



PSCC Subcommittee [Working/Study Group, Task Force] Meeting Minutes

Designation: S0		Name: Cybersecurity Subcommittee			
Meeting Location: Hybrid – Nashville, TN		Meeting Time: 2:45 PM CT	Meeting Date: 2022/09/14	Minutes Revised:	Minutes Approved:
PAR Output: NA	PAR Output: NA	PAR Approval Date: NA	PAR Expiration Date: NA	Target Sponsor Ballot Date: NA	Target Completion Date: NA
Presiding Officer: Scott Mix (Chair), Theo Laughner (Vice-Chair)			Recorded by: Theo Laughner	Draft Number: 1.0	

Attendance:			
		Attending via Phone (P) / Web (W) or Local (L)	
Name	Affiliation		M/CM/G

Scott Mix	PNNL	L	M
Theo Laughner	Lifescale Analytics	L	M
Jay Anderson	SEL	L	M
Eugenio Carvalheira	Omicron	L	M
TW Cease	Consultant	L	M
Ed Cenzone	SEL	L	M
James Formea	Eaton	L	M
Didier Giarratano	Schnieder	W	M
Shane Haveron	Ametek	W	M
Anthony Johnson	SCE	L	M
Marc Lacroix	EMCREY Canada	W	M
Jeff Pack	Power Engineers	L	M
Eric Thibodeau	Hydro Quebec	L	M
Nathan Wallace	Ampirical	W	M

M: Member			
CM: Corresponding Member			
G: Guest			

--

Item no.	Notes	Action by
CALL TO ORDER		Scott Mix
INTRODUCTIONS AND QUORUM	14/27 members present, quorum established.	Scott Mix/Theo Laughner
CALL FOR PATENTS		
CHAIR'S REMARKS		Scott Mix
AGENDA APPROVAL	Eric Motion/Theo Second – Motion Carried with amendment by changing name from Colon to Colin.	Scott Mix
APPROVAL OF PREVIOUS MINUTES	Jay Motion/Eric Second – minutes approved.	Scott Mix
S1 Report	<p>WG S1: Revision of IEEE 1686 IED Cyber Security Capabilities</p> <p>PAR Approval: yyyy/mm/dd PAR Expires: 2022/12/31 Target Completion: yyyy/mm/dd Draft: 1.4</p> <p>Chair: Marc Lacroix Vice-chair: Éric Thibodeau Secretary:</p> <p>Scope: The standard defines the functions and features to be provided in intelligent electronic devices (IEDs) to accommodate cybersecurity programs. The standard addresses security regarding the access, operation, configuration, firmware revision and data retrieval from an IED. Confidentiality, integrity and availability of external interfaces of the IED is also addressed.</p> <p>Status: S1 met on Monday at 10:40 AM CST with 10 members out of 14. Quorum was met.</p> <ul style="list-style-type: none"> • Our last ballot recirculation received an approval rate of 95% and on an 80% return rate. Three comments were received. The BRG response was to reject all the comments. • The WG voted to approve the resolution and to submit the 1.4 draft to RevCom as was submitted to the last recirculation. <p>Next Meeting Requirements: [Room Size=35] [Projector=Yes][Telecom=Yes][Conflicts=]</p>	Eric Thibodeau

Item no.	Notes	Action by
<p>S2 Report</p>	<p>WG S2: P1711.1 Serial SCADA Protection Protocol (SSPP)</p> <p>PAR Approval: yyyy/mm/dd PAR Expires: yyyy/mm/dd Target Completion: yyyy/mm/dd Draft: xxxx</p> <p>PAR Approval: yyyy/mm/dd PAR Expires: yyyy/mm/dd Target Completion: yyyy/mm/dd Draft: xxxx</p> <p>Chair: Ed Cenzone Vice-chair: Andrew Wright* Secretary: Mike Dood</p> <p>Scope: This standard defines the Serial SCADA 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.</p> <p>Status: S2 met at 3:30pm 5/9/2022. 7 members present out of 10. Quorum achieved.</p> <p>Minutes from the January 2022 meeting were read and approved.</p> <p>Chair accepted a motion to submit 1711.1 for MEC review. WG voted to approve.</p> <p>Chair accepted a motion to request S0 to form a ballot pool for 1711.1 post MEC review with only editorial changes. WG voted to approve.</p> <p>Chair accepted a motion to submit 1711.1 to ballot contingent on only editorial edits returned from MEC review. WG voted to approve.</p> <p>Chair accepted a motion to list Andrew Wright as vice-chair on 1711.1 (posthumously). WG voted to approve. Also, Mike Dood volunteered to help as Secretary. Thank you, Mike!</p> <p>Chair accepted a motion to request S0 to let 1711 PAR expire. WG voted to approve.</p> <p>Next Meeting Requirements: [Room Size=20] [Projector=Yes][Telecom=Yes][Conflicts=P2]</p>	<p>Ed Cenzone</p>
<p>S3/S4</p>	<p>Inactive</p>	

