bank account information for Electronic Funds Transfer (EFT) on the financial information page. Contact the supporting Federal Service Desk at www.fsd.gov, or by telephone at 866-606-8220 (toll free) or 334-206-7828 (internationally) Monday through Friday from 8 a.m. to 8 p.m. (ET), for FREE assistance. Entities are responsible for ensuring that their information is current and correct in SAM in accordance with paragraph (b) of Federal Acquisition Regulation (FAR) clause 52.232-33 or Title 2 of the Code of Federal Regulations Part 25 (2 CFR § 25.310 and Appendix A), as applicable, and should routinely review such information for accuracy.

Who should entities contact if they find that payments due them from Federal agencies have been paid to a bank account other than their own?

If an entity suspects a payment due them from a Federal agency was paid to a bank account other than their own, they should contact the Federal Service Desk at www.fsd.gov, or by telephone at 866-606-8220 (toll free) or 334-206-7828 (internationally), Monday through Friday from 8 a.m. to 8 p.m. (ET), for FREE assistance.

Where can an international entity find information about the notarized letter process?

Entities not located in the U.S. or its outlying areas should read the international entity instructions posted at the Federal Service Desk that outline procedures and provide links to letter templates. If they have additional questions, international entities should contact the Federal Service Desk at www.fsd.gov, or by telephone at 866-606-8220 (toll free) or 334-206-7828 (internationally), Monday through Friday from 8 a.m. to 8 p.m. (ET), for FREE assistance.