NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

ENERGY PROVIDER COMMUNITY (EPC) OF INTEREST MEETING – April 2017

Date: 4/25/2017

Time Start-End: 2-3 PM Eastern

Attendees

NCCoE Team and Roles:

Jim McCarthy (Federal Lead)
Barbara DePompa (Outreach & Engagement)

Kristen Klein, MITRE
Tim Clancy, Arch Street LLC
Joe Garmon, Seminole Electronic Cooperative
Michael Cohen, MITRE
Siv Houmb, IADC / SecureNok
Isiah Jones, FERC
Mike Presher, Black and Veatch
Pete Tseronis, Dots & Bridges
Julie Steinke, MITRE
Gerardo Uria, American Petroleum Institute (API)
Patricia Eke, FERC
Ron Beck, Central Lincoln PUD
Ralph King, EPRI
Steve Griffith, NEMA
Andrew Spangler, NCC Group

Agenda

- NCCoE Energy Sector Planned Activities
- Status of Energy Sector (and related) Projects
- EPC Special Guest Speaker, Peter Tseronis, CEO of Dots & Bridges, pete@dotsandbridges.com (301)602-7589
- Comments / Questions

Jim McCarthy to Energy COI:

Recent events in the NCCoE Energy sector

- Second Annual Intelligence in national security forum, sponsored by OSIsoft in Tyson's Corner. Don Fouts backed me up discussed situational awareness at this event by OSIsoft, NCEP partner.

- American Council for Technology (ACT) and Industry Advisory Council (IAC), Cybersecurity Community of Interest Monthly Meeting on April 28. Jim will speak at this cybersecurity event.

Jim McCarthy to Energy COI: We are planning the next six months of travel and conferences and will provide more information shortly. This meeting will provide an opportunity to learn more from Pete Tseronis, who will shed some light on the innovative activities and efforts within the Energy Sector.

But first I want to give you a quick update on the four projects now in various phases for the energy and manufacturing sectors.

Energy/Manufacturing Sectors project status

- **Supply Chain Cybersecurity use case proposal** -- sent to management on April 17. Management team is reviewing this document. Several compelling ideas—initial opinion is this may still be too big to tackle. The use case proposal is likely to be pared down for the NCCoE to build into a practice guide.
- **Cybersecurity for Manufacturing** – about ten Letters of Interest have arrived so far, to address behavioral anomaly detection (BAD). Based on letters of interest, we specifically asked five suppliers to collaborate. Will let you know when organizations have signed on based on those letters of interest. Kick off meeting will be held in the coming weeks, to get going on that project.
    - https://nccoe.nist.gov/projects/use_cases/capabilities-assessment-securing-manufacturing-industrial-control-systems
- **Situational Awareness SP 1800-7 (a,b,c)**
    - Released public draft - 02/16/2017
    - Comment period was closed on 04/17/2017
    - https://nccoe.nist.gov/projects/use_cases/situational_awareness
- **Identity and Access Management SP 1800-2 (a,b,c) –published in Aug. 2015, can be read at the URL below.**
    - Still waiting on finalization of this publication
    - Read more at https://nccoe.nist.gov/projects/use_cases/idam

Jim McCarthy to Energy COI: Now I will introduce our guest speaker, Peter Tseronis, CEO for Dots and Bridges and the former CTO of the U.S. Department of Energy, who will discuss the following topic**:** ***Convergence of IoT, Cyber and Advanced Analytics in the Energy Sector***

Peter Tseronis to Energy COI: I've been fortunate to meet Jim, and meet some of you in person. I spent 25 years in government, including the last seven and a half years at the Department of Energy. Now I'm seeing fruits of that labor in the smart grid, ICS and the Internet of Things (IoT). I've also recently been in Detroit talking to Department of Transportation about autonomous cars and technology implications.

I’m a passionate believer in being a broker for industry, academia and government. In my real job I help vet companies, working for energy sector companies on prospecting for grants, finding sources of funding -- not only for energy, but other sectors as well. For those in government or industry who want a platform, I am often asked about those who are thought leaders, who would like to express views in talking about this industry domain. Being a connective tissue officer as well as a chief technology officer, I am happy to share my contact info.

- Peter Tseronis, CEO of Dots & Bridges, pete@dotsandbridges.com (301)602-7589

Our theme today revolves around IoT and convergence -- how analytics and cybersecurity can drive innovation across our nation. I endorse IoT as a great starting point. At a recent conference, Melissa Hathaway, who served in two U.S. presidential administrations, spearheading the Cyberspace Policy Review for President Barack Obama and leading the Comprehensive National Cybersecurity Initiative (CNCI) for President George W. Bush, said that the ICS market is a projected to be a $3.5 trillion industry in 2017, with a big portion of that market dedicated to cybersecurity.

Our power grid embraces IoT. When you think about 9,000 electricity generating units, millions of megawatts of generating capacity, and 300,000 miles of transmission lines in the U.S., it’s the ultimate use case to describe when talking about IoT or big data on a smarter grid. It’s important not to be drowned by alarmist discussions about the risk of cyber hackers and the threats that come with innovation in this area.

If we agree the century-old power grid can be improved through new transmission lines, and through recovering the construction cost of transmission lines built from state to state, ensuring the network of long distance transmission lines can leverage distributed energy resources – These are challenges that don’t speak to the cybersecurity impact. Outside the beltway, embracing autonomous vehicles, biometrics are important topics for discussion. Inside the Beltway, it’s more about the need for compliance, or how to avoid getting mired in regulations. I love FERC, MERC and the regulatory sides of the house. But with consumer sector interest in smart, connected devices, in cars, planes, medical devices that take care of us -- Those topics outweigh regulatory compliance issues for most business owners and consumers.

