EUCI
SYMPOSIUM

FOSSIL PLANT PHYSICAL SECURITY AND CYBER RISK SYMPOSIUM

August 14-15, 2017
Millennium Knickerbocker Hotel Chicago
Chicago IL

TAG US #EUCIEvents
FOLLOW US @EUCIEvents

AUTHORIZED IACET PROVIDER

EUCI is authorized by IACET to offer 1.0 CEUs for the symposium

OVERVIEW

Power generators today face unprecedented challenges when it comes to both physical and cyber security. Given the immense amount of power generated and critical role power plants play in the nation's infrastructure, the cost of a security breach goes beyond mere financial damage – it can affect the safety of an entire region. For this reason alone, it is imperative for utilities and plant managers to initiate effective security protocols within their operating budgets.

Cyber security attacks on infrastructure targets are happening with increased sophistication and frequency. Each power generation site has a complicated collection of controls that may include both legacy systems and smart assets. Each system presents challenges that range from patching to the introduction of an entire array of not-well-understood vulnerabilities. Many plants are old, and upgrading them is more than a simple matter of adding new technologies. Old systems may need to be replaced or upgraded as well. When new technologies are built on top of legacy systems, new risks may emerge as different systems interact.

The Fossil Plant Physical Security and Cyber Risk Symposium gives plant managers, plant operators, heads of physical, cyber and corporate security a full understanding of what is at stake when it comes to securing their plant and how they can ensure the safety and security of their operations. The symposium will cover the role of fossil fuel plants as part of the nation's critical infrastructure. Attendees will learn to recognize the external drivers and regulatory requirements for plant physical security. They will learn to organize their plant for cyber and physical security as well as safety. Attention will be paid to how to assess and upgrade a plant's current security organization. Experts will review how to apply cyber security guidelines and advanced technologies for power generation security programs. Finally, there will be a "utilities Q&A" so attendees can ask their own questions of how utilities are handling their security protocols.

LEARNING OUTCOMES

- Reduce risk by securing critical infrastructure against human, physical and cyber threats
- Examine costs and benefits of security investments
- Comply with NERC regulations
- Identify mitigation efforts that will ensure rapid recovery of plant operations in the case of security breaches
- Recognize where cyber security and physical security overlap
- Set benchmarks for intrusion detection, perimeter patrol, lighting
- Effectively upgrade security protocols when responsibilities are transferred from one department to another
- Bring older facilities up to current standards
- Explain fossil plants' role as part of the country's critical infrastructure
- Establish rapid response and recovery protocols in the case of a cyber security breach
- Define current threats to plant security based on recent incidents
- Discuss the intersection between plant safety and security

WHO SHOULD ATTEND

- From Utilities
  - Directors of Plant Management
  - Plant Operators
  - Heads of Security
  - Cyber and Corporate Security
- Security Companies
- Software Companies
- Law Firms
- Engineering Firms

AGENDA

MONDAY, AUGUST 14, 2017

8:00 - 8:30 am **Registration & Continental Breakfast**

8:30 - 9:30 am **Keynote Presentation: Fossil Fuel Plants as Critical Infrastructure**

Seventy percent of the country's 6,413 power generation plants run on fossil fuel. Virtually all industries rely on electric power, making the security of these plants a matter of concern for everyone. The majority of energy infrastructure is owned and operated by the private sector, resulting in a complex network of companies, agencies, and organizations that must coordinate in order to ensure security and resilience of the grid. This presentation will discuss:

- Assessing security risks and threats to fossil fuel generation plants
- Securing critical infrastructure from all hazards
- Enhancing critical infrastructure resilience
- Sharing information to enable risk-informed decision making
- Adopting learning and adaptation in the face of changing conditions

Alex Joves, Office of Infrastructure Protection, US Department of Homeland Security

9:30 - 10:30 am **Recognizing External Drivers and Regulatory Requirements for Plant Physical Security**

- Review the history of the NERC Physical Security Standard CIP-014-2
- Examine the events that shape today's thinking on plant security
  - o Evaluate how to use lessons learned from previous events to make your plant more secure
    - Expand your understanding of what risks your plant may face
    - Share best practices for plant security that have evolved in response to past attacks
  - o Putting protocols into effect that will protect your plant from threats and vulnerabilities revealed by the Metcalf Substation attack
- Preparing to comply with CIP-014-2 Mandatory Requirements
- Recognize how NERC implements compliance monitoring and actions

