PENNSYLVANIA PUBLIC UTILITY COMMISSION

CYBERSECURITY SUMMIT

TUESDAY, AUGUST 20, 2019

8:30 AM TO 3:30 PM
Cybersecurity Summit Agenda

8:30 AM  Opening Remarks
          Gladys Brown Dutrieuille, PUC Chairman

9:00 AM  Keynote
          Joseph H. McClelland, FERC - Office of Energy Infrastructure Security

9:30 AM  Guest Speakers
          Scott Aaronson, MPM, Vice President, Security and Preparedness, Edison Electric Institute

10:00 AM  Franco Cappa, Cybersecurity Advisor - CISSP, C|CISO, ITIL, Cybersecurity and Infrastructure Security Agency

11:00 AM  Break Out Sessions

Executive Track
          Major Christine Pierce, PA National Guard Cyber Branch Chief / Defensive Cyber Operations Element Team Chief

Regulatory Track
          Matthew Thomas, GSTRT, GISP, ReliabilityFirst - Manager, CIP Compliance Monitoring

Threat Track
          Ronald L. Keen, Senior Energy Advisor, National Risk Management Center (NRMC), CISA, U.S. Department of Homeland Security

Technical Track
          Jerome Farquharson, MS, CISSP, CRISC, Sr. Principal Director, Regulatory Risk Management & Cyber Security, Senior Principal Director of Burns & McDonnell’s Regulatory Risk Management & Cyber Security Group

12:00 PM  Complimentary Lunch
<table>
<thead>
<tr>
<th>Time</th>
<th>Break Out Sessions</th>
</tr>
</thead>
<tbody>
<tr>
<td>1:00 PM</td>
<td><strong>Executive Track</strong></td>
</tr>
<tr>
<td></td>
<td>Secretary Rosemary Chiavetta, Esq., Pennsylvania Public Utility Commission</td>
</tr>
<tr>
<td></td>
<td><strong>Regulatory Track</strong></td>
</tr>
<tr>
<td></td>
<td>Phyllis Lee, Senior Director of CIS Controls, Center for Internet Security</td>
</tr>
<tr>
<td></td>
<td><strong>Threat Track</strong></td>
</tr>
<tr>
<td></td>
<td>Matthew D. Duncan, GCIP, Manager, Policy and Coordination, Electricity Information Sharing and Analysis Center</td>
</tr>
<tr>
<td></td>
<td><strong>Technical Track</strong></td>
</tr>
<tr>
<td></td>
<td>Jonathon Monken, MBA, Senior Director, System Resilience and Strategic Coordination</td>
</tr>
<tr>
<td>2:00</td>
<td><strong>Break Out Sessions</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Regulatory Track</strong></td>
</tr>
<tr>
<td></td>
<td>Kelly Monaghan, MBA, CPA, CGFM, CFE, CISA, Director of the Bureau of Audits for the Pennsylvania Public Utility Commission</td>
</tr>
<tr>
<td></td>
<td><strong>Threat Track</strong></td>
</tr>
<tr>
<td></td>
<td>Jennifer Lyn Walker, Cybersecurity Threat Analyst, Water ISAC</td>
</tr>
<tr>
<td></td>
<td><strong>Technical Track</strong></td>
</tr>
<tr>
<td></td>
<td>Dr. Steven McElwee, PhD, MBA, CISSP, Chief Information Security Officer, PJM Interconnection</td>
</tr>
<tr>
<td>3:00 PM</td>
<td><strong>Closing Remarks</strong></td>
</tr>
<tr>
<td></td>
<td>Michael Holko, PUC Director - OCCO</td>
</tr>
</tbody>
</table>
Joseph H. McClelland, Director, Office of Energy Infrastructure Security (OEIS)

Joseph H. McClelland was appointed the first Director of the Office of Energy Infrastructure Security (OEIS) by Chairman Jon Wellinghoff in September 2012. OEIS is the new Federal Energy Regulatory Commission (FERC) office that will provide leadership, expertise and assistance to identify, communicate and seek comprehensive solutions to potential risks to FERC-jurisdictional facilities from cyber attacks and such physical threats as electromagnetic pulses.

Prior to directing OEIS, Mr. McClelland served as the first Director of the Office of Electric Reliability, which was created in 2007. He joined the Commission in 2004 as Director of the Division of Reliability within the Office of Energy Markets and Reliability.

