IEEE Power System Communication & Cybersecurity Committee

CYBER SECURITY SUBCOMMITTEE – S0

Chair: Steven Kunsman

Vice chair, Jim Bougie

Secretary: Farel Becker

S0 website: http://sites.ieee.org/pes-pscc/cybersecurity-subcommittee-s0/

AGENDA/Minutes – May 11, 2017, Albuquerque, NM

1. Introductions / Attendees
   Subcommittee met with 13 attendees of which 6 have signed up to be members.

Name	Company	S0 Member or Guest
Farel Becker	Siemens	M
Steve Kunsman	ABB	M
Anthony Johnson	SCE	M
Craig Preuss	B&V	M
Mike Dood	SEL	M
Marc Lacroix	EMCREY Canada	M
Benton Vendiver	ABB	G
Deepak Maragal	NYPA	G
David Minshall	ABB	G
Charles Sufana	GE	G
Mark Benou	Iniven	G
Chris Huntley	SEL	G
Galina Antonova	ABB	G

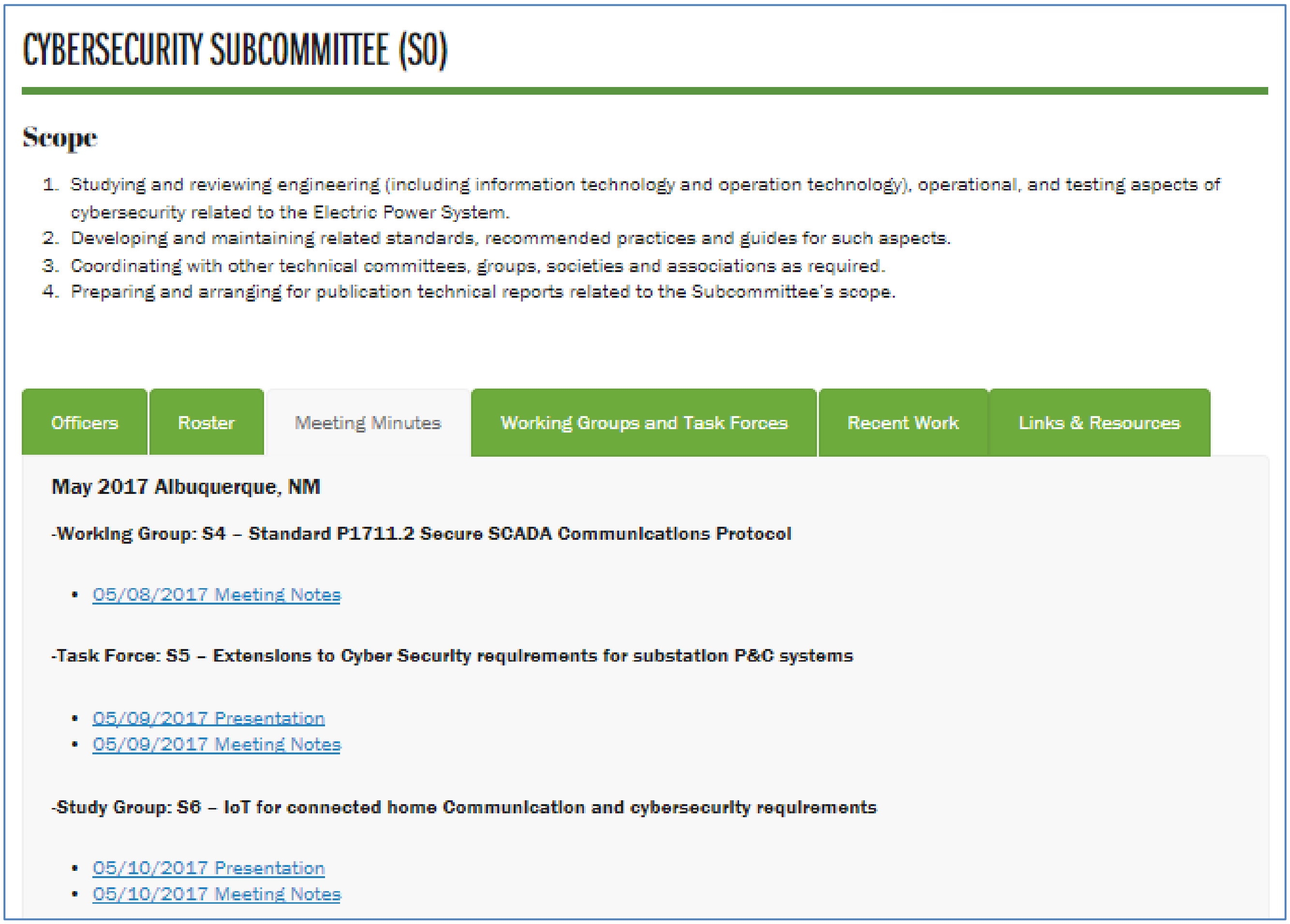
2. Subcommittee membership, requirements, and signup list
   a. Requirements for SC membership
      i. Be a member of IEEE PES
      ii. Be an active member of S SC working group(s)

iii. Be willing to regularly attend and participate in the S SC

An email will be sent to those group members not in attendance to solicit their interest in becoming a S0 subcommittee member.

