NFC Agency Security Officer User Group Meeting
Wednesday, November 13, 2013 – 10:00 a.m. – 11:30 a.m. Central Time
Meeting Notes

The meeting was opened and it was announced that the presentation could be found at https://www.nfc.usda.gov/Security/user_group.html. Participants were asked to place their phones on mute, and send their name and agency information to AMB via the Notes tab; however, several callers had to be muted by the presenter during the call due to taking calls that could be heard by all participants during the webinar. Approximately 112 individuals participated in the webinar.

Performance Metrics:

Metrics for the fiscal year beginning October 2012 and September 2013 were presented. The average number of days to process 9,873 requests received, of all types, was 8.54 days. One thousand fifteen expedited requests, which have been declining in number, and are expected to continue to decline, were completed in an average of 7.89 days. New Service Level Agreements (SLAs) will be used for the current fiscal year, and will consider number of userIDs on the request and complexity of the request for the estimated completion date.

Access Updates:

When re-establishing accounts after they have been deleted due to inactivity, ASOs should choose the 'CREATE ID…' summary option in Remedy Requester Console, instead of using the 'MODIFY ID…' option. When accounts have been deleted due to inactivity, all traces of the previous access have been removed; therefore, the UserID must be created as if a new employee account is being established.

ASOs were reminded to extend access for year-end account expirations timely to ensure that users do not lose their access.

The various types of requests that make up Simple, Moderate and Complex requests were provided.

AMB Team:

Names of AMB Team members were provided.

ASO Best Practices:

A notification by Joanne Nelson at AMS to users in her agency was provided as a good example of how ASOs should manage the inactive accounts process.

Project Updates:

- **Access Forms**:   The various forms available and the advantages of using them were provided. Agencies can use their own forms if they already have developed one. Reporting Center and SALL access will be automatically granted to ASOs when their AD-3100-A, Agency Security Officer Designation Form is processed. Section numbering on the AD-3100-R, Reporting Center Request for Security Access Form will be corrected (there were two Section 6's). A block to add Profile Name will be added to the

AD-3100-P, Payroll Personnel Request For Security Access.

- **Role Based Security**: Role Based Security is a method of regulating access to computer or network resources based on the roles of individual users within an enterprise. Agencies will develop their roles, or profiles, based on the user's need to know specific types of information, ensuring that the role contains the least privilege necessary for the job function, and that separation of duties are considered to prevent a user from having authority to perform functions in which he/she could conceal fraudulent activity without proper approvals. The benefits of Role Based Security were provided, as well as some typical roles that agencies might consider when developing their profiles. Agency and AMB responsibilities were also discussed. As each agency is implemented, they will receive a detailed timeline. Agencies who are interested in moving forward should send an email to AMB (nfc.aso@nfc.usda.gov), after they have an idea of what roles will be required.

- **Scheduling Software**: AMB is still in the process of implementing software to allow users to self-register for courses. More information will follow.

- **Inactive Accounts Email Notification**: AMB is working with GESD to develop a process to notify users when their NFC system accounts have been inactive for 30 days, and when they have been disabled due to 60 days of inactivity. More information will be provided as it becomes available.

- **Electronic Forms Entry**: Development of paper access forms is a first step in developing an electronic forms entry system. AMB will now monitor usage of the forms to determine what changes are needed.

Action Items:

1. AMB will update the forms with changes identified during the ASO User Group Meeting.
2. Agencies will review their current profiles and identify where the access can be streamlined into defined roles.
3. AMB will post notes from the August 2013 ASO User Group Meeting (as well as the November 2013 ASO User Group Meeting) on the NFC web site.
4. AMB will research adding a Comments or Remarks field to the Security Access Forms.

Questions & Answers

1. **Can data on the forms be saved?** No, the data on the forms cannot be saved. This will ensure that ASOs make conscious decisions about the access being requested and do not inadvertently request access for a user that was left over from another user's request.
2. **Can data on the forms be printed?** Yes, after the form is filled out, it can be printed with all of the data entered.
3. **When will NFC discontinue use of Social Security Numbers on security access request forms?** NFC has no plans to discontinue use of SSNs. SSNs are the only way to uniquely identify users and cross reference security records to those in other NFC systems.
4. **Can agencies continue to use their own access forms?** Yes.

5. **Will a detailed project plan for Role Based Security implementation be provided?** Yes, as each agency is implemented, a project plan with tasks, durations, start and end dates, responsible groups, and dependencies will be provided.
6. **Do forms have to be encrypted in Remedy Requester Console if they contain an SSN?** Yes. Unencrypted forms containing PII data (SSN) will be deleted by AMB and will have to be resubmitted by the ASO. For instructions on how to encrypt documents, please refer to [How To Encrypt a File using Windows Explorer and WinZip For Use With All PII Data.](#)
7. **I don't have 'CREATE ID…' in the Drop Down List in Remedy. Can someone please call me?** AMB responded and the option is available.