Mr. McClelland came to the Commission with more than 20 years of experience in the electric utility industry. He began his career with Allegheny Energy Inc., holding a variety of positions in engineering, marketing, regulation and rates, and project development. Immediately prior to joining the Commission, Mr. McClelland was the General Manager of the Custer Public Power District in Broken Bow, Nebraska. He holds a Bachelor of Science degree in Electrical Engineering from Pennsylvania State University.
Mr. Aaronson has been with EEI since 2009 when he joined the government relations department focusing on security and several emerging technology issues, including electric grid modernization, cybersecurity policy, and telecommunications priorities. He now leads EEI’s security and preparedness team where he focuses on industry security and resilience initiatives, establishing collaborative partnerships between government and electric companies—and across critical infrastructure sectors—that enhance security for the energy sector.

In addition to his role at EEI, Mr. Aaronson also serves as the Secretary for the Electricity Subsector Coordinating Council (ESCC). The ESCC is the primary liaison between senior government officials and industry leaders representing all segments of the sector. This partnership is held up as a model for how critical infrastructure operators can work with government, yielding dramatic improvements in security and preparedness for the electric power sector and the nation.

Mr. Aaronson received a Bachelor’s Degree in journalism from the University of Colorado at Boulder for his undergraduate studies, and a Master’s Degree from The George Washington University Graduate School of Political Management. He also has received continuing education in executive leadership from the University of Pennsylvania’s Wharton School of Business.

**Presentation: An All-Hazards Approach to Cyber Threats** – Electric companies prepare for contingencies against all threats, including cyber risks. Developing more resilient infrastructure to support national and economic security, as well as the life and safety of customers, is a responsibility shared by government and industry. This presentation will explore how the electric power industry is working with stakeholders to better defend its infrastructure, and preparing to respond and recover should any threat impact grid operations.
FRANCO CAPPA, Cybersecurity Advisor – CISSP, C|CISO, ITIL, Cybersecurity and Infrastructure Security Agency

Mr. Cappa is a Certified Information Systems Security Professional (CISSP) with over 30 years of experience in the Information and Communications Technology (ICT) industry, the majority of which dedicated to security—both in a cyber and physical environment. Mr. Cappa is highly skilled in recognizing potential security threats and assessing compliance with numerous security standards and regulations.

He has performed duties as team lead, supervisor and senior manager in both technical and non-technical delivery environments for multiple industries and sectors (e.g., Chief Information Security Officer for an intergovernmental organization and Director of Security Services in higher education among others). Mr. Cappa has worked in the management, design, architecture and implementation of security solutions for customers in Americas, Asia, Europe, Africa and the Middle East, on multi-million-dollar projects.

During his extensive career Mr. Cappa has delivered innovative solutions for the protection of information and assets in general. He is also an active contributor to security professional organizations and working groups like the International Information System Security Certification Consortium, or ISC2 and the National Institute of Standards and Technology (NIST)

Presentation: Homeland Security Perspectives for Building Cyber Security Capacity, Capability, & Resilience — The presentation describes the current landscape of threats to the nation’s infrastructure and how education and joint efforts between government and the private sector can protect us all from cyber criminals.
Major Christine Pierce has been working in the Information Technology field for the last 16 years and has served as the PA National Guard Cyber Branch Chief and Defensive Cyber Operations Element Team Chief for the last 5 years.

As the Cyber Branch Chief, she has worked on many cyber initiatives across the Commonwealth and within the PA National Guard. The initiatives included building and establishing the first cyber branch in the PA National Guard; establishing a Joint Cyber Training Facility at Fort Indiantown Gap; integral contributor to the PA cyber working group and the Pennsylvania Cyber Incident Annex; leading the state cyber training and exercise workgroup, and working with PA state and local governments, educational institutions, and private companies to provide cybersecurity assistance and cyber incident response across the Commonwealth.

Presentation: The Role of the National Guard in Domestic Cyber Operations and Incidents — The presentation will review the role of the National Guard in domestic cyber operations and how the PA cyber team can provide cybersecurity assistance to state and local government as well working with the private sector on cybersecurity concerns.
SECRETARY ROSEMARY CHIAVETTA, ESQ., Pennsylvania Public Utility Commission

Rosemary Chiavetta was appointed Secretary of the Pennsylvania Public Utility Commission on April 15, 2010. Prior to her return to the Commission, Secretary Chiavetta was the sole proprietor of Chiavetta Consulting specializing in legal advice and government relations for clients in the areas of public utilities, labor, health care, education, financial investments, mergers and acquisitions, and the environment.

