8th Annual Security Summit

Tuesday, September 25th

Noon - 7:00	Vendor & Guest Registration	
Noon - 1:30	**National Electric Sector Cybersecurity Organization Advisory Board Meeting (closed session)**	
1:30 - 4:30	Pre-Summit Workshop NERC CIP-007 Deep Dive	Pre-Summit Workshop Assessing & Auditing Control Systems with Nessus
4:30 - 6:00	**EnergySec Board of Directors Meeting (closed session)**	
7:00 - 7:45	**Welcome Address** Patrick Miller, President and CEO of EnergySec and Principal Investigator of NESCO	
8:00 - 10:00	Hosted Welcome Reception	
10:00 - Midnight	**Birds of a Feather Sessions** (see information board at event)	

Wednesday, September 26th

7:00 - 4:00	Vendor & Guest Registration	
7:00 - 8:00	Hosted Breakfast	
8:00 - 8:15	Welcome	
8:15 - 8:45	Opening Keynote Address - Richard Clarke	
8:45 - 9:30	Make Your Employees Mal-AWARE: Implementing a Scalable Behavior Modification Program	
9:30 - 10:00	Hosted Networking Break	
	Compliance Track	**Technical Track**
10:00 - 10:45	Regulation, CIP is Only the Beginning	Doubt, Deceit, Deficiency and Decency - A Decade of Disillusionment
10:45 - 11:30	NERC CIP Access Monitoring: What Constitutes a Shared Account?	Detecting Malware Without AntiVirus
11:30 -1:00	Hosted Lunch Break	
1:00 - 1:45	ES-C2M2 Case Study	Substation Remote Access - Entergy Style
1:45 - 2:30	Behind the Curtain: *the challenge as seen through the eyes of a CIP auditor*	Identifying and Managing Network Zones in CIP-005
2:30 - 3:00	Hosted Networking Break	
3:00 - 3:45	Grass Roots Compliance: *how communities improve compliance*	Keys to a more Successful Security Program
3:45 - 4:30	Privacy Fact & Fiction: *what you really need to know*	All My Exes: *a view of the industry from those who have left*

Wednesday, September 26th continued

4:30 - 5:00	Regulation and Policy Roundtable	Best Practices Managing Ports and Services
5:00 -7:00	Hosted Reception	
7:00 - 10:00	**Birds of a Feather Sessions** (see information board at event)	

Thursday, September 27th

7:00 - 11:30	Vendor & Guest Registration	
7:00 - 8:00	Hosted Breakfast	
8:00 - 8:15	Welcome	
8:15 - 8:45	Can You Regulate Attitude? - Steven Parker	
8:45 - 9:30	The Power of Community - Deb Bryant	
9:30 -10:00	Hosted Networking Break	
	Compliance Track	**Technical Track**
10:00 - 10:45	The View From Here: a state regulator's perspective	The Stories We Could Tell: *lessons learned in the field*
10:45 - 11:30	Plenary Session - Seán McGurk	
11:30 -1:00	Hosted Lunch Break	
1:00 - 5:00	National Electric Sector Cybersecurity Organization Town Hall Meeting	
5:30 - Midnight	Spirit Mountain Casino Night (no-cost but registration is required)	

Friday, September 28th

8:00 - 9:00	Summit Advisory Board Breakfast
9:00 - 5:00	CISO Forum (invitation only)

Conference Sessions

Session Details: Compliance Track | Technical Track | Plenary Session

Tuesday, September 25th

1:30 - 4:30 **CIP-007 Deep Dive**

Steve Parker, VP of Technology Research and Projects and EnergySec and NESCO
This workshop will get into the nitty gritty details of CIP-007 covering many technical aspects of security log management, account management, security testing and more. This will be specific to control environments and directly related to what needs to be implemented and managed to help meet the NERC CIP standard requirements. Steve Parker is a former NERC CIP auditor with a vast amount of practical experience in the field. Join this workshop to learn from his experiences and expertise.

