November 18 - 20
2019

THE ACADEMY

Cybersecurity Summit

Nashville, Tennessee

PublicPower.org/CyberSummit

AMERICAN PUBLIC POWER ASSOCIATION

Monday November 18

PRE-SUMMIT SEMINARS

Separate registration and fee required

8 a.m. – 4 p.m.

DOE's CyberStrike Workshop

PARTHENON AB

Get a hands-on, simulated demonstration of a cyberattack, drawing from elements of the 2015 and 2016 cyber incidents in Ukraine, and defend against a mock cyberattack on the industrial control equipment you routinely encounter. The U.S. Department of Energy's Office of Cybersecurity, Energy Security and Emergency Response, in collaboration with the Electricity Information Sharing and Analysis Center and Idaho National Laboratory, developed this workshop to prepare energy sector owners and operators in the U.S. for a cyber incident impacting industrial control systems. Build your skills and learn from industry experiences that give you insight into the multifaceted interdependencies between the country's critical infrastructure and how you can detect threats and respond within compressed timelines to prevent highly impactful consequences.

***Tim Conway**, CyberStrike Instructor, Idaho National Laboratory*

8:30 a.m. – 4:30 p.m.

Cybersecurity for Industrial Control Systems: Architecture, Asset Inventory, Network Security Monitoring & Event Detection

PARTHENON DE

Recommended CEUs .7/PDHs 6.5/CPEs 7.8

Building off of the Association's introductory cybersecurity courses, take a technical focus to outlining a cybersecurity program in the industrial control system environment. Review the principles of a defensible architecture, learn how to conduct a thorough cyber asset inventory, and discover the necessary event detection techniques and network security monitoring tools to identify an attack in the ICS. Explore how network security monitoring provides visibility into the operational technology network, including determining a baseline for normal operations and alerting you to unexpected events. The course is ideally suited for utility IT or ICS technical personnel who are responsible for, or interested in, applying cybersecurity standards and best practices to the industrial environment.

***Gus Serino**, PE, Principal ICS Security Analyst, Dragos, Inc., Boston, Massachusetts*

Tuesday, November 19

7:30 – 8:30 a.m.

Registration & Coffee

FRANKLIN FOYER

8:30 – 10 a.m.

Welcome and Introductions

PARTHENON BALLROOM

***Mike Hyland**, Senior Vice President, Engineering Services, American Public Power Association; and **Decosta Jenkins**, President & CEO, Nashville Electric Service, Tennessee; and Chair, American Public Power Association*

KEYNOTE PRESENTATION

Threat Briefing: Utilities, Be Aware

Threat actors continue to focus on how to break into the U.S. power system, with attempts becoming more frequent and sophisticated. The threats do not stop coming after you make improvements to your systems. Hear what you need to know about this evolving threat landscape and what you need to watch for now and in the future to keep your utility protected.

***Jonathan Homer**, Chief of Industrial Control Systems, U.S. Department of Homeland Security, Arlington, Virginia*

10 – 10:15 a.m.

Break

10:15 – 11:45 a.m.

I Was Hacked: True Stories from Utilities

The warnings aren't exaggerated if they are true: municipalities and organizations have had critical files encrypted in ransomware attacks. Hear true stories of utilities that were hacked and learn how they recovered and revamped their cybersecurity measures to come out stronger on the other side.

***Victor Lay**, City Administrator, City of Spring Hill, Tennessee; and **Chris Lindell**, Electronic Systems Analyst, Beatrice Board of Public Works, Nebraska*

11:45 a.m. – 1 p.m.

LUNCH KEYNOTE

DOE's Cyber Update

Get an update from the Department of Energy on its cybersecurity initiatives and hear about new developments of interest to public power.

***Karen S. Evans**, Assistant Secretary, Office of Cybersecurity, Energy Security, and Emergency Response (CESER), U.S. Department of Energy, Washington, D.C.*

1 – 1:15

Break

1:15 - 2:45 p.m.

GridEx V: What Did We Learn?

The North American Electric Reliability Council's Grid Security Exercise (GridEx) is an opportunity for utilities to demonstrate how they would respond to and recover from simulated coordinated cyber and physical security threats and incidents. Discuss some of the early lessons learned from the public power utilities who participated in GridEx V, including ways to strengthen essential crisis communications relationships.

***Warren Brooks**, PE, Manager-Electric Line Engineering, City Utilities of Springfield, Missouri; **Ken Lewis**, Principal Planning Analyst, Business Continuity & Emergency Management, Salt River Project, Phoenix, Arizona; and **Brandon Pixley**, Director, Threat Intel & Security Awareness, CPS Energy, San Antonio, Texas*

2:45 – 3 p.m.

Break

3 - 4:15 p.m.

E-ISAC Industry Engagement Program

Learn about the E-ISAC's Industry Engagement Program, an innovative effort started by public power utilities to foster collaboration and information sharing between the E-ISAC and utilities. Learn how to be a part of the feedback loop, discuss ways to take action on information that is shared, and hear examples of changes that have been made because of feedback from public power organizations.

