PSCC Subcommittee S10SG Meeting Minutes

Designation: S8	Name: WG Testing Power System Cybersecurity Controls				
Meeting Location: Pittsburgh, Pennsylvania		Meeting Time: 8:00 AM	Meeting Date: 05/09/2018	Minutes Revised:	Minutes Approved:
PAR Output:	PAR Request Date: 12/31/2022	PAR Approval Date: 03/08/2018	PAR Expiration Date: 12/31/2022	Target Sponsor Ballot Date: 01/2020	Target Completion Date: 10/2020
Presiding Officer: Chair: Nathan Wallace, Vice Chair: Deepak Maragal			Recorded by: James Formea	Draft Number: NA	

Attendance:

Name	Affiliation	Attending via Phone (P) / Web (W) or Local (L)	M/CM/G
Nathan Wallace	Cybirical	L	M
Deepak Maragal	NYPA	L	M
Dennis Holstein	OCG	L	M
Ralph Mackiewicz	SISCO	L	M
Steven Kunsman	ABB	L	M
Chris Bonstje	SEL	L	G
Herb Falk	GTB Consulting	L	M
Rebekah Goldman	BPA	L	G
Ryan Newell	TRC	L	M
Harry Zapata	Duke	L	G
Didier Gianakano	Schneider Electric	L	G
James Formea	Eaton	L	M
Eric Thibodeau	Gentec	L	G
Luke Saladyga	Google	L	G

M:Member
CM: Corresponding Member
G: Guest

Item no.	Notes	Action by
CALL TO ORDER		Nathan
INTRODUCTIONS AND QUORUM	Had several new guests. Quorum was achieved with 8 members present.	
CALL FOR PATENTS	Presented new patent slides. No concerns raised.	Nathan
CHAIR'S REMARKS	PAR has been approved. Now have Working Group status.	Nathan
AGENDA APPROVAL	James approved Meeting Agenda, Seconded by Dennis. No dissenters. Motion carried.	
APPROVAL OF PREVIOUS MINUTES	Previous Minutes reviewed. Steve made motion to approve. Seconded by Dennis. No dissenters. Motion carried.	
Scope Review	Reviewed newly approved PAR that included scope and purpose. Also, showed/reviewed purpose slides.	

Item no.	Notes	Action by
General Discussion	-Steve asked for a quick overview of some acronyms shown in the overview slides: SIEM - security information event management RBAC - role-based access control SDN - software-defined networks DoS - denial-of-service NSM - network security monitoring or network security management Comment by Steve Kunsman that the WG may want to check with the Computer Society or other groups that may have formally defined the acronym NSM IDS - intrusion detection system AAA - authentication, authorization, and accounting Herb Falk asked "who will be doing the testing?" He explained that in IEC 61850, there is separation between protection & control functions and security functions. Nathan suggested that we don't necessarily need to differentiate in our definition of the tests. Herb countered that the tests need to be designed with the executor of the test in mind. Some of the tests that may be called out could violate some of the principles of cybersecurity that the controls are intended to address. Brief discussed ensued on the depth of guidance expected in the developed standard -- will focus on "what" to test, but with "some" information on "how" to test , in general terms. Not necessarily application-protocol specific. Didier Giarratano mentioned that this same construct is known as "security auditing" in the European community. Herb asked about testing certification expiration and revocation. This testing needs to occur before devices are made operational in the field, as certificates should not be revoked for testing in an operational system. Didier asked about the timing of the proposed testing. If this testing is performed during operation, there are risks. Perhaps some of the testing needs to be performed only in commissioning. Herb asked about failover testing. Nathan recommends that it be tested, but notes that it can be difficult. Nathan mentioned that he does consider failover a cybersecurity control in some cases. PAR was approved by IEEE-SA on March 8, 2018, and is active until December 31, 2022. Nathan reviewed the PAR submittal. Expected date of draft submitted for initial sponsor ballot is January 2020. Dennis clarified with Nathan that the resulting work will be a numbered "Guide" even though the PAR is for a new standard. Dennis mentioned the potential inclusion of "ABAC" - attribute-based access control.	

Item no.	Notes	Action by
(cont)	Nathan presented slides for discussion on types of tests based on discussion in the January meeting. Herb mentioned that certificates and passwords may need to be considered outside of the normal process. Default credentials and certificates need to be replaced before any tests dependent on certificates are conducted. A second set of certificates is then appropriate to be loaded after commissioning to move into production. James recommended a category of "Credential and Identity Management", which may need to be the first set of steps carried out as part of the testing process. Ryan Newell asked if Maintenance is intended to cover application of routine upgrades/patches? That may be one of the most important pieces of functionality to test. Herb mentioned some work going on in IEC for remote system configuration. Luke Saladyga mentioned that messing with certificates on a live system can be risky. Herb described the IEC stance that multiple device certs are required for availability. Perhaps even certs signed by different trusted root CAs. OCSP and CRL interaction could pose significant challenges to securing the grid with certificates. Luke mentioned that the document needs to discuss the important of properly managing certificates, credentials, etc. and planning for revocation/expiration. Didier asked if chain of trust needs to be considered? We must balance the security with resiliency and availability. Dennis asked about application verification testing - would this be in a QA laboratory? This may need to be called out as major utilities usually go through a QA lab first with live data feeds to verify no adverse effects. Perhaps this is addressed in "Customer Functional Testing". Additional discussion was had around QA test lab operations at utilities. Decommissioning/disposal - this needs to be handled carefully. James pointed out that many device decommissioning/disposal functions being specified by system operators require a logically-destructive operation that leaves the device in a state that prohibits redeployment without sending the device back to the manufacturer. Nathan presented a proposal for approach to the WG's work product. 1. Collection of online reference material a. Information is currently being posted on the WG S8 website section 2. Formulation of an outline 3. Determination of interest in the different sections to be developed	

Item no.	Notes	Action by
(cont)	NIST SP800-115 was briefly shown/discussed as a good source document for this work. Herb suggests mentioning Penetration Testing to be part of the recommendation, but not necessarily detailed out into steps, as effective Pen Testing is typically carried out by a third party. The group is interested in soliciting input and participation from firewall and IDS system vendors. Dennis mentioned possibly putting the relevant information for the work products on iMeet as well so that all discussion and reference can be conducted on the same site. Nathan discussed next steps Steve made a recommendation against a double-session at the September meeting. Dennis recommended holding virtual meetings with different work streams developed to support different writing sections.	
Call for Participation	Several guests volunteered as contributing members.	
Assignments	- Setup iMeet Central - Begin searching for and commenting on reference material. Send any reference material to Nathan - Nathan will then post resources on iMeet and PSCC website.	Nathan All Members Nathan
ITEMS REPORTED OUT OF EXECUTIVE SESSION	N/A	
TIME OF FINAL ADJOURNMENT	James made a motion to adjourn; seconded by Dennis. No dissenters. Motion passed. Meeting closed at 913am.	
NEXT FACE TO FACE MEETINGS	Minneapolis, MN	
FUTURE MEETING ROOM REQUIREMENTS	Room for 30, Projector needed	