3. Group Minutes (will be posted online)
   a. Summary minutes to be provided to SC officers after your group meeting.
   b. Detailed minutes to be provided to SC officers within 2 weeks after your group meeting.

Thank you Nathan!



CYBERSECURITY SUBCOMMITTEE (S0)

Scope

1. Studying and reviewing engineering (including information technology and operation technology), operational, and testing aspects of cybersecurity related to the Electric Power System.
2. Developing and maintaining related standards, recommended practices and guides for such aspects.
3. Coordinating with other technical committees, groups, societies and associations as required.
4. Preparing and arranging for publication technical reports related to the Subcommittee's scope.

May 2017 Albuquerque, NM

-Working Group: S4 – Standard P1711.2 Secure SCADA Communications Protocol

- 05/08/2017 Meeting Notes

-Task Force: S5 – Extensions to Cyber Security requirements for substation P&C systems

- 05/09/2017 Presentation
- 05/09/2017 Meeting Notes

-Study Group: S6 – IoT for connected home Communication and cybersecurity requirements

- 05/10/2017 Presentation
- 05/10/2017 Meeting Notes

4. S SC Working Group/Study Group/Task Force Summary / Status (details in group minutes)

WG S2: P1711.1 Serial SCADA Protection Protocol (SSPP)

Chair: David Whitehead

Scope: This standard defines the Substation Serial Protection Protocol (SSPP), a cryptographic protocol to provide integrity, and optional confidentiality, for cyber security of substation serial links. It does not address specific applications or hardware implementations, and is independent of the underlying communications protocol.

Status: Draft standard is being finalized and proceed to MEC review. WG vote and proceed to ballot. Plan is to be in ballot resolution by September 2017. WG PAR completion is Dec 2017

WG S3: P2030.102.1 Standard for Interoperability of IPSEC Utilized within Utility Control Systems

Chair: Jim Bougie

Scope: This standard specifies requirements for interoperability of devices utilized within utility control systems which implement the Internet Protocol Security (IPsec) protocol suite within an IPv4 environment.

Status: Received feedback from IEC TC57 WG15 and will address comments. New leadership has been appointed: Jim Bougie chair, Marc Lacroix vice-chair, James Formea secretary. PAR needs to be revised as well deadline extended.

WG S4: P1711.2 Trial-Use Standard for Secure SCADA Communications Protocol (SSCP)

Chair: Mark Hadley

Scope: This trial use standard defines a cryptographic protocol to provide integrity with optional confidentiality for cyber security of substation serial links. It does not address specific applications or hardware implementations and is independent of the underlying communications protocol.

Status: Draft standard is ready for proceed to MEC review and WG vote to proceed to ballot. Plan is to be in ballot resolution by September 2017. WG PAR completion is Dec 2017.

TF S5: Cyber Security Requirements for Power System Automation, Protection and Control Systems

Chair: Steve Kunsman

Scope: Revision of IEEE C37.240 to included new technical requirements for power system cyber security. Based on sound engineering practices, requirements can be applied to achieve high levels of cyber security of automation, protection and control systems independent of voltage level or criticality of cyber assets.

Status: Task force developed a PAR and plans to submit in June for IEEE SA approval. S6 should be transitioned to a WG by the September meeting.

SG S6: IoT for connected home - Communication and cybersecurity requirements

Chair: Marc Lacroix

Scope: The study group presents a project for IoT connected home. Proposes the creation of TF or WG. The next step is to produce a report that describes the different use cases that make use of the Connected Homes concept, presents a security risk analysis and propose requirements for telecommunication (Volume, frequency, speed) and cybersecurity. Guidelines for utilities experts will be listed.

Status: Recommendation to proceed with this project since these new technologies will impact the utilities. Since we don't have enough data at the moment, the creation of a task force will be proposed at PSCC management meeting.

5. Old Business

6. New Business

a. September meeting PSCC Cyber Security Subcommittee to be scheduled on Wednesday late afternoon to allow a greater participation.

b. SC vote on S6 recommendation to proceed in creating a task force

Approved: SC attendees voted to approve S6 to become a task force.

c. Brainstorming on new areas of interest

Develop profiles for use in Power Systems Communications:

- Syslog with possible collaboration with WG15
- Security HMI for operator usability – ISA and CIGRE have worked in this area
- SSH
- LDAP/Radius
- SSL
- TLS
- SNMP
- NTP
- HTTPS
- SFTP

Wireless cyber security – PAR exists for IEEE 1777

Maturity models and risk management (NIST Framework – DHS C-cubed)

Guidelines for appropriate Cyber Security with end to end security with deep packet inspection

Building secure code – University of Illinois activity

Cyber Security Architecture

d. Other items:

The PSCCC needs to promote to the utility IT security personnel the benefits of this committee and have a recruiting effort to start attending the PSCC meetings as our scope includes all utility communications. The IT domain expertise is required in our efforts.

7. Adjourn