***Randy Crissman**, Sr. Reliability and Resilience Specialist – Utility Operations, New York Power Authority, White Plains, New York; and **Bluma Sussman**, Associate Director, Member Engagement, Electricity Information Sharing and Analysis Center, North American Electric Reliability Corporation, Washington, D.C.*

4:30 – 5:30 p.m.

Roundtable Discussion

Join your fellow attendees for in-depth discussions on topics covered throughout the day.

5:30 – 6:30 p.m.

Reception

ACORN BALLROOM

Wednesday, November 20

8 – 8:30 a.m.

Registration & Coffee

FRANKLIN FOYER

8:30 – 9:45 a.m.

Don't Go It Alone: Making the Most of Strategic Partnerships

PARTHENON BALLROOM

It is okay to ask for help with cybersecurity. Learn how public power utilities use strategic and innovative partnerships to manage cybersecurity activities, including using cyber mutual aid and teaming up with universities.

***Carter Manucy**, Cyber Security Manager, Florida Municipal Power Agency, Orlando, Florida; **Scott Smith**, CISSP, CGCIO, Chief Information Security Officer, City of Bryan, Texas*

9:45 - 10 a.m.

Break

10 – 11:15 a.m.

Recruiting, Retaining and Training Your Cybersecurity Workforce

Cybersecurity personnel are in demand, and we aren't just competing with other utilities for talent. Hear how public power utilities are reaching this workforce, what their staffing plans are for the future, and how they are training employees to develop critical cybersecurity skills.

***Sharon Chand**, Principal, Cyber Risk Services, Deloitte & Touche LLP, Chicago, Illinois; and **Fred Christie**, Chief Information Officer, Easton Utilities Commission, Maryland*

11:15 - Noon

Closing Discussion

Synthesize what you learned in a roundtable discussion with your peers on the issues addressed throughout the summit, including ongoing challenges and new questions. Plan your next steps and talk about how public power can work together to secure the grid against cyber attacks.

Noon

Summit Adjourns

Wednesday, November 20

POST-SUMMIT SEMINAR

Separate registration and fee required

1:30 – 5 p.m.

Shore Up Supply Chain Security, Prepare for Compliance

PARTHENON DE

Recommended CEUs .3/PDHs 3.25/CPEs 3.8

Discuss the new NERC supply chain management security standards and security best practices for your equipment and software suppliers. Review NERC Critical Infrastructure Protection Supply Chain Standard (CIP-013) requirements and prepare for compliance starting July 2020. Whether you are with a large or small utility, you will benefit from learning how five public power entities are implementing practices and controls for the CIP-013 requirements. Discuss your initiatives and ask the experts about issues with your supply chain risk management program. Participate in a roundtable discussion to drill down on risk management planning and controls, CIP-013 implications for other standards, vendor outreach and contractual language, accreditation and self-certification, and software acquisition management with risk identification and secure updates.

***Anirudh Bhimireddy**, Program Manager, Business Systems, New York Power Authority, White Plains, New York; **Casey Fallon**, Director – Purchasing, Warehouse, Fleet, SMUD, Sacramento, California; **Diane Gil**, Sr. Director, Procurement Governance Analytics, New York Power Authority, White Plains, New York; **AJ Jacobs**, CISO, SMUD, Sacramento, California; **Kevin Johnston**, CISO, Snohomish County PUD, Everett, Washington; **Michael McGann**, Vice President of Supply Chain, Lower Colorado River Authority, Austin, Texas; and **Skip Peeples**, Principal Analyst, Supply Chain, SRP, Phoenix, Arizona*

Thank You Sponsors

Thank you to our sponsors for the generous financial support to help us offer the best experience for attendees.

Signature Sponsor

axio

Diamond Sponsors

AMPCUS CYBER An Ampcus Company

ARCHER

1898 & CO.

DRAGOS

IPKeys POWER PARTNERS

n-dimension solutions

tyler cybersecurity

Silver Sponsor

BEAM REACH CONSULTING GROUP Make the most of your resources.

Key Facts

Summit Evaluation: A link to an online survey about the summit will be emailed to attendees after the conference. We appreciate your valuable feedback.

Summit Presentations: Copies of the speakers' presentations are available on the American Public Power Association's website here: https://www.publicpower.org/cybersecurity-summit-past-presentations.

Guest Activities: Summit registrants may bring a guest to the Tuesday evening reception.

Restricted Sessions: The Association reserves the right to designate any meeting or session open only to Association regular members (public power utilities, rural electric cooperatives, joint action agencies and state/regional associations). Please inquire at the registration desk if you have any questions.

Antitrust Statement: Various state and federal laws prohibit the exchange of information among competitors regarding matters pertaining to price, refusals to deal, market division, tying relationships and other topics that might infringe upon antitrust laws and regulations. No such exchange or discussion will be tolerated during this event. A copy of the Association's Statement of Compliance with the Antitrust Laws is available upon request.

Code of Conduct: Attendees of American Public Power Association meetings agree to abide by the APPA Code of Conduct. If attendees engage in unacceptable behavior as outlined in the Code of Conduct, the Association may take any action it deems appropriate, including but not limited to, expulsion from the current and future meetings, with no warning or refund.