1:30 - 4:30 **Assessing and Auditing Control Systems with Nessus Workshop**

Reid Wightman, DigitalBond
The default scan in Nessus Vulnerability Scanner is powerful, but not appropriate for control systems and does not take full advantage of the tool's capabilities. In this course students will learn the most effective way to use Nessus to assess and audit control systems. There are techniques to significantly lessen the impact and risk of a scan. Special configuration settings can check for default credentials in databases and other applications. Bandolier security audit templates can compare settings to an ICS vendors recommendations and more. In this course, taught by Digital Bond, students will use their own laptop and learn how best to use Nessus as a security tool on their SCADA or DCS.

Wednesday, September 26th

8:15 - 8:45 **Opening Keynote Address**

Richard Clarke, Good Harbor
Cyber risks to the electric power industry have become increasingly significant in recent years and will continue to grow with the adoption of new networked technologies. As a result, the electric industry faces increasing oversight and scrutiny from regulators, legislators, executive government agencies, insurers, and others. Because of the severe financial, legal, operational, and reputational consequences cyber risks pose, responsibility for managing these risks must reside with senior corporate executives. In his keynote, Richard Clarke will discuss how electric power executives can manage these risks through improvements in internal governance, application security development processes, vendor risk management, and crisis preparedness.

8:45 - 9:30 **Make Your Employees Mal-AWARE: Implementing a Scalable Behavior Modification Program**

Rohyt Belani, CEO of PhishMe
Cyber crime and electronic espionage, most commonly, initiate with an employee clicking a link to a website hosting malware, opening a file attached to an email and laden with malware, or just simply giving up corporate credentials when solicited via phishing websites.

Phishing has been used to hijack online brokerage accounts to aid pump n' dump stock scams, compromise government networks, sabotage defense contracts, steal proprietary information on oil contracts worth billions, and break into the world's largest technology companies to compromise their intellectual property. Technical controls presented as silver bullets provide false hope and a false sense of security to employees, promoting dangerous behaviors. This continued threat makes it more important than ever for companies to provide an effective security awareness program to users on their networks. During this talk, I will present the techniques used by attackers to execute these attacks, and real-world cases that my team have responded to that will provide perspective on the impact. I will then discuss countermeasures that have been proven to be effective and are recommended by reputed bodies like SANS. It's about more than awareness training, it's about modifying employee perception of phishing emails and the responses to these types of attacks.

10:00 - 10:45 **Regulation: CIP Is Only the Beginning**

Prudence Parks, Director of Government Affairs and Legislative Counsel for UTC
The availability of spectrum for utility communications networks, heightened consumer protection and privacy concerns, cloud computing and its application to the smart grid, supply chain security – these are just some of the policy and regulatory issues that could have a significant impact on utilities as they integrate millions of data points for more efficient control of the modernized grid. Attention has been focused on compliance with NERC-CIP mandates and passing audits, but what is their place in the broader security picture? Will other policy developments change the landscape of grid security?

10:00 - 10:45 **Doubt, Deceit, Deficiency and Decency - A Decade of Disillusionment**

James Arlen, Push the Stack Consulting
It's been nine years since the oft quoted Blackout of 2003. It's been nine years since Urgent Action Standard 1200. It's been eleven years since I began seriously working in the utility space. I cannot escape the feeling that I have wasted a decade of my life. Can I prove myself wrong? Through a mixture of news stories, teachable moments, hard-won experience and perhaps an interpretive dance - you will be taken on a journey of maturity and self-discovery -- an examination and ultimately a determination on one information security professional's decade of trying to make a difference.

*NOTE: Due to union regulations there shall be no interpretive dance.

10:45 -11:30 **NERC CIP Access Monitoring: What Constitutes a Shared Account?**

Spencer Wilcox, Excelon
NERC CIP standards 003-007 define access and shared accounts. What constitutes a shared account? Does your IAM account for all personnel with access to your UNIX and Windows systems? This presentation will explore the intricacies of access, and help you to better document your access and account management evidence leading up to your next audit.

