

CSWG / NIST Smart Grid Users Guide Subgroup

November 02, 2012

Attendance:

- Mark Ellison (co-lead)
- Craig Rosen (co-lead)
- Vicki Pilliteri
- Neil Greenfield
- Reynaldo de Leon
- Tim Alrich
- Amanda Stallings
- Jody Fraser

Discussion about inputs during GridSec Summit 2012; Mark Ellison and Craig Rosen discussed.

Action item: Craig Rosen to review materials received and to bring feedback to the team during next meeting.

The meeting primarily covered Neil Greenfield and Mark Ellison's comments to the draft as provided to the team.

Section 1 – Executive Summary – Question focused on whether to use the term tool or methodology. Neil noted that the term tool gets overused; Craig Rosen noted that the NISTR provides the methodology already; one of the intents of the user guide is to align with the NISTR rather than deviate from it, and the tool concept avoids conflict with this alignment.

Section 2 – Scope – The team discussed the term “security requirements” versus “controls.” The team preference expressed was use the term “requirements” to align to NISTR and terminology that the NISTR uses to avoid confusion. The consensus was to remove verbiage of “easy to follow” in the context that the team is applying judgment by doing so.

Identify threats and vulnerabilities inserted into Section 2 - Scope; team discussed, and came to concurrence that organizations may have different ways to approach or interpret, outside of leveraging the RMP. The team agreed that leaving out the comment leaves more flexibility.

Section 4 – Identify Smart Grid Processes – The team discusses initial recommendation for rejecting the insertion of added verbiage in paragraph A, since the topic is dealt with in more detail in Section 7; additional feedback is that it is better to introduce initial detail early. The team concurred that the approach of the document was to increase the granularity in progressing through the document. The team chose to add a footnote regarding adding additional management in the Risk Management Governance Team.

Section 4, Paragraph B - the team consensus was on clarifying high risk elements. Wording was added through this subsection. Team discussed terminology of “high risk” and “priority business functions.”

Section 5 – Identify Systems That Support the Business Processes - Typos and editorial updates were accepted by the team through Paragraphs A and B, and made by concurrence of the team. The red text was added in by Mark Ellison to facilitate discussion at GridSec 2012 Summit; the text is no longer needed, and was removed during today’s meeting.

Section 6 – Map Systems to Logical Interfaces – Removed the red text; this was added by Mark Ellison in preparation for GridSec 2012 Summit, and is no longer needed. Typos and editorial updates from Neil accepted into the document.

Section 7 – Identify Assets Associated with the High Risk Systems - Neil’s editorial comments are accepted. Under Paragraph B, Firmware – Mark’s addition of “type” and “version” is accepted by concurrence from the team. Changed “Associated System” to “System,” and moved to top of the bullet list to align with how the fields of the table are set up.

Action Item: The team made a note to itself that it needs to create an example spreadsheet here.

Section 8 – Identify System and Asset Requirements - Removed the red; this was again added by Mark Ellison in preparation for GridSec 2012 Summit, and is no longer needed. The term “high risk” was added under Paragraph A. The team discussed how to map three impact rating values, to a single set; the discussion involves the high-water mark, alignment with the NISTR. The team referenced page 64 (Figure 2-21) NIST 7628 Guidelines for Smart Grid Cyber Security v1.0 in this discussion, and subsequently page 79 (Table 3-3). The team reached concurrence, but also noted that this is one of the areas of the “meat” of the user guide, where the team needs to “click down into” the content in more detail for the benefit of the reader. Section 8, Paragraph B was highlighted. Team commentary that once the reader arrives at the recommended levels of CIA from the NISTR, and does their own analysis, but subsequently finds out if their individual levels of CIA are lower, they will then need to circle back around and double-check their analysis, rather than simply trusting their instincts. If there is a major divergence in the results of the risk analysis between recommendations and the results of the reader’s analysis, then this is the point to “double click” down into Volume 3 of the NISTR. There was team concurrence on this note.

Section 1 – Scope – There was additional verbiage incorporated into the draft to complement the updates made throughout the document during the team’s session today.

General Team Administration:

Next meeting will be scheduled one week out with the intent to get the team and the user guide activity back in sync. Thereafter, the team aligns back into the 2 week cycles.

Next call: Friday, November 09, 2012; 2:00pm Eastern; team meetings will resume their normal 2-week cadence thereafter.