David Hilt, President, Grid Reliability Consulting

10:30 - 11:00 am **Networking Break**

11:00 - 11:30 am **Recognizing External Drivers and Regulatory Requirements for Plant Physical Security (Continued)**

11:30 am - 12:30 pm **Group Luncheon**

12:30 - 1:30 pm **Organizing Your Plant for Cyber and Physical Security**

- Clarifying cyber requirements vs. physical requirements
  - o Defining "culture of compliance" across the responsible areas
  - o Communicating about risk and strategies to build, communicate, and demonstrate a culture of compliance as mandated by NERC
- Organizing for compliance
  - o Identifying the functional groups involved in plant security
  - o Examining the difference between decentralized and centralized corporate security
  - o Evaluating options for organization
- Dealing with NERC
  - o Recognizing how NERC compliance fits with other enterprise compliance needs and risk management
  - o Stressing the need for a culture of compliance, and how to implement it.
  - o Maintaining confidentiality of critical infrastructure and compliance
  - o Demonstrating a culture of compliance to auditors for the CIP standards
  - o Managing security related documentation and evidence

David Hilt, President, Grid Reliability Consulting

AGENDA

MONDAY, AUGUST 14, 2017 (CONTINUED)

1:30 - 2:30 pm **Assessing Plant Physical Security from a Newcomer's Perspective**

- Assessing an established organization for security risk factors
- Fortification of existing intrusion detection
- Intrusion detection and monitoring
- Policies and programs
- Integrating company culture with new initiatives

Jason Maldonado, Security, Emergency Manager, Platte River Power Authority
Justin Allar, Security Systems Operator, Platte River Power Authority

2:30 - 3:00 pm **Networking Break**

3:00 - 4:00 pm **Navigating the Overlap Between Safety and Security**

- Regulatory compliance and what drives it
  - NERC/FERC requirements
  - OSHA requirements
- Duty to protect employees
  - Threats of workplace violence
- Emergency management and incident response
  - Roles of safety professionals versus security professionals

Jason Maldonado, Security, Emergency Manager, Platte River Power Authority
Justin Allar, Security Systems Operator, Platte River Power Authority

4:00 - 5:00 pm **Fossil Fuel Power Generation Plant Security Q&A for Utilities**

Security heads for utilities will take the stage to offer insights to questions from the audience.
Panelists:
Joe VonDer Haar, Plant Manager, East Kentucky Power Cooperative
Jason Maldonado, Security, Emergency Manager, Platte River Power Authority
Justin Allar, Security Systems Operator, Platte River Power Authority

5:00 pm **Day One Adjourns**

TUESDAY, AUGUST 15, 2017

8:00 - 8:30 am **Continental Breakfast**

8:30 - 10:00 am **Cyber Security Guidelines and Advanced Technologies for Power Generation Security Programs**

This session shares an overview of research commissioned by the Electric Power Research Institute (EPRI) in concert with 16 different companies to develop guidelines for cyber security programs for power generation.

The research is designed to develop new capabilities in key applied research areas:

- Evaluating and developing risk-based approaches for new and existing threats to protect generation assets from a cyber incident
- Real-time identification of a generation cyber incident
- Established and practiced approaches and contingencies to rapidly respond to and restore from any power generation cyber incident

Learn how power generation companies are handling security, including best practices and recognized gaps that need to be addressed in the following areas:

- Interactive remote access
- Configuration management and hardening cyber assets
- Patch management
- Access and permission management
- Real-time detection
- Scanning
- Security status monitoring
- Reference architecture

Justin Thibault, Senior Technical Leader, Electric Power Research Institute (EPRI)

10:00 - 10:30 am **Networking Break**

10:30 am - 12:00 pm **Cyber Security Guidelines and Advanced Technologies for Power Generation Security Programs (Continued)**

12:00 pm **Conference Adjourns**

INSTRUCTORS

Alex Joves

Office of Infrastructure Protection, US Department of Homeland Security

Alex Joves is the U.S. Department of Homeland Security (DHS), National Protection & Programs Directorate (NPPD), Office of Infrastructure Protection (IP) Regional Director for Federal Region V (Illinois, Indiana, Michigan, Minnesota, Ohio, Wisconsin).

