From: Sandy Bacik
Sent: Thursday, June 09, 2011 8:18 AM
To: csctgtesting@nist.gov
Subject: CSWG Testing & Certification minutes from 20110607

All links were tested in this email before it was sent. If I have missed anyone on the attendance, please let me know. My Outlook is not liking some of my fonts, so I apologize if the font size varies in the email.

Our twiki site:
http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/CSCTGTesting
Co-Leads: Nelson Hastings (nelson.hastings@nist.gov), Sandy Bacik (sandy.bacik@enernex.com)

20110607 Minutes
1. Open Items
a. Reviewing and updating the assessment objectives spreadsheet:
http://collaborate.nist.gov/twiki-sggrid/pub/SmartGrid/CSCTGTesting/Assessment-Sample-Matrix-v0p4.xls

i. We still need additional volunteers to assist in writing assessment objectives.
ii. We started a review of the "Assessment Objectives" tabs and the "Assessment Objective" column.
1. The content of the SG.AC has too brief of assessment objectives and need to be updated using the SP800-53a. Sandy will work on this for next Tuesday.
2. SG.AT-1 is in a good format, but Supplemental Guidance should not be included. Sandy will work on this modification for next Tuesday.
3. SG.IA-1 is also a good format, but the Supplemental Guidance and Additional considerations should not be included. Sandy will work on this modification for next Tuesday.
iii. We want the assessment objective written in the NIST SP800-53a format.
iv. We want the main portion of the NISTIR 7628 requirement and the requirement enhancement included in the assessment objective. The supplemental guidance and additional consideration of the NISTIR 7628 requirement will be part of the assessment case later in our development.
b. We will be working on developing the assessment cases and requirements at a later date and the format will be discussed at this time.
i. As we move forward we will discuss the detail level, such as requirements for a bronze, silver, or gold level to put it in context of the assessment scope. The assurance level will be after we completed after the assessment objectives.
c. The maturity of this and future documents will improve over time, such as CMM that Rick Sheldon had mentioned on the call.
d. Scott Shorter asked about the CSWG Risk Management framework and how it would fit into this process. Marianne Swanson relayed some of the response of the selecting controls based on the mission with the CIA and the high, moderate, low level and that is within the Federal government. We need to have a baseline, and the utilities can use compensating controls to mitigate or accept the risk.

e. In the future we will need to define the maturity levels (what are you doing) and the assurance level (degree to which it is being examined) and this will be based on the criticality of the system. We discussed that maturity is how far along the path to compliance or how well is the process being met. We discussed that assurance is about the level of confidence. We need to consider both of these as we proceed.
f. Along with documenting the process of our development, we will want to add a lessons learned to the document. In the future when a test program is implemented we will need to determine how to keep a lessons learned throughout the testing.
2. Attendees
a. Don Weber
b. Douglas McGinnis
c. Gio Gallo
d. Jose Guzman
e. Marianne Swanson
f. Mark Freund
g. Michaela Iorga
h. Mike Ahmadi
i. Nelson Hastings
j. Richard Scott
k. Rick Sheldon
l. Sandy Bacik
m. Scott Shorter
n. Shrinath Eswarahally

Regards,
Sandy Bacik, CISSP, CISM, ISSMP, CGEIT
Principal Consultant
EnerNeX
p: 865.696.4470
e: sandy.bacik@enernex.com // www.enernex.com