Item no.	Notes	Action by
S5	<p>WG S5: Revision of IEEE C37.240 Cybersecurity Requirements for Power System Automation, Protection and Control Systems</p> <p>PAR Approval: yyyy/mm/dd PAR Expires: yyyy/mm/dd Target Completion: yyyy/mm/dd Draft: xxxx</p> <p>Chair: TW Cease Vice-chair: --vacant-- Secretary:</p> <p>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.</p> <p>Status:</p> <p>Discussion to disband and to turn over material to ISA WG 14. ISA Co-Chair (Steve Kunsman) would welcome the contribution. However, several approvals from IEEE and ISA are required. The membership list needs to be cleaned.</p> <p>Next Meeting Requirements: [Room Size=40] [Projector=Yes][Telecom=Yes][Conflicts=]</p>	TW Cease
S6	Inactive	

Item no.	Notes	Action by
<p>S7</p>	<p>WG S7: P2808 Function Designations used in Electrical Power Systems for Cyber Services and Cybersecurity</p> <p>PAR Approval: yyyy/mm/dd PAR Expires: yyyy/mm/dd Target Completion: yyyy/mm/dd Draft: xxxx</p> <p>Chair: Nathan Wallace Vice-chair: Mike Dood Secretary: Deepak Maragal</p> <p>Scope: This standard applies to the definition of function designations for cyber related services, and cybersecurity controls and measures used to detect, identify, protect from, respond to, and recover from, security threats to electric power systems. These designations apply to the design, procurement, and operation of electric power systems. This standard also provides examples of how to represent systems using these designations.</p> <p>Status:</p> <ul style="list-style-type: none"> • Approximately 13 Attendees / 8 of 12 Members present / 5 Guests, • Notes: Quorum achieved. Discussed the idea of defining Keys normatively for each designation as optional. Going to be requesting IEC 61850-6 documentation for the WG. Will be setting up monthly meetings. Next meeting 20 people, projector, wifi, and hybrid. • PAR Details: <ul style="list-style-type: none"> ○ Original Scope: This standard applies to the definition of function designations for cyber related services, and cybersecurity controls and measures used to detect, identify, protect from, respond to, and recover from, security threats to electric power systems. These designations apply to the design, procurement, and operation of electric power systems. ○ New Proposed Scope (Pending MC approval): This standard defines and applies to function designations for cyber related services, and cybersecurity controls and measures used to detect, identify, protect from, respond to, and recover from, security threats to electric power systems. These designations apply to the design, procurement, and operation of electric power systems. This standard also defines engineering and modeling documentation using these designations. ○ Timeline: <ul style="list-style-type: none"> ■ Type of Project: New IEEE Standard ,PAR Request Date: 23-Jan-2019, PAR Approval Date: 21-Mar-2019 , PAR Expiration Date: 31-Dec-2023 • Action Item: Submit request to MC S0's approve request to accept S7's change of scope. <p>Next Meeting Requirements: [Room Size=20] [Projector=Yes][Telecom=Yes][Conflicts=]</p>	<p>Nathan Wallace</p>