As IP Regional Director since June 2016, he leads IP's efforts across Region V to strengthen public-private partnerships and coordinate programs to protect the Nation's critical infrastructure, assess and mitigate risk, build resilience, and strengthen incident response and recovery. Mr. Joves joined IP in 2012 as Director, National Infrastructure Coordinating Center (NICC) – the national focal point for 24/7 situational awareness and integrated actionable information to secure the Nation's critical infrastructure. Within Region V, he also served in the field as a Supervisory Chemical Security Inspector overseeing regulatory inspections of chemical facilities posing high-risk of vulnerability to terrorist attack and/or theft or diversion of hazardous chemicals under the Chemical Facility Anti-Terrorism Standards (CFATS), 6 CFR 27.

Mr. Joves is a graduate of the U.S. Coast Guard Academy (Bachelor of Science) and The George Washington University Law School (Juris Doctor). Formerly, he was an attorney in private practice. The DHS Office of Infrastructure Protection Region V office is based in Chicago, IL.

Jason Maldonado

Security, Emergency Manager, Platte River Power Authority

Jason Maldonado joined Platte River Power Authority in 2016 as the Manager of Security, Emergency Management, and Safety. In this role, Jason oversees the implementation of Platte River's Security and Safety programs as well as the staff in each department. As a Safety and Health professional, Jason has worked in a wide variety of industries including: defense, heavy construction, industrial chemical operations, and electric utilities. His career focus has always been to educate and empower through teaching employees the why behind policies and procedures. Jason is a Certified Safety Professional (CSP) and Certified Reliability Leader (CRL) intent on helping make Platte River a safer and more secure company through the application of his unique experience and outlook.

Justin Allar

Security Systems Operator, Platte River Power Authority

Justin Allar joined Platte River Power Authority in 2016 as their Security Operations Supervisor. In this role he currently oversees the Physical Security of critical cyber assets, personnel, and locations. He previously worked at Concentric Advisors for eight years providing physical security and close protection for Bill Gates. Prior to this role Justin worked at a Global Security Operations Center, as a Watch Commander for a private family supervising security operations worldwide. Justin is also a veteran of the US Air Force serving from 2001 to 2005 as a Security Forces Raven. He provided physical security for nuclear weapons in Montana, and spent two years overseas stationed in Guam. Justin also completed his Bachelor's degree in Management from American Military University graduating Magna Cum Laude, and has an Associate's degree from Bellevue College.

INSTRUCTORS

Joe VonDer Haar

Plant Manager, Spurlock Power Station East Kentucky Power Cooperative

Joe VonDerHaar has over 30 years of experience split between the utility and manufacturing industries. On the utility side he has held positions in System Operations, Transmission & Distribution and Power Generation. On the manufacturing front he was a Plant Manager for a Power Transmission OEM. A common thread in both industries is the tremendous change in process and mission as a result of competition and regulation. Being able to adapt and even welcome change is critical to success. Joe is currently the Plant Manager at the Spurlock Power Station, a 4-unit, coal fired, 1500MW facility in Maysville Kentucky. He holds an engineering degree from the University of Dayton.

Justin Thibault

Senior Technical Leader, Electric Power Research Institute (EPRI)

Justin Thibault, P.E. is a Senior Technical Leader with the Electric Power Research Institute's (EPRI) Generation Sector include managing research & developing solutions to technical challenges for our members in Controls System Cyber Security coordinating research with EPRI's technical sectors (Generation, Nuclear, Power Delivery and Environment) as the project manager of the Generation Cyber Security collaborative project. Justin has worked for nearly 20 years in the power generation in both fossil and nuclear in Engineering, Software Development, Equipment Reliability, Operations and Maintenance and Cyber Security.