Before entering private practice, Secretary Chiavetta served as an Assistant Counsel in the Commission’s Law Bureau from 1993 to 1995, as Counsel to former PUC Chairman John M. Quain from 1995 to 1997, and as the Commission’s Director of Legislative Affairs from 1997 to 1999, where she was instrumental during the passage and implementation of electric and telephone deregulation in Pennsylvania.

Prior to her first tour of duty at the Pennsylvania Commission, Secretary Chiavetta served as a Legislative Assistant and Counsel in the Pennsylvania House of Representatives from 1979 to 1993. Secretary Chiavetta earned a B.A. from the College of Notre Dame in Baltimore, Maryland, and received her J.D. from the Dickinson School of Law in Carlisle, Pennsylvania.

Presentation: How to Maintain Transparency in Government and Protect Confidential Security Information (CSI) — The presentation will address how the PUC complies with Pennsylvania’s Sunshine Act/Right to Know Law and secures CSI when requests to examine records containing security information are made by members of the public.
MATTHEW THOMAS, GSTRT, GISP, ReliabilityFirst - Manager, CIP Compliance Monitoring

Mr. Thomas is the Manager of Critical Infrastructure Protection (CIP) Compliance Monitoring at ReliabilityFirst and he is responsible for planning, developing, coordinating and overseeing the day-to-day operations of the CIP Compliance Monitoring processes and team. His primary responsibilities include development of the annual CIP audit plans to assess regional risk, providing oversight of compliance engagements and participation in ERO Enterprise initiatives and projects. Previously, Mr. Thomas held several positions throughout ReliabilityFirst as a CIP Auditor, Senior Application Developer and as a Senior Security Analyst.

Mr. Thomas is a graduate from the University of Dayton with a Bachelor of Science Degree in Business Administration with a concentration in Management Information Systems. Mr. Thomas holds his GIAC Information Security Professional and GIAC Strategic Planning, Policy and Leadership certifications.

Presentation: ReliabilityFirst’s Critical Infrastructure Protection Compliance Monitoring Program — An overview of the North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) Standards and how ReliabilityFirst (RF) performs compliance monitoring engagements of the Bulk Electric Systems’ users, operators and owners. The presentation will cover the methods RF uses to monitor compliance, review controls to ensure a sustainable compliance program exists and to assist entities in improving their security programs and posture.
PHYLLIS LEE, Senior Director of CIS Controls, Center for Internet Security

Ms. Lee is the Senior Director for Controls at the Center for Internet Security (CIS). She has over 20 years of experience in information assurance and has performed vulnerability assessments, virtualization research and worked in security automation. Prior to joining CIS, she worked at the National Security Agency (NSA).

Presentation: CIS Controls Implementation Group 1 and ICS — As IT and OT converge, it is more important for technical controls, like the CIS Critical Security Controls, are implemented across an ICS enterprise. This presentation will give an overview of Implementation Group 1 (IG1), CIS’ new prioritization scheme starting in Controls v7.1. IG1 is now being referred to as basic cyber defense. All organizations should be able to implement IG1 on their networks. We will also discuss how IG1 can defend against many of the most common attacks recorded against ICS systems.
KELLY MONAGHAN, MBA, CPA, CGFM, CFE, CISA, Director of the Bureau of Audits for the Pennsylvania Public Utility Commission

Ms. Monaghan has spent her professional career as an auditor in various roles for the Commonwealth of Pennsylvania. She is currently the Director of the Bureau of Audits for the Pennsylvania Public Utility Commission which is responsible for performing financial, management, operational and specialized audits on electric, natural gas, steam heat, wastewater, water and telecommunications utilities. The Bureau also reviews certain adjustment clause rate filings and 1307(e) reconciliation statements and a limited number of reviews of the annual assessment reports for transportation companies.

Ms. Monaghan received her Bachelor of Arts degree from Pennsylvania State University and a Masters of Business Administration in accounting. Her professional certifications include Certified Public Accountant (CPA), Certified Government Financial Manager (CGFM), Certified Fraud Examiner (CFE) and Certified Information Systems Auditor (CISA). Ms. Monaghan is an active member of the Association of Government Accountants (AGA) and serves as the Secretary on the NARUC Subcommittee on Accounting and Finance.