10:45 -11:30 **Detecting Malware Without AntiVirus**

Jeff Bryner, P0wn Labs
When it comes to actual, real-world, active malware detection there are surprisingly few choices. Most companies invest in one anti-virus vendor and when they suspect a compromise they simply wait for them to issue signatures. If a company thinks they may be compromised but there is no AV signature, then what? What if we could use basic python scripting to identify malware based on signatures we produce in real time? There are plenty of python tools, scripts and frameworks for malware identification including yara, pefile, nsrl hash db, pyemu, hachoir, volatility and pyew. What if we could integrate these together into a system for centrally issuing indicators of compromise? What if hosts we suspect as being compromised used this system to check themselves for compromise? Lets find out... What if we could integrate these together into a system for centrally issuing. indicators of compromise? What if hosts we suspect as being compromised used this system to check themselves for compromise? Lets find out...

1:00 - 1:45 **ES-C2M2 Case Study**

Benjamin, Beberness, Snohomish PUD
John Fry, ICF International
The Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2), which allows electric utilities and grid operators to assess their cybersecurity capabilities and prioritize their actions and investments to improve cybersecurity, combines elements from existing cybersecurity efforts into a common tool that can be used consistently across the industry. The ES-C2M2 was developed as part of a White House initiative led by the Department of Energy in partnership with the Department of Homeland Security (DHS) and involved close collaboration with industry, other Federal agencies, and other stakeholders. This presentation covers a real world “case study” of how this ES-C2M2 work can easily be adapted to improve cyber security at your organization.

1:00 - 1:45 **Substation Remote Access - Entergy Style**

Chris Sistrunk, Entergy
Increasing cyber threats and changing NERC/CIP standards have caused Entergy to design and implement a new system for substation remote access. This system provides the access that engineers and technicians need, utilizes security best practices, leverages existing equipment, and is poised for future expansion and technologies.

1:45 - 2:30 **Behind the Curtain: the challenge as seen through the eyes of a CIP auditor**

Josh Axelrod, Ernst & Young - Moderator
Matt Stryker, SERC
Brent Castegnetto, WECC
Darren Nielsen, WECC
This panel of current NERC CIP Auditors will share their perspectives about the various challenges entities are facing with regard to demonstrating compliance. The moderator will be asking tough questions about the consistency of approaches amongst the Regional Entities, the impact of Compliance Application Notices on the audit process, and their thoughts on the maturation of Technical Feasible Exceptions.

1:45 - 2:30 **Identifying and Managing Network Zones in CIP-005**

Edmond Rogers, Information Trust Institute, University of Illinois
Urbana Champaign - Identifying and managing network zones for CIP compliance can require long hours of effort in review of visio diagrams. The presentation will provide an overview of the issues that administrators face when dealing with the challenges of providing for documentation that can be flexible and meet both operational and compliance needs in regards to identifying and managing network zones within a critical infrastructure network. The presentation will close with an overview of Network Access Policy Tool (NetAPT). NetAPT is designed to provide for automated documentation of network trust zones.

3:00 - 3:45 **Grass Roots Compliance: how communities improve compliance**

Lisa Carrington, EnergySec - Moderator
Karl Perman, National Transmission Forum
Matt Jastram, Western Interconnection Compliance Forum
John Heintz, ERCOT CIP Working Group
Josh Sandler, North American Generator Forum

Often the most powerful and successful efforts start with a few people coming together to solve a problem. In the past 5 years a number of “compliance communities” have sprung up across North America. Panelists give their individual takes on how they are using these communities to keep up on current industry-specific security regulatory developments and how they are sharing this information with the forums they represent. The panel will discuss the challenges of providing relevant information to their constituencies, communication strategies, community-driven solutions and the power of group dynamics as it relates to addressing security regulation as well as their thoughts on the importance of participating in community-based programs.

