Cybersecurity Summit

November 13-14, 2018 • Austin, Texas

AMERICAN PUBLIC POWER ASSOCIATION ACADEMY

ELITE SPONSOR

axio

CO-HOST

TPPA Texas Public Power Association

Tuesday, November 13

Noon - 1 p.m.

Registration

CAPITAL AB FOYER

1 – 2:30 p.m.

Welcome and Introductions

CAPITAL BALLROOM

***Mike Hyland**, Senior Vice President, Engineering Services, American Public Power Association*

***Khalil Shalabi**, Vice President, Strategy, Technology and Market Operations, Austin Energy, Texas*

Keynote Presentation

High Tech, High Threat: Next Generation Cyber Challenges

Recommended CEUs .2/PDHs 1.5 /CPEs 1.8

Today, almost any device with an on-and-off switch can be connected to the Internet and to other devices. By 2020, there could be more than twenty-six billion connected devices. As this Internet of Things and other technologies evolve, so do threats to the electric grid. Today, cyber attackers are targeting more than laptops and servers. They are looking to break in at the operations, distribution, and even consumer level. Learn about new cyber vulnerabilities and how you can protect against them. Review the risks that emanate from the use of drones, robots, artificial intelligence, autonomous systems, AMI, and more. Learn how to mitigate the risks so you can leverage technologies of the future to provide safe, reliable service.

***Peter Morin**, Director, Cyber Security Services, KPMG, Halifax, Nova Scotia, Canada*

2:30 – 2:45 p.m.

Break

2:45 – 4 p.m.

Know Your Enemy: Active Defense & Penetration Testing for Utilities

Recommended CEUs .1/PDHs 1.25 /CPEs 1.5

Understanding your adversaries and how they operate is crucial to cyber defense. This intelligence can lead to more effective prioritization of controls and improved detections for organizations "hunting for evil" in their networks. This knowledge of adversary capabilities can also be leveraged to simulate real-world attack scenarios on infrastructure during penetration testing efforts and reveal the risk remediation that matters most. Hear from two public power utilities that have used active defense and penetration testing to better protect their IT/OT systems.

***Dan Gunter**, Principal Threat Analyst, Dragos Inc., San Antonio, Texas; **Brent Heyen** and **Mark Johnson-Barbier**, Senior Principle Analysts, Cyber Security Architecture, SRP, Phoenix, Arizona; and **Jessica Matlock**, Director, Government Relations, External Affairs and Strategic Accounts, Snohomish County PUD, Everett, Washington*

4 – 4:15 p.m.

Break

4:15 – 5:30 p.m.

Assessments Made Simple: The New Cybersecurity Scorecard

Recommended CEUs .1/PDHs 1.25 /CPEs 1.5

The new Cybersecurity Scorecard from the American Public Power Association is being used by a growing number of public power utilities to assess cybersecurity risks and build up defenses.

Based on the DOE's Electricity Subsector Cybersecurity Capability Maturity Model, the scorecard—at a basic level—allows your utility to start assessing your cyber risks and vulnerabilities by completing a self-assessment comprising 14 questions. Based on the score, you get customized recommendations you can use to build a cybersecurity action plan. Learn how other utilities have benefited from using the scorecard to issue a wake-up call to management and get buy-in from policymakers to invest in cybersecurity. You can sign up for the scorecard platform at no charge at the end of the session.

***Carter Manucy**, Cyber Security Manager, Florida Municipal Power Agency, Orlando, Florida; and **Chad Schow**, IT Manager, Franklin PUD, Pasco, Washington*

5:30 – 6:30 p.m.

Reception

STEPHEN F'S

Wednesday, November 14

8 – 8:30 a.m.

Registration & Coffee

CAPITAL AB FOYER

8:30 – 9 a.m.

DOE Opening Address

CAPITAL BALLROOM

Recommended CEUs .1/PDHs .5 /CPEs .6

***Karen Evans**, Assistant Secretary for Cybersecurity, Energy Security, and Emergency Response, Department of Energy, Washington, D.C.*

9 – 10:15 a.m.

Better Informed Is Better Prepared: Threat Alerts and Analysis

Recommended CEUs .1/PDHs 1.25 /CPEs 1.5

An essential component of your cyber defense system is to monitor industry-wide and cross-sector threat alerts so you'll know what you should be prepared for. Two trusted sources for threat information and analysis are the E-ISAC and MS-ISAC. E-ISAC offers situational awareness on security threats, remediation, task force reviews, and other resources. MS-ISAC, operated by the nonprofit Center for Internet Security, is the go-to resource for cyber threat prevention and recovery for U.S. state, local, tribal, and territorial government entities. Hear from both entities about the threat monitoring and analysis services they offer. Learn from the experience of a public power utility that has used both portals to stay aware of threats. Find out how you can participate in these portals, distill the information, and plan your responses and action plan.

***Kenneth Carnes**, Chief Information Security Officer, New York Power Authority, White Plains, New York; **Bill Lawrence**, PMP, Vice President and Chief Security Officer, E-ISAC, Washington, D.C.; and **Ryan Spelman**, Senior Director, Center for Internet Security, Albany, New York*

10:15 – 10:30 a.m.