**Presentation: Traditional Audits, Internal Audit, and Cybersecurity Audits**

Audits — Audits are typically thought of solely as part of the financial management function. However, the corporate frauds of the 2000s and the disruptive technologies of the teens are causing businesses and governments to demand more from their auditors. Far from being a rubber stamp on an organization’s financial reporting, auditors are now part of utilities’ risk management, improving organizations’ ability to deal with threats and opportunities proactively. Ms. Monaghan’s presentation will explore how auditors address cybersecurity and how organizations can make sure they get the most value from their audits.
Mr. Keen has served as the Senior Energy Advisor for the National Risk Management Center, Cybersecurity and Infrastructure Security Agency, U.S. Department of Homeland Security (DHS) since the Center’s creation in July 2018. Prior to working with DHS, Mr. Keen served as a Division Director with the Office of the Utility Consumer Counselor for the State of Indiana, offering oral and written testimony in over 250 cases on topics covering a wide range of energy and telecommunication issues.

He is a highly decorated and retired Air Force officer and has a Masters Degree in Aeronautical Science with a Bachelor Degree majoring in Business Management.

**Presentation: Pipeline ICS - The Threat We May Not Realize** — The presentation will explore how the increasing commonality of ICS across sectors may be creating potential threats and vulnerabilities both within and across critical lifeline sectors. Mr. Keen will explore the potential threats posed by adversaries as well as how and why the adversary may use one sector against others and how this strategy could present significant issues for the planner seeking to mitigate or negate the threat/vulnerability.
MATTHEW D. DUNCAN, GCIP, Manager, Policy and Coordination, Electricity Information Sharing and Analysis Center

Mr. Duncan serves as the Policy and Coordination Manager at the Electricity Information Sharing and Analysis Center (E-ISAC), focusing on North American electricity industry resilience policy and cross-sector coordination.

Prior to the E-ISAC, Mr. Duncan was a Program Manager at the U.S. Department of Energy, managing sector specific agency and state government outreach. Other previous roles include: Deputy U.S. Political Officer at the Helmand Provincial Reconstruction Team in Afghanistan; a strategic Policy Analyst at the Pentagon; and a Research Assistant for a U.S. Attorney.

Mr. Duncan holds a Master’s Degree in International Relations from the Maxwell School of Citizenship and Public Affairs at Syracuse University, and a Bachelor’s of Arts in Political Science from Saint Joseph’s University in Philadelphia.

Presentation: GridEx V and the Role of the E-ISAC — ISAC will present on the upcoming GridEx V exercise that will be held November 13-14, 2019. The exercise is designed for distributed play, coordinated locally by a designated asset owner and operator lead planner. GridEx IV, held in November 2017, had more than 6,500 participants, representing 450 organizations. During the presentation, the E-ISAC will also cover its mission to reduce cyber and physical risk to the North American electricity industry, and how it coordinates with partners, including states.
Ms. Walker is a cybersecurity professional with over eighteen years’ experience supporting critical infrastructure and State, Local, Tribal & Territorial (SLTT) governments. Currently at WaterISAC, she assesses cyber threats facing the Water and Wastewater Sector. She also advises and consults on cyber threats related to homeland security for other critical infrastructure and vital lifeline sectors.

Ms. Walker is experienced in malware analysis, threat assessments, cyber threat intelligence, compliance, and cybersecurity awareness.

Presentation: Increase Cyber Resilience: 15 Cybersecurity Fundamentals for Water and Wastewater Utilities — There are myriad cyber threats facing the Water and Wastewater Sector, and the impacts of a cyberattack on a utility can be great. Although many water and wastewater utilities have invested significant time and resources in cybersecurity, more progress is necessary on the part of the sector to secure IT and OT systems. This presentation and its accompanying guide (15 Cybersecurity Fundamentals for Water and Wastewater Utilities) are intended to show a path toward that goal. In the spirit of information sharing and to greater enhance overall Water and Wastewater Sector resilience, this session is designed to be interactive so participants can share what is working (or not working) and lessons learned with utilities that may have fewer resources devoted to cybersecurity.
TECHNICAL TRACK

JEROME FARQUHARSON, MS, CISSP, CRISC, Sr. Principal Director, Regulatory Risk Management & Cyber Security, Senior Principal Director of Burns & McDonnell’s Regulatory Risk Management & Cyber Security Group.

Mr. Farquharson leads with a multi-disciplined background of cyber and physical security, information systems and business advisory consulting and has provided technology-oriented advisement for numerous Fortunes 500 companies across the nation and possesses crossindustry expertise. He possesses a unique blend of technical, business and project management skills to effectively provide value to diverse client and industry verticals.

Mr. Farquharson is an experienced Security Network Engineer with 14 years IT experience that includes experience in Network Design Implementation using the NIST, ISO, ISA and FISMA standards as well as 13 years of regulatory compliance experience with HIPPA, FERC, and NERC standards. He has performed numerous compliance audits for large investor owned utilities to determine the level of regulatory exposure and define mitigation strategies to minimize penalty.