3:00 - 3:45 **Keys to a More Successful Security Program**

Joachim Gloschat, ICCT
An effective security program is a living thing. It is comprised of a myriad of equipment, actions, policies, and procedures all of which interconnect and rely on each other in order to provide a comprehensive and effective program. The collection of documents, together forming the security program, must be, by design and intent, focused on three primary missions: remedial measures, preventative measures, and, overlapping both of these, education. The security plan must accurately describe situations both present and future; capture potential scenarios and consequences; detail the organization’s actions both during and following specific events; and, educate the organization on the specific roles specific groups play. Joachim Gloschat's presentation will address all this and more as he explores what makes a successful physical program security.

3:45 - 4:30 **Privacy Fact & Fiction: what you really need to know**

Lisa Carrington, EnergySec - Moderator
Gal Shpantzer, EnergySec
Chris Shepherd, ICCT
Lee Tein, Electronic Frontier Foundation

There is a tremendous amount of public concern about the privacy of the data being collected and used as part of the national Smart Grid push. This panel will explore the importance of privacy matters with respect to Smart Grid efforts. The moderator will be asking questions about government’s role in protecting consumer privacy, to what extent is personal data being exposed, and what smart grid implementers should consider with regard to the protection of personal data.

3:45 - 4:30 **“All My Exes” - A view of the industry from those who have left**

Brandon Dunlap, EnergySec - Moderator
Dave Lewis, AMD
James Arlen, Taos
Lisa Tawfall, Bechtel
Don MacVittie, F5 Networks

Each person on this panel has recently left a security related job in the energy sector. This panel will discuss their various reasons for leaving, what Industrial Control System security issues they believe should be on the top of everyone’s list, and their unique perspective on the security compliance programs that are currently in place in the industry or on the horizon.

4:30 - 5:00 **Regulation and Policy Round Table**

Patrick Miller, EnergySec
Those things that have the greatest impact on compliance are very often the things we have the least control over. This discussion takes a look at currently evolving policy, regulation and trends to considers their impact on the various cyber security efforts currently underway in the industry. The format of this discussion is roundtable which means everyone is encouraged to participate and offer your own thoughts and insights about you are seeing in your own company.

4:30 - 5:00 **Best Practices on Managing Ports and Services**

Jacob Kitchel, Industrial Defender
Copy and paste netstat into and Excel spreadsheet - DONE! Save nmap output into a spreadsheet - DONE! Copy a vendor’s ports list into a spreadsheet - DONE! Our industry’s fascination with managing compliance data by taking default tool output and throwing it into Excel spreadsheets is widely known. This presentation on managing ports and services will finally provide you with the desire to pry those spreadsheets from your hands in exchange for a more robust, accurate, and sustainable solution. We will cover methods to support security and compliance while at the same time increasing accuracy, reliability, and insight into ports and services through the use of automation, change control, and visibility.

Thursday, September 27th

8:15 - 8:45 **Can You Regulate Attitude?**

Steve Parker, VP Technical Research, EnergySec and NESCO - Winston Churchill once said, "Attitude is a little thing that makes a big difference." Indeed, when it comes to security, fostering the right attitude is essential. But can attitude be mandated? Or must it be carefully cultivated and encouraged? This presentation will discuss the limitations of regulatory approaches to security, and explore what is really needed to secure our critical energy infrastructure.

8:45 - 9:30 **The Power of Community**

Deb Bryant, Deb Bryant and Associates
Increasing complexity and ever presence demand on cyber/information security is placing greater pressure on managing and remediating those risks. With the rise of the SmartGrid, a networked world has broad implications for security. Networking the solution - not in technical terms but in human and organizational terms - may provide the best approach to flanking the speed of the challenge. Easier said than done, but the model for developing open source software might work, so says a recent study.

A recently completed study underwritten by EnergySec and conducted by Oregon State University suggests the Energy industry is beginning to follow others including open source software in their solution set and, perhaps most significantly, adopting the model itself to develop tools and applications within their own community.