David Hilt

President, Grid Reliability Consulting

David W. Hilt has nearly 40 years of experience in electric power system engineering, operation, and regulatory activities. He has been a manager responsible for the design, specification, and construction of electric substations from distribution to EHV including protective relaying. He has also managed transmission and resource planning activities for a major Midwestern electric and natural gas utility providing expert testimony before FERC and state regulators for transmission expansion and 20 year resource plans. Mr. Hilt has directed the development and installation of state estimation and OASIS systems for a Midwestern Reliability Coordination Center. As a Vice President at NERC, he led the development of the compliance monitoring and enforcement program for the bulk-power system reliability standards in North America working closely with the industry, FERC, and Canadian regulatory authorities. He also developed audit programs and event analysis and investigation prorocess. While at NERC he led the investingation of the August 2003 blackout in the Northeastern United States and Canada providing the technical input to the U.S. – Canada Power System Outage Task Force report. Mr. Hilt's recent experience includes assessment of risk from physical attack and grid resiliency.

INSTRUCTIONAL METHODS

Case studies, PowerPoint presentations, group discussion

REQUIREMENTS FOR SUCCESSFUL COMPLETION

Participants must sign in/out each day and be in attendance for a minimum of four hours to be eligible for any continuing education credit.

IACET CREDITS

EUCI has been accredited as an Authorized Provider by the International Association for Continuing Education and Training (IACET). In obtaining this accreditation, EUCI has demonstrated that it complies with the ANSI/IACET Standard which is recognized internationally as a standard of good practice. As a result of their Authorized Provider status, EUCI is authorized to offer IACET CEUs for its programs that qualify under the ANSI/IACET Standard.

EUCI is authorized by IACET to offer 1.0 CEUs for the symposium

EVENT LOCATION

A room block has been reserved at the Millennium Knickerbocker Hotel Chicago, 163 E Walton Place, Chicago, IL 60611, for the nights of August 13-14, 2017. Room rates are $189 plus applicable tax. Call **1-312-751-8100** for reservations and mention the EUCI event to get the group rate. The cutoff date to receive the group rate is July 16, 2017 but as there are a limited number of rooms available at this rate, the room block may close sooner. ***Please make your reservations early.***

REGISTER 3, SEND THE 4TH FREE

Any organization wishing to send multiple attendees to this event may send 1 FREE for every 3 delegates registered. Please note that all registrations must be made at the same time to qualify.

REGISTRATION
to register CLICK HERE or

Call: 201 871 0474
fax: 253 663 7224
email: register@pmaconference.com/
web: http://pmaconference.com/
Mail: POB 2303 Falls Church Va 22042

Please make checks payable to: "PMA"

EVENT LOCATION

A room block has been reserved at the Millennium Knickerbocker Hotel Chicago, 163 E Walton Place, Chicago, IL 60611, for the nights of August 13-14, 2017. Room rates are $189 plus applicable tax. Call **1-312-751-8100** for reservations and mention the EUCI event to get the group rate. The cutoff date to receive the group rate is July 16, 2017 but as there are a limited number of rooms available at this rate, the room block may close sooner. ***Please make your reservations early.***

PLEASE REGISTER

◯ **FOSSIL PLANT PHYSICAL SECURITY AND CYBER RISK SYMPOSIUM SYMPOSIUM**
AUGUST 14-15, 2017 | CHICAGO IL: US $1395
Early bird on or before July 28, 2017: US $1195

◯ I'm sorry I cannot attend, but please email me a link to the symposium proceedings for US $295

How did you hear about this event? (direct e-mail, colleague, speaker(s), etc.)

Print Name | Job Title

Company

What name do you prefer on your name badge?

Address

City | State/Province | Zip/Postal Code | Country

Phone | Email

List any dietary or accessibility needs here

CREDIT CARD INFORMATION

Name on Card | Billing Address

Account Number | Billing City | Billing State

Exp. Date | Security Code (last 3 digits on the back of Visa and MC or 4 digits on front of AmEx) | Billing Zip Code/Postal Code

OR Enclosed is a check for $ _____ to cover _____ registrations.

Substitutions & Cancellations
Your registration may be transferred to a member of your organization up to 24 hours in advance of the event. Cancellations must be received on or before July 14, 2017 in order to be refunded and will be subject to a US $195.00 processing fee per registrant. No refunds will be made after this date. Cancellations received after this date will create a credit of the tuition (less processing fee) good toward any other EUCI event. This credit will be good for six months from the cancellation date. In the event of non-attendance, all registration fees will be forfeited. In case of course cancellation, EUCI's liability is limited to refund of the event registration fee only. For more information regarding administrative policies, such as complaints and refunds, please contact our offices at (201) 871-0474.