

PRE-SUMMIT WORKSHOP DAY | September 18, 2017

Attend the Pre-Summit Workshop Day to create a secure system architecture for industrial control

The Pre-Summit Workshop Day focuses on **Detection, Deterrence and Awareness** methods. Security professionals will work together to identify potential threats and strategize solutions to create a resilient power system. Ultimately, sessions will build the framework for a secure industrial control system.

8:30 AM

REGISTRATION

9:00 AM

DETECTION: IDENTIFY THE PRESENCE OF CONCEALED THREATS TO THE GRID WITH ENHANCED SURVEILLANCE CAPABILITIES *[SECURITY LEADER BREAKFAST SESSION]*

- Overview of detection projects and requirements
- Methods to determine “smoking hole” in power system
- New developments in subsystem security enhancements

10:45 AM

MORNING NETWORKING & REFRESHMENT BREAK

11:00 AM

DETERRENCE: APPLY INDUSTRY BEST-PRACTICES BY CREATING A SECURE ARCHITECTURE FOR INDUSTRIAL CONTROL SYSTEMS

- How to piece it all together: tech/business process, policy and internal controls
- Apply good data hygiene to best utilize new technology and information systems
- Strategies to limit hacker sphere of influence

Speaker: Erfan Ibrahim, Center Director, **National Renewable Energy Laboratory (NREL)**

12:45 PM

NETWORKING LUNCH

1:45 PM

AWARENESS: INCREASE PERCEPTION OF SYSTEM VULNERABILITIES AND POTENTIAL REGULATORY CHANGES

- Anecdotal evidence of recent system threats
- Potential dangers of attacks and weather related disruptions
- Developments on national cybersecurity strategy and CIP compliance

3:00 PM

AFTERNOON NETWORKING & REFRESHMENT BREAK

MAIN SUMMIT DAY ONE | September 19, 2017

7:30 AM

REFRESHMENTS & REGISTRATION

8:30 AM

CHAIRPERSON'S WELCOME & OPENING REMARKS

8:45 AM

PHYSICAL ACCESS CONTROL FRAMEWORKS USED TO SECURE THE PERIMETER

- Security processes, training and detection methods
- Strategies to take corrective action and remain compliant with NERC standards
- Criteria/capabilities needed to protect substations
- Dialogue on potential regulatory changes and how to prepare

Speaker: **David Carroll**, Substation Automation, **Pacific Gas and Electric**

9:30 AM

IMPROVE DISTRIBUTED GENERATION WITH SUSTAINABLE MICRO-GRIDS

- Military use of micro-grid to make Cape Cod Air Force Station self-sufficient
- Use of existing wind turbines for directed energy use
- Cost-effective technologies and methods to address high-priority environmental requirements

Speaker: **Shawn Doyle**, Deputy Commander/Base Civil Engineer, **Otis Air National Guard Base**

10:15 AM

MORNING NETWORKING & REFRESHMENT BREAK

10:45 AM

HOMELAND SECURITY: SAFEGUARDING CRITICAL INFRASTRUCTURE FROM CYBER THREATS

- Suite of cyber security tools from the U.S. Department of Homeland Security
- Overview of National Cyber Security Division efforts to secure cyber assets and networks
- Cyber security evaluation, onsite assessment and resilience review planning

Speaker: **Kelly Wilson**, Protective Security Advisor-San Diego District, **U.S. Department of Homeland Security [Pending]**

