

NFC Agency Security Officer User Group Meeting
Wednesday, February 12 – 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. Approximately 119 individuals participated in the webinar. There were far fewer incidents of background noise during this webinar as there were in past webinars. Participants were encouraged to ask questions throughout the webinar, as opposed to at the end only, and this allowed the presentation to flow more smoothly and allow more questions to be addressed. The following topics were discussed.

Performance Metrics:

Metrics for the fiscal year beginning October 2013 and December 2013 were presented. The Service Level Agreement was not met during this period due to the backlog of requests resulting from the Furlough in October, 2013. NFC has taken action to remove the backlog, including modification of work schedules and expanding daily monitoring. (As a result, there was almost a 70% increase in the number requests processed in January over both November and December.) Although the number of requests received in December did not increase significantly over the number of requests received in prior months, there was a significant increase in the number of UserIDs processed during December and January (up to 53% more UserIDs processed in December). There was an 86% surge in the number of High Priority requests from November to December; and a 23% increase in the number of Expedited requests from November to December. The increasing numbers of these types of requests pose a risk to adequately managing workload and ensuring that all customers are served equitably.

Access Updates:

ASOs were encouraged to take a number of suggested actions to improve access management. Users who utilize Reporting Center only (no mainframe applications), should send a request to be placed in a 'Reporting Center Only' department in TopSecret. The EOS output management tool will be decommissioned, and anyone using the EOSEVT1 SESSID will need to use the CTMS (Control-D) SESSID to access mainframe reports. Details and timelines for testing were provided. Internal audits of the Reporting Center and Insight applications are underway. ASOs may receive access reports to review and should submit access requests via Remedy Requester Console to make required changes.

ASO Best Practices:

A notification by Kimberly Sherlock Drayer of Treasury to users in her agency was provided as a good example of how ASOs should manage the audit review process.

Role Based Security:

Role Based Security will eventually be implemented for all agencies serviced by NFC. Those agencies undergoing mandated reorganizations will receive priority, followed by small agencies, then larger agencies and those with more complex requirements, such as servicing other agencies. A list of current agencies being implemented or in consideration were provided, along with a basic implementation plan that will be refined as necessary, after each agency

implementation.

Access Forms:

Participants were encouraged to use NFC (or agency forms) to prevent errors, which can delay processing. Incomplete or inaccurate forms will not be calculated within SLA metrics. Detailed changes to forms were discussed. If a request is submitted for multiple agencies (agencies who service other agencies), EACH agency should be listed on the form or notated in the Notes field within Remedy Requester Console.

Annual ASO Verification:

ASOs should respond to notices to be distributed via GovDelivery in the near future to indicate changes among ASOs.

Training Update:

Changes in the ASO course curriculum were discussed, as well as how to register on the website for available courses and ASO User Group Meetings, and complete evaluation forms.

Wrap Up:

A recap of action items was provided. The next ASO User Group Meeting will be held on May 14, 2014.

Action Items:

1. AMB will develop a form to request access reports to ensure that all required information is provided.
2. AMB will update the training registration software to include dial in information for the ASO User
3. Agencies will review their current profiles and identify where the access can be streamlined into defined roles.
4. AMB will research why the only data from some payroll personnel reports is from last year.
5. AMB will distribute basic roles and role based security information to agencies.

Questions & Answers

1. **I have flagged requests in Remedy Requestor Console at the 'Critical' level. I rechecked a few of these requests and they were changed to low priority. Why?**
The initial level you put on a request is overwritten when the request is verified for completeness and accuracy. Requests are not marked critical unless an email is sent to nfc.aso@usda.gov to request it be expedited. If the ticket is **not yet past its target completion date**, NFC must give approval to expedite; otherwise, no approval needed.
2. What is the difference between High Priority and Expedites?
High Priority requests are those that are automatically placed at a higher level of processing than routine requests. Examples are CUAT requests, and time-sensitive projects.
3. How should EmpowHR password resets be submitted.
Password resets should be submitted to osc.etix@usda.gov. All other requests for

adding, modifying or deleting access should be submitted via Remedy Requester Console.

4. Can requests for new employees be expedited?
Requests for new employees can be expedited if the need exists; however, we encourage you to submit new employee access requests at least one week before they report for duty to ensure that they receive access when needed.
5. How early can requests for new employees be submitted?
Requests for new employees should be submitted no earlier than two weeks before and no later than one week before a new employee reports for duty.
6. Why am I required to sign on to the mainframe? I don't reset passwords – I only submit requests.
The mainframe is our central point for storing user accounts. To ensure that we have a valid database of active ASOs, you should log on at least every 30 days to keep your account active, and to maintain your status as an ASO. Users who do not use mainframe applications should be in a profile that contains no mainframe access so that they will not be required to log on to the mainframe every 30 days.
7. Payroll/Personnel reports in Reporting Center are reflecting old data. Why?
NFC will investigate this.
8. Is Role Based Security Access mandatory?
Role Based Security access is strongly recommended, but not yet mandatory.
9. How will you let agencies know when to begin Role Based Security Access implementation?
AMB will contact agencies after mandatory implementation of agencies undergoing organizational realignments.
10. FEC is a small agency. How can we join Role Based Security implementation and how long will it take?
Implementation for agencies will take place first for mandatory implementations, then small agencies. Implementations vary based on the size of the organization and the complexity of the access required. A time frame for completion will be negotiated for each agency.
11. How can I attach multiple documents to my request in Remedy Requester Console?
You may attach multiple documents by saving your request, then attaching documents to multiple Work Info entries. (Refer to training materials for more information.)
12. How do I follow up on Remedy Requester Console status?
The status is provided within the Work Info section of the ticket.