In her talk Deborah Bryant, international open source expert and Principal Investigator for the study will share perspectives from a range of energy industry stakeholders, discuss early adopters and innovators, and explore some other public sector examples of organizations using an open source approach to solving some of their most challenging problems.

10:00 - 10:45 **The View From Here: a state regulator's perspective**

Patrick Miller, EnergySec - Moderator
Christopher Villarreal, California
Commissioner John Savage, Oregon
Thom Pearce, Ohio
Alan Rivaldo, Texas

The State Regulatory role is highly influential, setting policy direction at the state, regional and national levels. Many state Commissions are becoming more interested in cybersecurity and posing challenging questions to their covered utilities. A dynamic moderator and a panel consisting of staff and Commissioners from four states across the country will discuss topics such as grid modernization, emergency response, FERC's reach into distribution, and rate recovery.

10:00 - 10:45 **The Stories We Could Tell: lessons learned from the field**

Slade Griffin, Enernex
"I belong to the warrior in whom the old ways have joined the new." As two-way communications become more widespread in control systems, the old begins to blend with the new in security research, vulnerability assessments, and penetration tests. Slade's presentation will be a brief recap, and interactive discussion, of the past two years testing industrial control systems, smart grid equipment, and emerging technologies. This will include real-life examples of vulnerabilities discovered, compliance gaps, and mitigations applied as utilities and vendors work together to apply security best practices in their environments.

10:45 - 11:30 **Plenary Session**

Seán McGurk
Critical Infrastructure Protection is at the forefront of the public and private sectors. With the interdependencies of the national critical infrastructure sectors on the electric sector many entities are focusing on risk mitigation to prevent a cascading event. Subsequently industry leaders are addressing challenges in policy, technology and procedures to reduce risk and provide a secure operational environment. As the threat landscape develops so must the capabilities of solution providers in order to counter the malicious activity. In his keynote address, Seán McGurk will discuss how technology is evolving with the use of intelligence reporting in order to enhance security to reduce risk for power company operations.

1:00 - 5:00 **National Electric Sector Cybersecurity Organization Town Hall Meeting**

Keynote Presentation: Pat Hoffman, U.S. Department of Energy
Security Legislation: Building the Bridge Between the Possible and the Practical

Cybersecurity of the nation as a whole or of the electric grid in particular has been the subject of dozens of Congressional hearings and close to 150 bills since 2009. Yet we seem no closer to defining what is the “right thing” and what are the respective responsibilities of government and the private sector to achieve a more secure grid.

Meanwhile, as the grid undergoes a massive modernization transformation, the migration to IP-enabled devices, and away from proprietary, islanded control systems, is required to achieve greater efficiency and interoperability. And dependence on Industrial Control Systems (ICS) augments daily.
Despite a hard court press by the Administration, the National Security Agency, military generals, and former Homeland Security officials, the Senate failed to pass cloture before recessing for the month of August on their latest iteration of the “right” thing, the Lieberman/Collins bill which would have enhanced public/private information sharing and devised a best practices federally-run framework. Earlier in the year, the House passed a bill limited to better information sharing.

Demands for federal legislation are based in part on particular examples of grid vulnerability, namely, Aurora, email spearphising exploits, and Stuxnet. But are these examples based on reality in terms of actual practices and controls that electricity system owners and operators already have in place? The first was a laboratory experiment (and has been memorialized by an exhibit in the National Spy Museum), the second the subject of Senate demonstrations and the third effectuated by actions of unsuspecting third parties. Legislation based on fear rarely makes good law.

How does the industry raise the security bar beyond the minimum required for compliance? The NERC CIP standards regime provides the sticks: Fines and audits to ensure compliance with standards. That’s the practical solution to address vulnerabilities as we understand them today and set baseline operational and personnel standards. What’s needed to help the industry stay ahead of the curve of the “possible” is better information sharing and collaboration, education and training, and workforce development. Should other policies be examined as well, especially those concerning issues “outside our sphere of influence”, such as supply chain integrity?