Item no.	Notes	Action by
<p>S8</p>	<p>WG S8: P2658 Guide for Cybersecurity Testing in Electric Power Systems</p> <p>PAR Approval: yyyy/mm/dd PAR Expires: yyyy/mm/dd Target Completion: yyyy/mm/dd Draft: xxxx</p> <p>Chair: Nathan Wallace Vice-chair: Deepak Maragal Secretary:</p> <p>Scope: This document provides test guidance for cybersecurity controls used in electric power systems. The guide encompasses testing and verification of cybersecurity services, applications, and controls, including end-to-end testing.</p> <p>Status:</p> <ul style="list-style-type: none"> • Approximately 12 Attendees / 6 of 11 Members present / 6 Guests, <ul style="list-style-type: none"> ○ Notes: Quorum achieved. Worked on draft of document. Discussed a better way to state the objectives of the Testing that is included in the guidance. Also, Erin brought up the approach of including an open downloadable link on IEEE SA's website for the templated testing forms. Will be setting up monthly meetings. Next meeting 20 people, projector, wifi, and hybrid. ○ Side Note: PAR scope change and Extension has been submitted to RevCom. Details include: <ul style="list-style-type: none"> ▪ New Scope (Pending RevCom approval): This document provides test guidance for cybersecurity controls used in electric power systems. The guide encompasses testing and verification of cybersecurity services, applications, and controls, including end-to-end testing throughout their lifecycles. ▪ (Pending RevCom Approval) PAR Expiration Date: 31-Dec-2025 ○ Action Items: No action items for S0. <p>Next Meeting Requirements: [Room Size=20] [Projector=Yes][Telecom=Yes][Conflicts=]</p>	<p>Nathan Wallace</p>
<p>S9</p>	<p>TF S9: Task Force on Utility IT-OT Cybersecurity challenges in roles and terminology</p> <p>PAR Approval: N/A PAR Expires: N/A Target Completion: yyyy/mm/dd Draft: xxxx</p> <p>Chair: Theo Laughner Vice-chair: Brian Smith Secretary:</p> <p>Scope: Assess the IT-OT challenge in Utility Cybersecurity roles. Determine if a Task Force is required to create a report to assist in building organizational understanding and collaboration</p> <p>Status:</p> <p>Met on Monday @ 9:20 w/quorum. Minutes from May 21, Sep 21, and May of 22 were approved. D5 was approved to submit to S0. Meeting space in January for 10 people with a project and avoid conflicts with H40.</p> <p>Next Meeting Requirements: [Room Size=30] [Projector=Yes][Telecom=Yes][Conflicts=H40]</p>	<p>Theo Laughner</p>


Item no.	Notes	Action by
<p>S10</p>	<p>TF S10: Utility & Municipality Challenges on Analyzing and Implementing Cybersecurity Standards and Best Practices</p> <p>PAR Approval: N/A PAR Expires: N/A Target Completion: yyyy/mm/dd Draft: xxxx</p> <p>Chair: Jeff Pack Vice-chair: --Vacant-- Secretary:</p> <p>Scope: Assess the challenge in utilities & municipalities with limited resources on the applicability and relevance of the cybersecurity standards and create a report to assist summarizing the relevant cybersecurity standards.</p> <p>Status:</p> <ul style="list-style-type: none"> • Meeting started on time at 2:22 P.M. CDT with approximately 15 attendees based on the room attendance list and the WebEx attendee list. A full attendee list will be included in the minutes once the WebEx attendance report is provided. • Four members were in attendance, so quorum was not achieved. • The vice chair position is open – the chair asked for any volunteers. • May 2022 minutes were not reviewed since there was no quorum. • Reviewed the draft report and received areas to address based on our quick scroll through the draft. Need to add some additional standards for the baseline, review the governance model for duplication of S9 content. Also need to look at adding more context based on organization size, discuss maturity model and develop an approach to address what it really means for staff and management. • The chair will schedule at least one working session to review the draft document and prepare it for S0 review. • The chair will upload the draft to iMeet Central and make sure that all contributors have access to review and comment. • Meeting was adjourned at 3:15 P.M. CDT <p>Actions:</p> <ul style="list-style-type: none"> • Finalize draft and upload to iMeet Central • Schedule working session to review and update draft <p>Next Meeting Requirements: [Room Size=40] [Projector=Yes][Telecom=No] [Conflicts=HTF55]</p>	<p>Jeff Pack</p>
<p>S11, S12</p>	<p>Inactive</p>	
<p>S13</p>	<p>WG S13: Review 1547.3 Guide for Cybersecurity of DERs Interface with Electric Power Systems</p> <p>PAR Approval: yyyy/mm/dd PAR Expires: yyyy/mm/dd Target Completion: yyyy/mm/dd Draft: xxxx</p> <p>Chair: Tony Johnson Vice-chair: R. Benjamin Kazimier Secretary:</p> <p>Scope: To jointly develop 1547.3 with SCC21.</p> <p>Status:</p> <p>Done with ballot. In ballot resolution, expect to be completed by end of the month for a recirculation ballot.</p> <ul style="list-style-type: none"> • No meeting expected for January 	<p>Tony Johnson</p>

