

CSWG / NIST Smart Grid User's Guide Subgroup

February 22, 2013

Duration 10:00 am – 12 noon

Attendance:

- Craig Rosen (co-lead)
- Scott Saunders
- Marianne Swanson
- Vicky Pillitteri
- Neil Greenfield
- Irene Gasko
- Leonard Jacobs
- Frances Cleveland
- Tanya Brewer
- Jody Fraser

Summary Overview

During the session, the Scott led a walkthrough of the significant updates he and Vicki Pillitteri had made to the draft of the User's Guide, including their reasoning and intent. The team provided feedback during the course of the walkthrough. At the conclusion of the session, the team agreed that the User's Guide had reached a point where there were some final action items to complete a review draft. As a consequence, the team should adjust its approach to drive to an agreed schedule and goal, with action items and deadlines for content/deliverables, aggregation of updates, edits, and next meeting date/time.

Detail of Session

Section 1.1, Scott described his approach to the changes implemented: references are named throughout the document; the term "artifacts" is used to imply the potential permanence of what the reader is creating; content, such as page 7, is tied to the RMP. The updates now reflect risk management and risk framing, which are all activities that one would expect of executives. On page 8, bullets reappear throughout the document, but differ in their context, in each case; in the business context, an organization would not be addressing the same loss of functionality as it would be at the technical layers but, rather, it would be speaking to it at another aspect. The executives create the first artifact as part of the risk ranking.

Scott placed call-out boxes throughout the document where salient points are made, important and repeatable concepts are notable. Step 2.5 sets the stage of subsequent activities, and sets the priority of the functions that lead; these include, mission and business processes that support, identification of the system assets that support each of those mission, and business processes.

Scott suggested that since you have all the right parties involved in inventorying the assets, then you need to accomplish multiple activities at once in data gathering, which will be used later on in the processes.

At this point, the reader will create the system inventory spreadsheet, identify the business processes that inherent with the business functions. These are on page 11, as presented in table 4.

In Section 4, the guide's organizational risk tolerance commentary needs to stay with the discussion on impact rating; in tandem, tie that comment back to the activities occurring with the technical SMEs and the executive staff. In some instances, other staff may be able to provide the previous set of stakeholders with identification and detail regarding risks of which they are not aware. Within Section 4, the user will make sure impact is in line as well. Step 4.5 addresses the asset inventory spreadsheet.

Section 5 is on page 12, and bounces right into the NISTIR mapping the systems to the logical interface categories. If we're pulling information together, then the tables are a much more direct way of conveying that information. Depending on the expertise and talent level, the reader might feel more comfortable with leveraging the NISTIR, or might feel more comfortable going directly to the logical interface diagrams; therefore, the team left that flexibility in the approach. A new column of "Actors" was added in Table 5; note that, through Section 5, the user will be gathering a whole lot of requirements.

Referring to Section 6, and specifically on page 15, table 6 is now a built-out table rather than a skeleton. The team brought forth to discussion common circumstances where a company has a different CIA risk level than what is presented as default. The user will need to compare what the NISTIR has versus what is specific to his organization. In this step, we're syncing up and review, because you will need that final step to move forward.

Vicki and Scott note that under HLR they will continue discussion regarding CIA impact levels and organizational specific fine-tuning.

Irene noted that there are some questions regarding security "requirements" and using some other term that doesn't imply requirements or mandatory activity. Irene would like to use the term "controls," with further discussion regarding why it was used in NIST SP 800-53 but not in this User's Guide. Scott underscored that he purposely approached with the intent of using the same terms as in the existing NISTIR guides. Leonard offered to craft some language for a footnote about difference in requirements, recommendations, countermeasures, controls. Irene would also like a poll as to how many people believe that use of the term "requirements" presents a potential problem.

In Step 6.3, updates to the User's Guide included adding another column, which are the GRC requirements. Scott noted that in the NISTIR, there are a lot of pages between 90 and 209; he inquired if it would be useful to put together a table for an appendix. Scott volunteered to do it to craft an appendix.

Scott noted that Steps 6.3 through Steps 6.5 include assets covered in Section 4, so the user will want to tie those two together.

Under page 15 and table 6 with the system inventory, Scott stepped the team through the process of evaluating the requirements. The result is a gap analysis, upon which the User's Guide sends the reader to two different guides in conducting a gap analysis of the security requirements.

Moving to page 16, table 8 – a column was added to table 8 called "Assessment Gaps," as well as a column called "Mitigations," which prompts to include what the user confirmed, and what wasn't confirmed.

