

Nina and George,

April 23, 2003

In the enclosed package, we include all the non-FSA specific C&A requirements and associated test procedures. Bob Ingwalson's team has reviewed them and made suggestions for improvement.

We recommend having your team perform a similar review and add your changes. We evaluated using the following criteria:

- Does the security requirement make sense and is it phrased clearly?
- Does the test methodology (I,O,T,D) make sense for a tier 3 or 4 system?
- Does the test procedure make sense and will it allow the CRG to validate the effective operation of the security control?

We defined the security tests - Interview, Observation, Test, Documentation - using 800-26 as our guide:

- Documentation: Does the system have procedures requiring the system to implement the security requirement?
- Interview: The test procedure should ask the appropriate person(s) whether the security requirement is effectively implemented.
- Observation: A security requirement that can be evaluated by physically viewing/observing the security control in operation.
- Test: a) A qualitative review of documentation to discover evidence that the security requirement is implemented appropriately (example – The requirement states that the system must maintain an up-to-date list of users. The test could be for the CRG to request for a list of users and verify that no expired user accounts exist in the system. Example 2 - A requirement may ask for a Disaster Recovery Plan. The test could be a requirement for the CRG to request a copy of the DRP and verify its existence.)  
b) A technical evaluation of a security requirement (example: Passwords must be alpha numeric. The test could be a requirement for the CRG to create a password with all alpha characters and verify that the password is denied.)

Additionally, in our Master list of requirements, including both FSA and non-FSA requirements, we have categorized them into 800-18/800-26 categories. In your copy, they are not divided. We suggest incorporating your comments and then giving them back to us to update with the Master list. We will then eliminate any FSA duplicates with ED documents and prepare the requirements for submission to Telos/Xacta through OCIO.

Happy Reading,

FSA Security and Privacy Team