

CSWG / NIST Smart Grid Users Guide Subgroup

August 31, 2012

Attendance:

- Craig Rosen (lead)
- Mark Ellison (lead)
- Marianne Swanson
- Amanda Stallings
- Scott Saunders
- Seth Bromberger
- Victoria Pillitteri
- Jody Fraser

Draft document - Team member made some updates, beginning with page 5 to identify smart grid function. That team member has also eliminated some of the comments that have made the content busy; added notes to sections 3 through 6.

In review of the mark-ups, the team considers the references placed in each of the sections, top and bottom, guiding the reader to where they can find actionable information. Scott suggests that whether the references are top, bottom or in the middle of the content, that the references are specific to actionable information.

Action item: Craft an introduction of how the links/references will guide the reader to action information and references. Place it perhaps in the executive summary or somewhere in the document in the front at a high-level and throughout the document as necessary.

Draft document Section 5 – reviewing the mark-ups. There is some discussion around the use of “mission critical.” This was removed as a continuing action item from the previous meeting. Craig brings up the point that for a reader flowing from Section 5 to Section 6, does the team need to add some guidance for when an entity doesn’t have data for every one of these elements in the bullet points? The team wants to avoid situations where the entity will abandon the document because an organization doesn’t have the full complement of elements.

Draft document Section 6b – Indicate which data elements and artifacts an organization may include or which it might include; that is, what is useful at this point, and what is necessary to continue with the process. Team members agree that an organization would want to have this information. An organization might currently have all of this information, but may not, depending on the entity. As examples, MAC addresses will change with hardware lifecycle activities; IP addresses may change automatically. An organization doesn’t necessarily need to have a MAC or IP address to identify or the S/N (these are good for asset management) – but the entity does need to know what asset is, what the asset’s job is. Craig wants the team to ensure that it sifts the wording to be inclusive so that the team’s work doesn’t alienate a class of entities who might be reading and using this

document. Marianne provides guidance in footnote. Another team member indicates that we mark these elements with asterisk as optimal items, but not critical for successful execution. Is the team in accord with solely putting asterisks next to and then adding a footnote? Another team member comments to avoid wording such as must and need, in order to avoid this being perceived as a requirements document. In wording, there is the suggestion to use terms such as logical addresses and physical addresses, then provide examples of these categories for each.

There is discussion about logical addresses and IP addresses, and how to approach Section 6 on usability. The team can see appending some forms and templates to the back of this document to provide the reader with tools to implement this approach.

Scott Saunders presents an opposing view, trying to approach with the idea of smaller entities in mind. Some of this data might not be obviously useful at this step, that the team begin getting the reader thinking about what they can use this data for in subsequent activities, going to the next level, or subsequent steps in the processes.

A question is posed: Does the team want to add another entry in Section 5 for firmware? The team doesn't want to just write something down to write something down. Each of these elements that the document is asking the reader to list should have some correlation to a useful activity that the document is subsequently asking the reader to execute.

Draft document Section 7 Logical and Physical Interfaces – These diagrams are definitely logical. Craig indicates that here the team needs to definitely guide the reader by giving specific guidance. That is, provide specific guidance how to approach the task and process – place the diagram on their right, and what data elements on their left, and detail how to approach the analysis and process. In this guide, the team is going to instruct and mentor the reader through the steps of analysis.

This logical diagram is really intimidating, even to a reader with a significant amount of technical background and understanding. Also, from a color coding perspective, it's important to understand what's applicable to your organization, from a business perspective. From that color perspective, an entity can then disregard anything inapplicable to its business. For example, if an entity engages in transmission, but not in generation, then there are color codings that it can potentially ignore.

At some point there are suggestions in this document that talk about the level of risk, and if the team can take this document and somehow identify the red, orange, yellow – heat with levels of risk associated with them. In addition, if there are aspects of the CIA model, then for security requirements perspective, as a security practitioner conducting a risk assessment, an individual can quickly assemble a deck of prioritized risks and interfaces on which to focus.

The team needs to provide a connection between what the reader is looking at in NISTR 7528 logical diagrams and refer them to the correct pages, how to look at things, and how to approach them.

There is a suggestion to the team, to take a use case and walk through it, and work it out. Talk the reader through the big NISTR diagram and what the reader will need to do.

Action item: Take a use case, and map this out. Agenda item for next meeting is to walk through this.

Will there be a couple of people who could take this use case, and put together some use case slides for next meeting?

Is there a set of NIST slides? There is a comment is that these are too high level. However, there was another set that was done would be fantastic; however, this was for a client, so the logistics of that will have to be worked out, and the artifacts sanitized. The team will help them identify applicable security requirements from that case, and made the requirements practical, and applied them.

Action item: Check about the availability of these client-produced slides.

There is discussion about the intent and action of sections 7 through 9. What the team is looking for is more pragmatic than prescriptive guidance to get them going.

Action item: Work through with Marianne over the next couple of weeks to develop these steps for a straw man.

There is an inquiry and action item to identify availability of stakeholders for next Friday 09/07 and Wed/Fri. The team members should communicate with email with annotations to documents. This appears to be a three-some for action.

NIST slides will be distributed out to the whole group. What the team writes, it needs to do step-by-step for the benefit of the reader. In parallel there will be team work on the primary document. The team will work in parallel on the two deliverables.

Next call: Friday, September 14, 2012; 2:00pm Eastern