Page 17, Table 8 discusses remediation, including classic aspects such as when the cost of the mitigation or control exceeds the cost of the risk/impact. Craig noted that it's equally important to note why you're doing something as why you are not doing something.

In Step 8.1, the User's Guide has added an activity called Risk Mitigation and has provided a short explanation. The User's Guide previously offered risk acceptance as the only option. However, Scott noted that there are a number of options or combinations of things an organization can do including accept, transfer, mitigate, etc. Here the User's Guide talks about a combination of risk response, especially in the highly regulated world of energy industry. Craig discussed some of the practical aspects of evaluating and presenting potential risk responses to decision-makers. Craig took the action item to write some content for Section 8 regarding risk response approaches.

In reference to Section 8, Scott discussed that this is not the area where the guide should discuss CIA, as that was already covered. Instead, we cover here the impacts to the organization. Here the same terms of threats, vulnerabilities, etc. are being used but in a different context because here we're speaking to business aspects of those same terms. Further, we couch the discussion of guiding the reader in determining how to approach the prioritization unique to their organization.

Moving to Step 8.5, page 19, Scott noted that this section might need a more work from an implementation plan perspective. The text was originally drafted by Jody; Jody will take the action item of providing more content on this. Scott suggested breaking out more steps, with bite-sized pieces that anyone could implement.

Proceeding on to Section 9, monitoring risk – Craig indicated that not all organizations understand that they are now entering a monitoring phase. It is important for each organization to develop some sort of cadence; otherwise, it gets stale pretty quick. The User's Guide should provide some advice on approaching the lifecycle, and maintaining the relevance and viability of the process. The worry and fear is that it is going to become static, as organizations complete all the hard work. The User's Guide should also give some guidance on how to develop the cadence, and enlisting the continued support to maintain it. Scott presented the suggestion of leveraging the RMP to provide more detail, create an artifact as part of the processes under the User's Guide, and get the reader to establish an initial entry into cadence leveraging that artifact. If the User's Guide can present this effectively, it would provide a balance to the entire document. Irene suggested leveraging existing organizational processes such as change management. Craig agreed that it is a good spot, but provided caution about organizations delegating the resolution under the broad category of "change management." Scott noted that it might be more appropriate to piggyback the processes on existing operational, program, and technical controls; there is a lot of variability to it, but ultimately the intent is to have an organization document its strategy and implement it for continuous operation.

Frances noted that all of this may be complicated when managing external third parties. Scott inquired if during the first time around, the organization will be identifying that some of its business processes and assets overlap or reside with external third parties. Craig discussed that, with external third parties, it is often setting thresholds in when specific controls are applied to an external third party. Frances took the action item to write more on this. Vicki discussed further regarding SLA's, contractual language, agreements between two organizations (e.g., ITIL alignment). The team discussed that the SLA relationship changes significantly if the external third party is a customer; Craig suggested that User's Guide can provide guidance regarding topic area

and thresholds that the reader may wish to incorporate into their planning and strategy for monitoring. Scott suggested Frances leverage the NISTIR and other existing documents in writing his content.

One team member revisited their action item taken earlier in series of meetings to provide reference architecture.

The team discussed whether to retain significant content on maturity model. The team's consensus was that the User's Guide needs to be independent of maturity model, and it is currently more focused on risk level. The team was in accord to strike the content focusing on maturity model.

The team discussed the next step on the User's Guide draft. Each team member's action items are to be completed by 03/08/2013, and the team will meet again on 03/15/2013. In addition to action items threaded throughout meeting minutes, Marianne volunteered to do wordsmithing and technical editing; Jody will incorporate the edits from everyone as an aggregation point. Per existing protocol, Tanya will schedule the GoToMeeting; Jody will send out notifications to distribution.

Meeting Administration:

Next call: The team will meet to continue to cover the updated draft and action items on March 15, 2013, 1:00pm to 2:30pm, EST. The completion of this meeting series is typically on a bi-weekly cycle.

Driving to March 15th: Please note the following additional dates, milestones and activities running from February 22nd through March 15th as a consequence of the action items from the February 22nd meeting:

- Monday, March 4 – Jody will send out reminder of inputs coming due at the end of week.
- Friday, March 8 – All items should be received by the evening of March 8th.
- Monday, March 11 – Jody will send out the updated draft to distribution.
- Friday, March 15 – The team will meet again to go through the draft.