MAIN SUMMIT DAY ONE | September 19, 2017

11:30 AM	DETERMINE PREPARATION AND RESTORATION STRATEGIES IN EXTREME WEATHER EVENTS <ul style="list-style-type: none">▪ Overview of National Grid Rhode Island Storm Room operations▪ Case study of Tropical Storm Irene preparation and restoration activities▪ Managing critical command centers in high pressure situations: Training, Drills, Exercises
12:15 PM	THEMED LUNCH TABLES: NETWORKING AND DISCUSSING THE CHALLENGES OF PHYSICAL AND CYBERSECURITY – DETECTION, DETERRENCE, AWARENESS
1:15 PM	FIRESIDE CHAT: AGILE CYBERSECURITY RESILIENCE <ul style="list-style-type: none">▪ End-user roundtable discussion with cybersecurity leaders▪ Methods to remain agile in detection and deterrence of concealed threats▪ Open discussion on strategies to facilitate CIP compliance via controlled access within substations Speaker PENDING: Hosted by Ben Tatera , Cybersecurity Principal, Pacific Gas and Electric
2:00 PM	AFTERNOON NETWORKING & REFRESHMENT BREAK
2:15 PM	PANEL: SYSTEM WIDE RESILIENCE – CONNECTING THE DOTS <ul style="list-style-type: none">▪ Creating a robust system architecture to ensure business continuity▪ Preparing for emergency situations and establishing response systems Speakers: Dennis Snook , Emergency Preparedness and Business Continuity Manager, Omaha Public Power
3:00 PM	CONDUCT PERFORMANCE BASED TESTING IN ORDER TO VALIDATE PLANS AND PROCEDURES <ul style="list-style-type: none">▪ “Red cell evaluation” techniques for critical infrastructure security programs▪ Flexibility and designs for utilities to remain current with physical and cyber developments
3:45 PM	CHAIRPERSON’S CLOSING REMARKS
4:30 PM	COCKTAIL HOUR / MURDER MYSTERY EVENT

MAIN SUMMIT DAY TWO | September 20, 2017

8:00 AM

REFRESHMENTS AND REGISTRATION

8:30 AM

CHAIRPERSON'S WELCOME & OPENING REMARKS

8:45 AM

CREATE A FRAMEWORK FOR INDUSTRIAL CONTROL SYSTEMS IN ORDER TO AUTOMATICALLY MANAGE DISTRIBUTION PROCESSES IN THE EVENT OF DISRUPTION

- Overview of ICS planning and controls
- Technological requirements to detect vulnerability
- Interactive session on communicating cybersecurity needs given changing threat dynamics

9:30 AM

INTERACTIVE SESSION: END-USER ROUNDTABLE ON PROTECTING THE GRID

10:15 AM

MORNING NETWORKING & REFRESHMENT BREAK

10:45 AM

LOW IMPACT BES FACILITIES: SUPPLY CHAIN REQUIREMENTS AND ACCESS CONTROL PLANNING

- Monitor upcoming regulatory changes and establish internal controls procedure
- Supply chain requirements under NERC regulation changes
- Control physical access based on low impact BES facility needs

Speaker: Linda Jacobson-Quinn, Regulatory Compliance Manager, **Farmington Electric Utility System**

11:30 AM

INNOVATION WALK-AROUND: ENGAGE WITH INNOVATORS DESIGNING SMART-GRID SOLUTIONS

12:15 PM

NETWORKING LUNCH

1:15 PM	TRACK 1: PHYSICAL SECURITY <ul style="list-style-type: none">▪ Regulatory perceptions of vulnerabilities and potential threats around the perimeter▪ Potential new requirements in CIP 014 language and data requests▪ Modernizing the Grid: drafting a distribution resource plan focused on storage and response	TRACK 2: CYBER SECURITY <ul style="list-style-type: none">▪ Advancements in detection software and applications▪ Requirements for IT risk management systems▪ Integrating cyber security network with access control programs
2:00 PM	CLOSED-DOOR SECURITY LEADER THINK TANK BUILD A RESILIENT POWER SYSTEM USING METHODS TO ASSESS SITE VULNERABILITY <ul style="list-style-type: none">▪ Developing information protection programs▪ Simulation techniques to determine criticality of substations▪ Identifying potential gaps in grid security programs	WORKSHOP TRACK: SUPPLYING NEW PRODUCTS AND SERVICES TO UTILITIES <ul style="list-style-type: none">▪ Best in class security equipment: barriers, fencing, shielding▪ Current demands for physical and cyber solutions to protect the grid▪ Methods to integrate new equipment in substation resiliency programs, ready for audit
2:45 PM	AFTERNOON NETWORKING & REFRESHMENT BREAK	
3:15 PM	IMPROVE WEATHER DETECTION SYSTEMS IN ORDER TO REDUCE SYSTEM DISRUPTIONS <ul style="list-style-type: none">▪ Software capabilities to detect and prevent weather related disruptions to the grid▪ Integrating technologies throughout systems to efficiently distribute power▪ GIS uses to enhance visibility of terrain in order to protect perimeter and safeguard against disruption	
4:00 PM	CHAIRPERSON'S CLOSING REMARKS	
4:45 PM	END OF MAIN SUMMIT DAY TWO	