Break

10:30 – 11:45 a.m.

An Unclassified Threat Briefing

Recommended CEUs .1/PDHs 1.25 /CPEs 1.5

The U.S. faces a complex global cyber threat. The Intelligence Community World Wide Threat Assessment notes that the leading state intelligence threats to U.S. interests will continue to be Russia and China, with other adversaries posing local and regional cyber threats. Adding to these threats is the clear targeting of the energy sector. Get information to help your organization understand threat actors and discuss options for enhancing energy security and resilience.

11:45 a.m. - 1 p.m.

Lunch Keynote

***Tim Roxey**, Chief Special Operations Officer, North American Electric Reliability Corporation, Washington, D.C.*

1 – 1:15 p.m.

Break

1:15 – 2:45 p.m.

Building a Cybersecurity Culture: Tips and Tricks

Recommended CEUs .2/PDHs 1.5 /CPEs 1.8

Humans are the weakest link in the cybersecurity chain. Changing the leadership and staff culture to be more aware is often harder than putting the right hardware and software in place. Yet without the culture change, no cyber plan can be effective. Hear from an organizational change expert as well as public power utility officials on how you can motivate and train everyone on your team to practice good cyber hygiene and secure the frontiers of your utility against attackers.

***Randy Black**, IT Manager, Norwich Public Utilities, Connecticut; **Joshua Cox**, Senior System Administrator, City of Westerville Electric Division, Ohio; and **Chris Kelley**, Vice President, Beam Reach Consulting Group, Severna Park, Maryland*

2:45 – 3 p.m.

Break

Thank You Summit Sponsors

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

ELITE SPONSOR

axio

DIAMOND SPONSORS

BURNS McDONNELL

Deloitte.

n-dimension solutions

3 – 4:30 p.m.

Cybersecurity Innovations: From Research to Reality

Recommended CEUs .2/PDHs 1.5 /CPEs 1.8

The Department of Energy's National Laboratories have served as leaders of scientific innovation for more than seventy years. They address large scale, complex research and development challenges with a multidisciplinary approach that places an emphasis on translating basic science to innovation. Learn more about what the National Labs are doing on the cybersecurity front and how they translate cyber threat information into actionable programs. See how you can work with the labs and what resources you can get from collaborating with DOE.

***David Manz**, PhD, Senior Cyber Security Scientist, National Security Directorate/Cyber Security Group, Pacific Northwest National Laboratory, Richland, Washington; and **Wayne Austad**, Technical Director, Cybercore Integration Center, Idaho National Laboratory*

4:30 – 5 p.m.

Closing Discussion: Next Steps

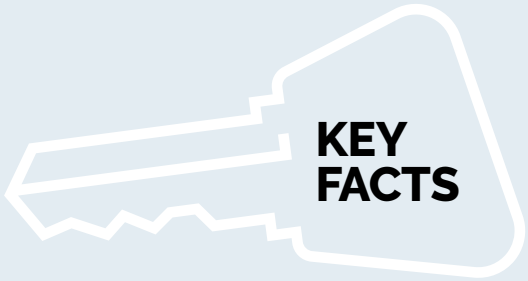
Recommended CEUs .1/PDHs .5 /CPEs .6

Limited to employees of public power utilities, state and regional associations, and joint action agencies

Join Association staff and your utility peers at a roundtable discussion on the issues addressed throughout the summit. Discuss challenges and questions with your peers. Plan next steps and see how public power can work together to secure the grid against cyber attacks.

5 p.m.

Adjourn



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 at: 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.

CONTINUING EDUCATION

Complete the Verification of Attendance form (available at the registration desk) to receive a certificate for continuing education credits. Certificates will be sent via email after the conference.

Continuing Professional Education (CPE) Credits
The American Public Power Association is registered with the National Association of State Boards of Accountancy (NASBA) as a sponsor of continuing professional education on the National Registry of CPE Sponsors. State boards of accountancy have final authority on the acceptance of individual courses for CPE credit. Complaints regarding registered sponsors may be addressed to the National Registry of CPE Sponsors, 150 Fourth Ave. N., Suite 700, Nashville, TN 37219-2417. Website: www.nasbaregistry.org.

Earn up to 12.6 CPE credit hours in Specialized Knowledge for attending this event. All sessions are intermediate-level, group-live offerings with no prerequisites and no advance preparation required. For more information regarding administrative policies, such as clarification of requirements, complaints, and refunds, please contact EducationInfo@PublicPower.org.

Continuing Education Units (CEUs)
The American Public Power Association is accredited by the International Association for Continuing Education and Training (IACET) and is authorized to issue the IACET CEU. 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.

Professional Development Hours (PDHs)
APPA educational practices are consistent with the criteria for awarding Professional Development Hours (PDHs) as established by the National Council of Examiners for Engineering and Surveying (NCEES). Course eligibility and number of PDHs may vary by state.

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.