Item no.	Notes	Action by
S14	<p>TF S14: Task Force on using TLS in Power System Applications</p> <p>PAR Approval: N/A PAR Expires: N/A Target Completion: yyyy/mm/dd Draft: xxxx</p> <p>Chair: Shashi Sastry Vice-chair: Colin Gordon Secretary:</p> <p>Scope: Develop a report on the implementation of TLS for usage in legacy (e.g., SCADA) and emerging (e.g., DER) power system applications</p> <p>Status:</p> <ul style="list-style-type: none">• Chair and vice-chair switched places - Chair is now Colin Gordon with Vice-Chair being Shashi Sastry.• Quorum was not met.• We reviewed changes to the draft report. It was pointed out that the wrong template was in use.• We will attempt some meeting(s) between now and January to generate report content.• Discussion of PSK modes. <p>Next Meeting Requirements: [Room Size=30] [Projector=Yes][Telecom=Yes][Conflicts=]</p>	Scott Mix

Item no.	Notes	Action by
S15	<p>WG S15: IEEE Guide for Securing Generic Object Oriented System Events (GOOSE) and Sampled Values (SV) Protocols of IEC 61850 using IEC 62351-6 and IEC 62351-9</p> <p>PAR Approval: yyyy/mm/dd PAR Expires: yyyy/mm/dd Target Completion: yyyy/mm/dd Draft: xxxx</p> <p>Chair: Jay Anderson Vice-chair: Shane Haveron Secretary: Dean Ouellette</p> <p>Scope: This guide provides information for suppliers and implementors on applying security from the most recently published versions of IEC 62351-6 and IEC 62351-9 to GOOSE (IEC 61850-8-1), R-GOOSE (IEC 61850-8-1), SV (IEC 61869-9), or R-SV (IEC 61850-9-2) protocols.</p> <p>Status:</p> <p>Patent slides, copyright slides, and behavior slides were displayed. With Quorum, the minutes from 9/21/21, 1/11/22, and 5/10/22 were all approved (note: need to correct the header from the 9/21/21 to indicate that we are a WG); Move to approve by C. Preuss, second by A. Apostolov. Agenda was approved as well (Preuss/Apostolov). Minutes will be uploaded to the S0 iMeet site.</p> <p>A submission was received from Marc Lacroix, who updated the Table of Contents and corrected formatting.</p> <p>The Chair discussed recent developments concerning the use of the subject 62351 standards, including the successful demonstration of a Key Distribution Centre (KDC) system delivering cryptographic keys to an IED at the 2022 UCA IOP in Milan, Italy in July, and increased interest from other vendors in KDCs and integrity and confidentiality systems, and a proposal to IEC TC57 WG 15 to consider adding MACsec for SV communications.</p> <p>We began to review the document, including the changes made by Marc. The group began a discussion on another potential attack vector, where configuration information could be retrieved from connected IEDs and used to inform attack methods. We also discussed the potential to corrupt a configuration in and IED. Other vectors discussed included the possibility of someone replacing an IED within an ESP but outside of a PSP, which could look like another form of spoofing that might be addressed using authentication protection. Writing contributions were solicited and promised.</p> <p>Additional sections to be considered for addition to the Guide include testing information (including considerations for Transient Cyber Assets) and use cases. Colin Gordon volunteered to develop a short presentation on 62351-9. A meeting will be scheduled to continue discussion in early November. Mark Adamiak and Farzad Khalilpour requested group membership.</p> <p>Next Meeting Requirements: [Room Size=35] [Projector=Yes][Telecom=Yes][Conflicts= H50, P1, H44, H47, C33, S2, H52].</p>	Jay Anderson

