



GRANTS.GOV<sup>SM</sup>

FIND. APPLY. SUCCEED.<sup>SM</sup>

# **Security Build Overview**

## **Applicants and Grantors**

**October 20, 2009**

# Security Build Overview

Health and Human Services (HHS) is the partnering agency for Grants.gov. Certification & Assessment (C&A) on HHS systems are mandatory to obtain the Authority to Operate (ATO). The Grants.gov Program Management Office (PMO) completed a preliminary self assessment on the Grants.gov system. The following is a brief overview of the items that need to be addressed as part of that assessment. These items must be implemented in a system build prior to the formal C&A. The date for implementation of these items is to be determined, but is tentatively scheduled for the end of the 2<sup>nd</sup> quarter fiscal year 2010. As this is not a final document, some of the status of these items may change.

## 1. Password complexity rules

*(System-to-System accounts will not apply to this rule)*

When an applicant (AOR/Individual), E-Biz POC, and/or a grantor, create or change a password in the Grants.gov system, the new password requirements will be enforced. The requirements include:

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

## 2. (90) day password expiration policy

*(System-to-System accounts will not apply to this rule)*

A (90) day password expiration policy for accounts will be implemented. That is, if the password is changed today, it is considered as day one. This password will be valid for 90 calendar days and will not be valid on 91<sup>st</sup> day onward.

- Applicants will not be able to submit their applications if the password is expired
  - They will be able to change their password and resubmit immediately
- All users who have a username and password will not be able to login using the browser
  - All users will be able to change their password and login immediately

## 3. Account lock-out procedure

After three (3) consecutive failures over a period of five (5) minutes to enter a correct password the account shall be locked for (15) minutes.

- Applicants will not be able to submit their applications during the lockout period
  - Applicants can change their password and resubmit immediately
- All users who have a username and password will not be able to login using the browser
  - All users will be able to change their password and login immediately

## 4. Changes to User Profile maintenance interface to tighten security controls

*GRANTOR SUPER USERS*

Grantors with 'Manage Agencies' role will have read-only view to the profiles of other grantors in the same agency and sub agencies. The following fields will be displayed on this screen:

# Security Build Overview

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

Password, Secret Question and Secret Answer fields will not be available on this page when a Grantor with 'Manage Agencies' role, can view other grantor's profiles.

## *APPLICANT USERS*

For applicant users, the following fields will be non-editable on the user profile maintenance page:

- Username
- DUNS

## *GRANTOR USERS*

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

- Username
- Agency Enrollment code

## *BOTH APPLICANT AND GRANTOR*

The following fields are editable on user profile maintenance pages:

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

## **5. Change Password Option**

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

The change password option will be provided on the login pages and within the applicant and grantor center, and E-Biz POC page.

# Security Build Overview

## 6. Enhance Forgot Password

For users, on 'Forgot My Password/Unlock My Account' page, a second option for the user will be available if the user forgets their security answer. The second option will allow the user to request the system to generate a one-time use password and automatically send the user an email with the temporary password. The system will use the email address found in the user's profile.

## 7. Account Status update to prevent Grants.gov accounts from being recycled

Usernames will be unique across all accounts at Grants.gov. No user will be able to recreate a username that already exists in the system.

## 8. Account cleanup procedures triggered by (1) year of account inactivity

Accounts which are inactive for one (1) calendar year will become 'inactivated'. An email notification will be sent to the user starting (4) weeks prior and continue every (1) week notifying user of Grants.gov account cleanup policies and pending account status will change to inactive, due to account inactivity. The username will be included in the email.

An inactive account is defined as having no login activity. To reactivate an account users must change their password and be granted permissions by the E-Biz POC and/or the Grantor Super User.

## 9. Authorized Organization Representative (AOR) Applicant enhancements 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 valid MPIN must be entered in order to be granted E-BIZ authorization. The AOR shall re-validate authorization each time they login to their AOR account. If the E-Biz POC authorization is granted, the AOR will be granted with E-Biz POC role functionality. If the E-Biz POC authorization is not granted, the E-Biz POC functionality will be revoked.

If the AOR account is granted the E-Biz POC role, the account owner can perform E-Biz POC functionality. These functionalities are available to all AORs who have the AOR role assigned. When a user selects the E-Biz POC links they will be prompted for an MPIN the first time an E-Biz POC link is selected. If the MPIN is correctly entered they will be granted access to the E-Biz POC links.

# Security Build Overview

## 10. Security controls for the E-Business Point of Contact (E-BIZ POC) account

MPIN will no longer be used as the password for E-Biz POC account login. The account will continue to use DUNS for the username. However, once this security control is implemented, during the process of setting up the E-Biz POC account, a temporary one-time use password will be used to create an account. The temporary password will be sent to the CCR email address on file with Grants.gov. Then the user will be forced to change the password upon login.