From: csctgtesting@nist.gov on behalf of Sandy Bacik [sandy.bacik@enernex.com]
Sent: Tuesday, April 12, 2011 2:29 PM
To: Multiple recipients of list
Subject: CSWG Testing & Certification minutes from 20110412

Thank you everyone for your participation on our call Tuesday. good discussion. All links were tested in this email before it was sent. If I have missed anything or anyone on the attendance, please let me know.

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)

20110412 Minutes
1. Current activities
a. Please perform a final review of the RFP security testing questions (http://collaborate.nist.gov/twiki-sggrid/pub/SmartGrid/CSCTGTesting/CSWG_TCC-Brainstorm-RFPQuestionsSecurityTesting-v1p3.doc)
and in the near future we will issue this as an SGIP document
b. We talked about using the NIST SP800-53a framework document to write our testing requirements
i. Concerns were raised that SP800-53a is for system-wide assessment of security controls and not product testing. We will need to look at a higher certification and accreditation framework - the SGTCC is looking into this.
ii. We will be using the NIST SP800-53a framework for writing the test requirements for the NISTIR 7628 version 1.0, because the NISTIR 7628 are at a system and higher level than technical controls.
iii. Within SP800-53a, there are three methods that can be used to make the test determination: (1) examine consists of reviewing, inspecting, observing, studying or analyzing objects (specifications, mechanisms, procedures, etc.); (2) interview consists of holding discussions with individuals or groups of individuals within an organization; and (3) test consists of exercising one. We will use these three methods for the NISTIR 7628 high level cybersecurity requirements.
iv. We will write test objectives for each NISTIR 7628 requirement.
v. When we have to write testing requirements for products and have stronger product technical requirements we will review using the SP800-53a and the common criteria evaluation assurance levels (EAL s).
c. We started the discussion on how to write our testing requirements, which we will potentially refine in the future
i. The term “shall” means the requirement is required.
ii. The term “should” means the requirement is optional.
iii. The requirement shall be

positively stated, whenever possible.

iv. The requirement shall contain one and only one action and may have many condition.

2. Open discussion

a. Gio Gallo distributed with permission of Wurldtech Security Technologies(WST) and OPUS Consulting Group (OCG) the WIB 2.0 – NISTIR 7628 Alignment analysis summary document and workbook prepared by OCG for WST last month. We will see get Dennis Holstein to give an overview of the WIB in a future meeting.

b. Clarification of the CSWG TCC relationship to the SGIP Testing and Certification Committee (SGTCC). The SGTCC twiki site is here: http://collaborate.nist.gov/twiki-sggrid/bin/view/SmartGrid/SmartGridTestingAndCertificationCommittee. A separate email will be sent on how our work integrated into the SGTCC.

3. Attendees

a. Aaron Gomez
b. Brian Monkman
c. Don Weber
d. Ernie Hayden
e. Gio Gallo
f. Mark Freund
g.Michaela Iorga
h. Mike Ahmadi
i. Nelson Hastings
j. Richard Bockenek
k. Rick Shelton
l. Sandy Bacik
m. Scott Shorter
n. Shrinath Eswarahally
o. Vicky Yan

Regards,

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