Item no.	Notes	Action by
<p>S16</p>	<p>TF S16: Task Force on Systems for Detecting and Preventing Network Intrusions in Electric Power Systems</p> <p>PAR Approval: N/A PAR Expires: N/A Target Completion: yyyy/mm/dd Draft: xxxx</p> <p>Chair: Eugenio Carvalheira Vice-chair: Eric Thibodeau Secretary:</p> <p>Scope: This task force will be investigating the current state of the art for network Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) used in Electric Power Systems (EPS). The report from the task force will have to document the different existing methods to perform detections. These include, but are not limited to, monitoring the associations between transmitters and receivers on the network, detailing the types of protocols used, recognizing signatures inside data packets, comparison to a baseline of existing traffic, etc. For prevention purposes, the task force should focus on active systems that can shut down a network intrusion under way. This excludes already well covered countermeasures like IED hardening, firewalls, network diodes, etc.</p> <p>Status:</p> <ul style="list-style-type: none"> - S16 met on Tuesday September 13 at 8:00 AM CDT. 4 members out of 8 were present at the meeting, quorum was not met - iMeet Workspace is now online to start contributing on the draft report - A few contributions were received, but there is still a lot to do. - We will try again to reach out to vendors to get support for sections 3 and 5. The former explains the types of systems available and the second explains architectures for deployment. Their input could be very valuable for the report. - For next meeting, room for 20 people, with projector and teleconference capabilities will be required. <p>Next Meeting Requirements: [Room Size=20] [Projector=Yes][Telecom=Yes][Conflicts=]</p>	<p>Eugenio Carvalheira</p>

Item no.	Notes	Action by
<p>S17</p>	<p><u>TF S17: Task Force on Use of SBOM in the Energy Sector</u></p> <p>PAR Approval: N/A PAR Expires: N/A Target Completion: yyyy/mm/dd Draft: xxxx</p> <p><u>Chair:</u> Éric Thibodeau <u>Vice-chair:</u> Marc Lacroix <u>Secretary:</u></p> <p><u>Scope:</u> Investigate Use cases for SBOM; Survey of SBOM initiatives; Survey of tools; Applicability of these initiatives to the energy sector; Recommendations</p> <p><u>Status:</u></p> <ul style="list-style-type: none"> • S17 met on Tuesday at 1:00 PM CST. • This was our first meeting as a task force. Initial membership was established with 7 people volunteering. • We started to brainstorm on the scope and purpose the task force • Since there are several entities working on the subject, our group feels the key to our report is not only to survey the efforts, but also to identify gaps that we could address within our subcommittee • It was highlighted that PSRC I47 (P37.231) included SBOM in its scope. We have an action item to get in touch with them to make sure our work is complementary • We will ask the IEEE SA to setup an iMeet workspace to go forward with our work • For next meeting, we will need room for 15, with projector and teleconference capabilities. <p>Next Meeting Requirements: [Room Size=25] [Projector=Yes][Telecom=Yes][Conflicts=I47]</p>	<p>Eric Thibodeau</p>
<p>Unfinished Business</p>	<p>Forward S7 scope change to main committee meeting.</p>	<p>Scott Mix.</p>
<p>New Business</p>	<p>WG S1 asks for a motion to approve submittal to RevCom of draft 1.4 of P1686 as was submitted to the last recirculation.</p>	<p>Motion by Eric. Second by Tony. Motion carries.</p>
	<p>Task Force S9 report to be sent out for S0 review. Comments due back to Theo Laughner (S9 chair) by December 1, 2022 for consideration by S9 with expected S0 approval of final report at January meeting.</p>	<p>Announcement</p>