For me, it’s exciting to embrace industry participation, and to help accelerate the cybersecurity practice guides created by the NCCoE. Driving innovation in government, this EPC COI is helping to identify threats and vulnerabilities and helping to mitigate those risks.

Let’s talk about the century-old grid, and what we will do to increase communications on that grid, while at the same time preserving the privacy of data and personal information, in the ping, power and the pipe. If you look at your gas bill, it shares information on analytics of usage. This information helps me see how energy is utilized. I own a smart meter and smart thermostat in my home. We are seeing what future holds starting at home. I have also been in discussions, meetings that describe automobiles of the future, and autonomous vehicle networks. And this concept has proven cars can be hacked. Yet the research on bad drivers, including drunk, or tired, or distracted drivers is so alarming that it seems to mitigate the cybersecurity risks. Those crash statistics make it possible to understand/embrace the concept of a smarter vehicle to mitigate ever-growing accident risks.
In the landscape of industrial control systems and processes, Quadrennial Energy Review (QER), hyperlink also pasted here:

https://energy.gov/epsa/quadrennial-energy-review-second-installment

provides an outstanding resource on the current and future state of the energy grid and where our nation is headed. One interesting area within the QER involves grants activity. I'm a big proponent of those grant opportunities. Energy innovation grant dollars are readily available and have helped develop concepts such as microgrids, syncho-phasers, and phaser measurement units (PMUs), which are 100 times faster than any other current SCADA units.

Microgrids are an exciting topic. What is connected to the electric grid locally? What can operate autonomously or resiliently? This is a phrase used frequently. The grid must be built for availability, meaning electric power must be available at all times. But what happens if there's an outage. That infrastructure is not state of art, though it works. If you add microgrids, you can build in resiliency along with greater availability and reliability in local regions.

Also protection is needed for substations. Not just physical security measures. As we modernize must respect the highly available grid infrastructure in place, much like any enterprise architecture currently in place in other industries as well.

JIM to EPC COI: We will see increased interdependency with IoT, and cybersecurity convergence. I'm not a fan of hyped cybersecurity risks. Our energy grid has been built to be resilient. Do you find in your efforts that people are overwhelmed with our current cybersecurity focus? Are they bombarded? We must strive for balance, in the need for cybersecurity, while not causing people to capitulate and do nothing because of creating the impression it is futile to do so.

Pete's response: From my role as CTO I worked to find use cases that are compelling and unique to the government world. At the Dept. of Energy, the 17 National Laboratories are driving cybersecurity research and innovation. I like to say we must embrace the concept that the sky is not falling. Threats are there, every day. Mitigation is what we need to do in data centers, phones, in our personal lives and on our energy grid. Enhanced synchophasers, advanced metering infrastructure are two emerging areas of opportunity. There is a need to build engineering and cybersecurity into these components. Integrated, two-way communications are needed to enable and run analytics. SDN can help with this as well. If you do any research into grants awarded to companies and localities the goal is to protect our access, and the information that protects those assets. The more I read about the grid, protecting information, or the data analyzed will be crucially important. Last year's cybersecurity national action plan focused on our critical infrastructure, meaning our roads, cars and the food. That plan spoke about secure technology, and the need to heavily invest in science, and tools to ensure infrastructure is engineered with sustainable security in mind.

EPC COI Member Question: NSF supports a line of centers, collaborating on IoT Cyber and analytics. Is there a formal collaboration across DoE and DHS?

Pete's response: The short answer is there is no shortage of well-intentioned working groups. After leaving government I worked to reengage and be part of NPPTD, the DHS national protection directorate. Their goal is to make sure the cyber community is talking to sector-specific agencies as well as international communities, to share information and best practices. We held a CSO roundtable two weeks ago to accelerate innovation on how to better collaborate, not just tiger teams, but to swing the pendulum forward. It's important to track the money being awarded by the primary grant-making agencies. About $152 billion is invested in R&D, per year. You can see the recipients of grants for cybersecurity to support critical infrastructure, those folks need to invent the next great thing. So far there is no nexus of collaboration yet. Well-intentioned groups exist, but no real government-wide collaboration.

EPC COI Member Question: We understand the need to share information and especially cybersecurity information. Concern is when a member shares info, they may inadvertently become a target. Can you talk about the confidentiality in sharing cybersecurity information?

Pete's response: Records management and the privacy and security of information is crucially important. This is why most large organizations have Chief Privacy Officers. In my prior roles, I worked with colleagues in this space. Chief privacy officers care about protection of data at rest, and in transit. There is an enormous need for innovation in protecting information from bad actors. And then there are insider threats. Who is the greatest threat? Today's identification methods through passwords and tools being developed to host monitoring, threat monitoring, user behavior analytics, those are all important. Identity and Access Management (IDAM) is also important. New technology domains have emerged, user behavior analytics is one example from this area. How you invest in those tools is crucial.
How is the data to be protected? CIOs focus solely on technologies. So we have a silo effect as a challenge here.

Worlds must converge, including cybersecurity and analytics, policy experts, and cyber-insurance. They must work together so that all data traversing the network is protected from bad actors to avoid taking down the grid, to maintain resiliency and prevent hacks, providence of the data can't be ignored. Privacy, protection of data must drive our conversations.

Meeting ended at 3pm.