GRANTS.GOV℠

FIND. APPLY. SUCCEED.℠

Security Build Overview

Applicants and Grantors

Updated September 13, 2010

Table of Contents

Security Build Overview
Applicants and Grantors

Background

The purpose of the Security Build for the Grants.gov system is for compliance with the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53A, recommended Security Controls for Federal Information Systems. The changes for the build will be available on October 11, 2010. These updates will not apply to System-to-System accounts.

1. Password Complexity Rules

When an applicant (Authorized Organization Representative (AOR)/Individual), E-Business Point of Contact (E-Biz POC) and/or a grantor, creates or changes a password in the Grants.gov system, the new password requirements will be enforced:

- Cannot be the same as the previous three (3) passwords
- Contain at least eight (8) characters
- Contain at least one (1) number
- Contain at least one (1) uppercase letter
- Contain one (1) lower case letter.

2. 90-Day Password Expiration Policy

A 90-day password expiration policy for accounts will be implemented.

Going forward all passwords will expire every 90 days. For example, if a password is changed today, it is considered as day one (1). This password will be valid for 90 calendar days and will not be valid on the 91st day onward. System impacts include browser login, applications and new email notifications.

BROWSER LOGIN

- All users who successfully log in to Grants.gov through the browser will receive a password expiration warning message starting 15 days before expiration. Grants.gov will display a countdown message of the number of days until the password expires or the password is changed.
- All users with an expired password will not be able to log in using the browser. Users can change the password by using the “Change My Password” button on the login page. Users will be able to log in after changing their password.

APPLICATIONS

- Applicants will not be able to submit their applications if the password has expired.
  - Applicants will receive an error message with instructions to change the password.
  - After changing the password applicants can submit the application immediately.

EMAIL NOTIFICATIONS

- All users will receive two (2) email notifications before the password expires.
  - The first email notification will be sent 15 days before the password expires.

  - The second email notification will be sent five (5) days before the password expires.

3. Account Lockout Procedure

Three (3) consecutive failed attempts at login or submission, over a period of five (5) minutes, will lock the account for 15 minutes.

BROWSER LOGIN

- All users who have a username and password and are locked out, will not be able to log in using the browser for 15 minutes.
  - After 15 minutes with no actions on the login page from the user, the user can log in to the system with a correct password.
  - All users will be able to unlock an account within 15 minutes by using the “Forgot My Password/Unlock My Account” or by requesting a system-generated password.

APPLICATIONS

- Applicants will not be able to submit their applications during the lockout period (15 minutes).
  - Applicants can unlock an account by using the “Forgot My Password/Unlock My Account” during the 15 minutes or by requesting a system generated password and submit immediately.
  - After waiting 15 minutes, applicants can submit the application using the correct password.

4. Changes To Maintaining User Profile

User profile updates will occur for grantors with manage agencies role, grantors and applicants.

GRANTOR WITH MANAGE AGENCIES ROLE
Grantors with “Manage Agencies” role will have read-only view to the profiles of other grantors in the same agency and sub agencies. Password, Secret Question and Secret Answer fields will not be visible on this page when a Grantor with “Manage Agencies” role views another Grantor’s profile.

The following fields will be displayed on this screen:

- First Name
- MI
- Last Name
- Job Title
- Agency Code
- Telephone
- Email
- Username.

GRANTOR VIEWING THEIR PROFILE
For grantor users, the following fields will be non-editable on the user profile maintenance page:

- Username
- Agency Enrollment code.

APPLICANT USERS
For applicant users, the following fields cannot be updated on the Manage My Profile page:

- Username
- DUNS.

BOTH APPLICANT AND GRANTOR
The following fields can be updated on the Manage My Profile page with a valid password:

- First Name
- MI
- Last Name
- Job Title
- Telephone
- Email
- Secret Question
- Secret Answer.

5. Change Password Option

The change password option will be implemented for grantor, E-Biz POC and applicant users. The change password request will challenge the requester by requiring entry and validation of the current password.

The change password option will be available on the login pages, as well as when the user logs in.

6. Enhance "I Forgot My Password"

Grantors and Applicants
On the newly titled "I Forgot My Password/Unlock My Account" page, a second option will be available if the user forgets the answer to the security question. The second option will allow the user to request the system to generate a password and automatically send the user an email with the password. The system will use the email address found in the user's profile.

E-Biz POC
On the "I Forgot My Password/Unlock My Account" page. Ebiz POC users can request the system to generate a password and automatically send the user an email with the password. The system will use the email address on file with Grants.gov.

7. Account Becomes Inactive After One (1) Year Of No Activity

Accounts that are inactive for one (1) calendar year will be deactivated. An inactive account is defined as having no login activity for one (1) year.

An email notification will be sent to the user starting four (4) weeks prior and continue every one (1) week informing the user that the account will become inactive. The username will be included in the email notification as well as a link to update the password.

AOR AND GRANTOR USERS
Once the account is inactive, the current role for AORs and role(s) for grantors will be removed and the user will not be able to access the system (roles are not assigned to E-Biz POC or individual applicant users). To reactivate an account, the user must change the password and the E-Biz POC, or the grantor super user must re-assign roles for the user requesting reactivation.

E-BIZ POC AND INDIVIDUAL USERS
Once the account is inactive, the user will not be able to access the system. To reactivate an account, the user must change the password.

8. Applicant Center Shortcut To Enable E-Business Point Of Contact (E-Biz POC) Functionality

An option will be available to the AOR to request E-Biz POC authorization once the AOR is logged into the Applicant Center. A prompt will be displayed for an MPIN the first time E-Biz POC functionality is selected. A valid MPIN must be entered at every session in order to be granted E-Biz POC authorization. Once a valid MPIN is entered the AOR can act as the E-Biz POC and perform the following functions:

- Issue AOR role(s)
- Revoke AOR role(s)
- View all submissions for the organization’s DUNS
- Deactivate AOR account(s)
- Revoke E-Biz POC role assigned to other AOR accounts.

If the AOR enters the correct MPIN at the Applicant Center, the AOR will begin to receive an E-Biz POC email notification when a new AOR registers under the organization’s Data Universal Number System (DUNS). If the AOR does not enter the correct MPIN they will not receive E-Biz POC email notifications until they enter a valid MPIN.

10. E-Business Point Of Contact (E-Biz POC) Account Login Update

When an existing E-Biz POC goes to log in for the first time after the Security Build is released, the E-Biz POC will enter the DUNS and for the Password field, enter MPIN. The system will immediately request the E-Biz POC to change the password and comply with the password complexity rules (see “1. Password complexity rules” on page two (2) for details).

Once this security control is implemented, when a new E-Biz POC account is established, a system-generated password will be sent in an email to be used to log in to the account. The new password will be sent to the CCR email address on file with Grants.gov.

Other Resources

Information to share with Grantor colleagues: www.grants.gov/securitybuildcomm.
Applicant specific information regarding the Security Build: www.grants.gov/securitybuild.
E-Biz POC specific information regarding the Security Build: www.grants.gov/securitycommebiz.

For more information about the Grants.gov process including finding grant opportunities, registration process and applying for a grant – review the Applicant User Guide, FAQs and find additional help by using the iPortal. All resources can be found at: http://www.grants.gov/help/help.jsp.