Item no.	Notes	Action by
	<p>Request from Mohammad (Reza) Khalghani, Florida Polytechnic University to sponsor a Panel Session at the 2023 PES General Meeting. If approved by S0, request will be forwarded to the MC for their consideration tomorrow.</p> <p>Panel session title: Resilient Control and Operation of Power Grids against Cybersecurity Threats: Challenges and Solutions</p> <p>Summary of the panel session: Similar to all engineering applications and systems, power and energy systems are designed to be controlled in a closed-loop structure. Closed-loop systems can regulate the components of power grids to react appropriately to any system changes. Since smart grids heavily tie the control system with cyber and communication interfaces, the entire grid becomes vulnerable to cyber anomalies. This panel will study the different aspects of control design for power grids to be resilient against cyber disruptions.</p> <p>Total time length: We need a two-hour session for this panel. Panel session chair and co-chair: Mohammad Reza Khalghani Expected panel presentations: Five speakers</p> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p>Panel Session Title: Resilient Control and Operation of Power Grids against Cybersecurity Threats: Challenges and Solutions</p> <ul style="list-style-type: none"> • Primary committee: PSCC • Subcommittee: Cybersecurity (S) • Potential Panelists: Five panelists from <ul style="list-style-type: none"> ○ Cybersecurity subcommittee members to disseminate the group accomplishments ○ Academic faculties • Potential Talks on: <ul style="list-style-type: none"> ○ DNP3 and IEEE P1815 Working Group outcomes ○ IEC 62443 / ISA99 Working Group outcomes ○ Subcommittee outcomes on “cyber-testing and design” (drawing and common language) ○ Subcommittee outcomes on “segmentation of networks” • Proposed by: Mohammad (Reza) Khalghani • Email: khalghani@ieee.org </div> <p> FLORIDA POLYTECHNIC UNIVERSITY</p>	<p>Motion from James. Second from Jay. Motion carries.</p>
	<p>“Scott and I have had brief conversations in the past on the new cyber security specifications being developed as part of the update to (Clause 7 of) Std 1815. (See flyers to be sent out with minutes.) This major development work is being undertaken by the Cyber Security TF (CSTF) of the DNP Users Group, but the IEEE reviews of this work are being coordinated by our WG P2, which I chair. Our challenge and opportunity is that the cyber security experts are mostly on the S0 team and not our P0 team!</p> <p>“We are anticipating a wide adoption by the industry (over time) as the level of priority and spend on OT security increases in the coming years, combined with a growing emphasis on authentication and zero trust. In other words, we believe this will be a very important body of work going forward.</p> <p>“Having said all that, we would REALLY appreciate some S0 people having a good look at this work. So far we can see two options:</p> <ol style="list-style-type: none"> 1. People join WG P2 as non-voting members...and/or 2. People join the DNP-UG CSTF to participate directly.”- r.farquharson@ieee.org 	<p>Ron Farquharson</p>

Item no.	Notes	Action by
Announcements	<ul style="list-style-type: none"> • Roster Cleanup for non-participating members (notice must be provided to non-participating members well ahead of removing them). • 123Signup Retirement and Replacement (123Signup is dead! Long Live Member Planet!) • Chairs must provide full meeting minutes within 2 weeks (by 09/30/2022). • Meeting Minutes (draft .doc and approved .pdf) are to be uploaded to the PSCC Committee iMeet site in addition to individual SG/WG/TF sites. • Meeting notice and WG/TF/SG agenda to be sent to sub-group members and SO Chair two weeks prior to any meeting. • Newly formed WG and TF (i.e., those migrated from SG) should issue a call for participation and establish a roster by the conclusion of their next meeting. • All sub-groups are expected to have Vice Chairs. Secretaries are optional (Vice Chair assumes role of Secretary if none). • Working Group chairs (standards activity) are now REQUIRED to take IEEE SA training. Training must be completed by the end of the year. • Understanding IEEE SA's Antitrust, Competition, and Commercial Terms Policies • IEEE SA Standards Working Group Chair Fundamentals • New Participant Behavior slides to be shown at all WG meetings have been released by IEEE SA. PowerPoint versions are available on the PSRCC website - https://site.ieee.org/pes-pscc/files/2022/05/Participant-Behavior-Individual-method.ppt • Reminder: Task Forces also need to manage membership and have quorum to approve minutes, and at the completion of their task to approve the reports out of the TF to go to the subcommittee. • If anyone has published a paper in an IEEE Transactions journal, let the chair know so that it can be considered for an award. • New PES PowerPoint Template is available. • Scott will serve as chair for another two years. 	Scott Mix
Roundtable	Tony is working on a way to manage digital collateral associated with standards. Nathan can send notifications out to the social media outlets.	All
Membership Activity	No report.	Scott Mix
TIME OF FINAL ADJOURNMENT	4 PM CT.	
NEXT FACE TO FACE MEETINGS	January 8-12, 2023 – Jacksonville, FL	
FUTURE MEETING ROOM REQUIREMENTS	30 People, Projector,	