Mr. Farquharson is actively involved with the NERC subcommittees and regional Information Systems Audit and Control Associations. His initiatives have helped define security, regulatory compliance and utility technology solutions for critical infrastructure organizations such as electric utilities, government facilities and process industries. Mr. Farquharson has also successfully completed the Fundamentals of Auditing for NERC Compliance Training Course.
Presentation: Utility Vulnerability, Threat, and Risk Management

— The U.S.’s cyber security approach to its critical infrastructure and Industrial Control Systems (ICS) has been a mix of voluntary guidelines and standards to regulated standards mandated by congressional actions, with a somewhat predictable outcome based on financial reporting and risk appetite of the enterprises. Federal regulations and standards, such as NIST, ISO27001 and FISMA, also drive IT-based system security. Critical infrastructure has moved from mechanical controls to digital technologies, computer networks and internet-driven devices. With each addition, the grid — along with the rest of the nation’s critical infrastructure — becomes increasingly vulnerable along with a constant evolving cyber threat landscape.

Every critical infrastructure entity cyber security and compliance team is using metrics to measure the effectiveness of their compliance program. It is important to acknowledge that “Not everything that counts can be counted, and not everything that can be counted counts.” Does the entity’s risk management program support the measures of the compliance & cyber program? Do the established metrics provide the entity with information and insight to assess risks and make the appropriate decisions?
JONATHON MONKEN, MBA, Senior Director, System Resilience and Strategic Coordination

Mr. Monken works to build enterprise-level resilience in the areas of business continuity, physical and cyber security, risk management, operations and planning for the largest grid operator in the world. He served as VP, U.S. Operations for the Electric Infrastructure Security Council working with government and industry to develop best practices and capabilities to improve the resilience of life support infrastructure systems to widespread, long-duration power outages, known as “Black Sky” events.

Mr. Monken also served as Director of the Illinois Emergency Management Agency (IEMA) and State Homeland Security Advisor from 2011 to 2015 where he oversaw Illinois’ disaster preparedness and response, nuclear safety and homeland security programs. At IEMA, Mr. Monken directed the response and recovery effort to 11 disasters including floods, blizzards, and tornadoes.

Mr. Monken also possesses a distinguished military career having served as an armor officer for one tour of duty in Kosovo and two combat tours in Iraq. Major Monken was awarded the Bronze Star Medal and the Army Commendation Medal with “V” Device for valor in combat. He is currently serving in the Army Reserves supporting the National Cybersecurity and Communications Integration Center (NCCIC) at the U.S. Department of Homeland Security. Mr. Monken earned a Bachelor of Science Degree from West Point and holds an MBA from Northwestern University.

Presentation: What is Cyber Resilience? — Resilience is a popular buzzword in critical infrastructure, but how does it apply to cybersecurity? Ultimately is comes down to a balanced approach that takes into every element of the cyber kill chain and reinforces the ability to prepare for, operate through, and recover from major events. The presentation will include discussion on the importance of underlying hardware and software flexibility and the role of risk assessment for prioritizing actions and capabilities.
DR. STEVEN McELWEE, PhD, MBA, CISSP, Chief Information Security Officer, PJM Interconnection

Dr. McElwee is the Chief Information Security Officer (CISO) at PJM Interconnection, which ensures the reliability of the high-voltage electric power system serving 65 million people in 13 states and the District of Columbia. He oversees the security risk management program at PJM, including threat and vulnerability management, supply chain cybersecurity, information protection, security monitoring and incident response, as well as IT compliance. He is engaged in a variety of industry, government, and academic collaborative partnerships.

Dr. McElwee holds a BA in Computer Science from Thomas Edison State College, an MBA from Alvernia University, an MS in Computer Information Systems from Boston University, and a PhD in Information Assurance from Nova Southeastern University. He has published papers on simulated spear phishing education as well as machine learning approaches for intrusion detection. He maintains the CISSP certification and is a member of the IEEE.

Presentation: Continuous Red Teaming to Find and Fix Vulnerabilities

— What vulnerabilities are lurking in your systems? Many security leaders trust that their policies, processes, and technologies are working to secure their systems and protect them against cyberattacks. Continuous red teaming challenges the assumptions that your security measures are effective. This presentation will discuss a case study of how PJM introduced continuous red teaming, the benefits it produced, and the lessons learned.