Et alia:

RE: Questions posited in the RFI – "Framework for Reducing Cyber Risks to Critical Infrastructure".

In response to requests for industry perspectives by the DOE and NIST, I would instead like to offer a posit for addressing the one single issue, the 'elephant in the room' if you will, to achieving a Digital Systems Security (DSS) Cybersecurity standard across the US Utility spectrum. That issue is the 'expanding redundant complexity' of the current approach to the problem domain. While one can appreciate the efforts in gathering more information from the industry at large for establishing and improving frameworks to raise the overall level of cybersecurity across the utility industry, the problem is that it does not address the inherent complexity of the problem. It only exacerbates it by creating yet more administrative requirements for decomposing and resolving the problem domain for each utility.

There are a number of issues, or challenges, to achieving a base level of digital systems security (DSS) across the utility spectrum (an overall 'cybersecurity standard'). One challenge is in large part due to the complexity in decomposing the myriad sets of requirements from competing regulatory bodies, each with their own frameworks. The largess of the effort required is not trivial; either from a resource perspective, a cost perspective, and in many cases a capability perspective. As the number of requirements (i.e.-'recommendations') expands, unless streamlined, it will require increasing amounts of resources from each utility to remain abreast of those requirements, let alone wade through each at the outset to decompose the requirements and obtain a true GAP for the utility. Given the very real threat of not addressing the GAP's in the larger utility domain, and the resources in total required to achieve that ideal, in a word, the process needs to be 'simple'.

A tool such as the Cybersecurity Evaluation Tool (CSET) does simplify this process by reducing the requirements to a 'single-source' for decomposing the problem domain. By enhancing the CSET with additional capabilities, used as the litmus for decomposing and managing the cybersecurity domain, updated by the standards body as new recommendations and requirements evolve, the complexities of this aspect of the process are simplified.

Another challenge: after having fully decomposed a problem domain into a set of requirement documents, the complexity and largess of the problem becomes fully exposed, and the effort it requires to satisfy the combined requirements realized. A fully codified requirements document, with all the underlying requirements to satisfy each parent requirement, leads to an exponential explosion of requirements that must be managed and satisfied to achieve a given cybersecurity standard. Further, once realized, the added requirements to subject change requests to the Security/System Development Life Cycle (SDLC), and to audit each of those new change requests to rigorous decomposition across the same multi-regulatory body of frameworks in a way that is manageable, can be overwhelming.

By enhancing the CSET to manage the SDLC aspects of the DSS domain, it would reduce administrative and redundant efforts otherwise required to manage the information between multiple systems, and serve as a living digital document of the DSS domain, thus simplifying the

process further. It could also be leveraged in a number of ways to expose related information for use in mitigating attacks, managing DSS assets, etc.

We used the CSET in its current state for these reasons. While the process is certainly not 'easy', it is relatively simple in comparison to wading through all the various requirements and recommendations, hoping to achieve a full decomposition of each. Some suggestions based on our experience with the CSET to date…

- Expand the CSET tool to encompass all requirements, expose them dynamically as the tool does now based on each utility's makeup, and use it as the de-facto litmus for assessing the current state and exposing the gap. In this manner, as each individual set of regulations are updated, the tool can be updated and any new gaps exposed. A 'single-source'.
- While the CSET implements a thorough qualitative risk analysis and some level of quantitative risk analysis, encompass any additional quantitative risk analysis requirements within the CSET tool, mainly because there really is no standard or encompassing methodology for performing a thorough quantitative risk analysis within the utility industry. Without that standard, efforts will be inefficient and risks the lack of exposure of otherwise known attack vectors.
- Expand the Component Diagram to allow decomposition of all other DSS domains (AMI network, Engineering network, etc.) to expose risks across the entire domain.
- Provide better guidelines for using the CSET tool… e.g. – perform the 'Enterprise Evaluation' first, address those issues, then perform the SAL's and standards based regulatory (NIST, CIP, etc.) assessments, followed by the Component Diagram. The reason for this approach is that by performing them in this order, much of the redundancy between the questionnaires could be eliminated with some CSET enhancements, thereby reducing the size of the requirement documents and DSS Team efforts considerably.
- Offer assistance to guide utilities at least through the Enterprise Evaluation section to get beyond the inertia, with some guidance for moving through the rest of what is required to achieve a robust level of protection, and DOE evangelists to assist further if needed.
- Finally, consider using the ES-C2M2 as the litmus for achieving a given level of maturity. The requirement/goal would be for a utility to operate at MIL3, with some form of motivation to get/keep them there.

The process would be as follows…

Process…

1. Team: Create a CSET profile for the Utility.
2. CSET: Based on the utility profile answers, populate the CSET 'Enterprise Evaluation' (EE) section with relevant information/questions.
3. Team: Complete the CSET 'Enterprise Evaluation' (EE).

4. CSET: Based on profile and answers to the EE, generate an Enterprise Evaluation GAP report as a Requirement document, enumerating those requirements in order of relative importance.
5. Team: Design, develop, and implement DSS solutions to remedy or mitigate the Enterprise Evaluation GAP report requirements. Update the CSET Enterprise Evaluation GAP with those results.
6. CSET: Reflect the EE updates across all relevant requirements, dynamically updating duplicate requirements to mitigate redundant efforts by the DSS Team.
7. Team: Complete the CSET Security Analysis Level (SAL) assessments.
8. CSET: Populate the CSET with regulatory standards-based requirements relevant to the Utility as revealed through the SAL answers.
9. Team: Answer the generated standards-based assessments, and then create the Component Diagram.
10. CSET: Populate the Component Diagram assessment questions based on the devices and architecture created in the diagram.
11. Team: Answer the Component Diagram assessment questions created by CSET (the CSET currently replicates those answers to like-components/devices if indicated by the DSS Team to avoid redundancy at the discovery levels).
12. CSET: Create a new requirement document, enumerating consolidated (non-duplicate) regulatory DSS requirements, in order of relative importance.
13. Team: Design, develop, and implement DSS solutions to remedy or mitigate the regulatory GAP requirements. Update the CSET Enterprise Evaluation GAP with those results.

SDLC (ongoing)…

14. Team: Enter each new change order for a device, or replacement device, into the CSET Component Diagram.
15. CSET: Generates new requirements for the added device.
16. Team: Completes the design, development, and implementation for the new device. Update the CSET to close the GAP.
17. CSET: As new standards based recommendations/requirements evolve, updates to the CSET will expose new GAP's will be exposed.
18. Team: Address any new GAP's exposed by upgrades as part of the normal SDLC process.

Simplifying the DSS Cybersecurity process in this fashion will save utilities, both individually and collectively, significant amounts of time and resources, and could galvanize the DSS efforts for both the regulatory bodies and utility industry combined.

Sincerely,

Dr. Les Cardwell, DCS-DSS
Enterprise Data Architect
Central Lincoln PUD
2129 N Coast Hwy
Newport OR 97365

Phone: 541.997.5615
Cell: 541.490.4301

CENTRAL LINCOLN
A PUBLICLY-OWNED ELECTRICAL UTILITY

EACOE Certified
Enterprise Architect

(This is the perspective and opinion of the author, and does not necessarily reflect the opinions of Central Lincoln.)