PSCC Subcommittee TF S10 Meeting Minutes

Designation: TF S10	Name: Utility & Municipality Challenges on Analyzing and Implementing Cybersecurity Standards and Best Practices

Meeting Location: WebEx Meeting	Meeting Time: 9:00 A.M. CDT	Meeting Date: 2020/05/04	Minutes Revised:	Minutes Approved: 2021-01-11

PAR Output: N/A	PAR Output: N/A	PAR Approval Date: N/A	PAR Expiration Date: N/A	Target Sponsor Ballot Date: N/A	Target Completion Date: N/A

Presiding Officer: Jeff Pack, Chair	Recorded by: Jeff Pack, Chair	Draft Number: [1.1]

Attendance:

Name	Affiliation	Attending via Phone (P) / Web (W) or Local (L)	M/CM/G
Jeff Pack	POWER Engineers, Inc.	W	M
Steve Mark	SEL	W	M
James Formea	Eaton	W	G
Mike Dood	SEL	W	M
Anthony Montoya	Centauri	W	G
Shane Haveron	Ametek	W	M
Priyanka Nadkar	SEL	W	G
Mario Jardim	Schneider Electric	W	G
Didier Giarrantano	Schneider Electric	W	G
Scott Mix	PNNL	W	M
Dinesh Baradi	ABB	W	G
Juan Urquijo	Beckwith Electric	W	G
Keith Gray	POWER Engineers	W	G
Maik Seewald		W	G
Marc Lacroix		W	G
Craig Pruess	Black and Veatch	W	M
Matt Garver	Beckwith Electric	W	M
Dennis Holstein	Opus Consulting	W	G

M:Member
CM: Corresponding Member
G: Guest

Item no.	Notes	Action by
CALL TO ORDER	Called to order by the chair at 9:03 a.m. CDT	Pack
INTRODUCTIONS AND QUORUM	Second TF meeting – all attendees on WebEx call.	Pack
CALL FOR PATENTS AND COPYRIGHT	Patent slides and copyright slides presented to group.	Pack
CHAIR'S REMARKS	TG had the first meeting in Jacksonville in January 2020. Meeting minutes were sent to attendees of the first meeting.	Pack
AGENDA APPROVAL	Agenda was presented with no specific comments.	Pack

Item no.	Notes	Action by
APPROVAL OF PREVIOUS MINUTES	Chair reviewed the minutes from the first meeting. Mix moved to accept the minutes and Dood seconded the motion.	Pack
Review TF10 Title, Scope, Purpose	The chair shared the purpose of the group and pointed out that Mix had noted previously that the purpose of the group does not discuss what the result of the effort will be. The chair added a second sentence that described the deliverable as a guidance report. Mix discussed that the word "guidance" may be interpreted as requiring a PAR to approve development. Formea indicated that keeping it generic as "report" would be enough to avoid the need for a PAR. The chair will change the deliverable to a report.	Pack
Audience	The chair discussed the intended audience for this report and presented a proposal that the audience be focused on Operations Engineering Management/Staff. Haveron mentioned that IT needs to be included in the audience due to the many interactions between Operational Technology (OT) and Information Technology (IT). Garver agreed. The chair discussed the need to add a section on OT and IT integration. Mix mentioned that EPRI had documents on "IT for OT People" and "OT for IT People" that may be useful.	Pack
Baseline Standards	The chair presented several options for baseline standards that were mentioned in the previous meeting. The chair asked for comments on any standards that were more international in their approach to include a global view for the report. Giarrantano commented that the EU uses the ISO 27000 series of standards and the focus is more on risk management than developing technical cybersecurity standards. Mix mentioned that ISO 27000 series focus on information protection, but that ISO 27019 has industrial standards. Giarrantano agreed that organizations will use ISO 27001 and ISO 27002 as a baseline and then add additional ISO 27xxx standards as needed for each system, so ISO 27019 would be applied on top of ISO 27001 and/or ISO 27002. Giarrantano stated that the report needs to address training on threats and response that are unique to electric power control systems.	Pack
Applicability Matrix	The chair discussed the need to provide a simplified way to provide a set of baseline requirements and allow an engineering manager or equivalent to develop a set of parameters for developing a cybersecurity program that meets baseline requirements and aligns with the organization's functions, capabilities, resources and staff. Holstein mentioned that there are two major maturity areas to address – staff and processes. The group writing ISA 99 has struggled with developing an appropriate methodology for developing an effective approach.	Pack
Maturity Model	The chair presented some sample maturity models for discussion. Links to C2M2 and the APPA models are provided below. Giarrantano stated that there is not a lot of focus on the maturity model in the EU – they use risk management as the measurement of maturity and provide guidance via ISO 27001 and ISO 27002. Holstein mentioned that CIGRE has been working on a maturity model for cybersecurity as well. Their model is related to the cyber kill chain methodology. EPRI has extended their maturity model to focus on metrics from the C2M2 model. C2M2 - https://www.energy.gov/ceser/activities/cybersecurity-critical-energy-infrastructure/energy-sector-cybersecurity-0 APPA - https://www.publicpower.org/system/files/documents/Cybersecurity_Scorecard_Overview.pdf	Pack

Item no.	Notes	Action by
Report Outline	The chair presented some organization models for the report that are based on existing frameworks, including NIST, APPA and a standard engineering approach. Holstein stated that the report needs to address the needs of stakeholders for the utility. The chair mentioned that the stakeholders in smaller utilities normally are focused on results and not on any of the details needed to get there. There are fewer stakeholders involved, so there is less debate than in larger organizations. Lacroix added that stakeholders often don't know what they want or are unable to articulate it related to cybersecurity. Holstein discuss the need to have an overlay or a seamless integration into the existing organization. Larger organizations would simply develop a new security group and overlay them into the existing groups, but that approach probably won't work in smaller organizations. The chair stated that most smaller organizations will need to define the security roles and responsibilities and the existing staff will need to add those to their existing workload. Mix stated that another methodology to review as part of the organization of the report is the "Plan, Do, Check, Act" methodology and that regardless of how the organization is structured, there is a need for a closed loop for feedback into the processes. The chair agreed with this position and will include that into the outline development.	Pack
ITEMS REPORTED OUT OF EXECUTIVE SESSION	N/A	
TIME OF FINAL ADJOURNMENT	9:57 a.m. CDT. Holstein moved for adjournment and Mix seconded the motion.	
NEXT FACE TO FACE MEETINGS	September 2020 - Reno	
FUTURE MEETING ROOM REQUIREMENTS	Room Size: 40 Projector: Yes Web Meeting: Yes Conflicts: All PSCC S	