NIST National Institute of Standards and Technology U.S. Department of Commerce

NCCoE NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

ENERGY PROVIDER COMMUNITY (EPC) OF INTEREST MEETING – AUGUST 2016

Date	**8/23/2016**	
Time Start-End	**2-3 PM Eastern**	
Attendees	**NCCOE team and roles:** Jim McCarthy (Federal Lead) Don Faatz (NCCoE Lead Architect) Karen Hathaway Viani (NCCoE Systems Engineer) Sallie Edwards (NCCoE ES Staff) Kori Fisk (NCCoE ES Staff) David Weitzel (NCCoE ES Staff) Susan Symington (NCCoE ES Staff) John Wiltberger (NCCoE ES Staff) Julie Snyder (NCCoE ES Staff) Julie Steinke (NCCoE ES Staff)	**Community Members**: Galen Rasche (EPRI) Ralph King (EPRI) Ron Beck (Central Lincoln) Isiah Jones (FERC) Megan Aikman (FERC) Mike Marlowe (ISA & Automation Federation) Karl Perman (EnergySec) Shawn Eck (Empire District Electric Company) Patrick Tronnier (OATI) Steve Mustard (Au2mation) Steve Pflantz (ISA) Darrell Stymiest (C&W) Richard Donohue (Black & Veatch/BRG) Angela Simonds

Agenda

- NCCoE Energy Sector News
- Current Projects
    - Identity and Access Management (IdAM) Project Update
    - Situational Awareness (SA) Project Update
- Oil and Natural Gas Sub-sector Development
- Open Discussion

Discussion

- NCCoE is focusing our Energy Provider Community (EPC) efforts on the development of use cases for the Oil and Natural Gas (ONG) sub-sector
- NCCoE has an ongoing project with Transportation sector to develop cybersecurity profiles based on the Cybersecurity Framework for Improving Critical Infrastructure Cybersecurity . This work includes a profile for Bulk Liquid Transport of Oil and Natural Gas (ONG). This work has helped build relationships with ONG organizations.
- EPC Question: Does NCCoE have relationships with waste water organizations? They have similar protocols to ONG
    - City of Austin already conducting a study with American Waterworks Association, would be a good chance to build relationships

- EPC Comment: Every utility has its own IdAM processes, makes it hard for people to work across different organizations.
    - The existing NCCoE IdAM solution in draft Special Publication 1800-2 is focused on IdAM within and organization as a good intra-organizational IdAM capability is necessary before addressing inter-organizational concerns. However, that solution can be expanded to support federation thereby addressing the inter-organizational problem.
- Jim McCarthy: Is there something that can be done for ONG now in lieu of no existing mandatory compliance standards?
    - EPC comment: Take the standards back to manufacturers so that manufacturers have something to build to. For example, ANSI standards at the protocol development level. A lot of protocol transformation has to be done to get products to work together.
    - EPC Comment: Product manufacturers need standards to help inform product interoperability before they bring products to market.
    - Jim McCarthy: the information generated in COI calls can help inform vendors.
- EPC Comment: Under Supply Chain Risk Management, FERC order 829 directed NERC to develop a reliability standard around software authenticity and access controls. There's a strong similarity in ICS for ONG, water, and electrical. This might provide an opportunity to dove tail into the larger energy sector
    - EPC Comment: Instead of the next cool cyber tools, many utilities have aged infrastructure. FERC supply chain risk management feeds into the need for Cybersecurity at a different level. For example, a compromise of a natural gas pipeline control system can kill people. People have increasingly been building houses near storage areas over the last 50 years. Power outages to hospital could cause loss of life.
    - Jim McCarthy: Do utilities use any particular model or guideline to determine Return On investment (ROI) – especially as related to cybersecurity investments?”
        - EPC comment: Yes. Guidelines consider how much aged infrastructure a provider has. Do you have military bases, major economic developments in the service area (ex: fuel spill - entities want federal money to reduce risks, but don't want to advertise consequences of risks such dead birds on the beach to make the case for money). Explanation of risks and activities to mitigate them need to be kept simple - almost to the level of who does a local elected official call and complain to when an outage occurs at 3am? This helps justify the need for people and capital for security group.
    - EPC Comment: A vetting process to verify products comply with standards and are interoperable is needed. A repository of vetted products would allow a greater level of trust in vendors.
- EPC Comment: I would like to see NCCoE address incident response at a higher/broader level to help organizations understand all that is involved. Organizations need to have real systems in order to detect cybersecurity events and plans created to deal with cyber compromises when they occur.
    - Jim McCarthy: Situational Awareness is a piece of that.
    - EPC Comment: Organizations don't have or exercise good incident response plans. Organizations need help understanding preparedness, training, tabletop exercises, and all elements of incident response from a holistic perspective.
- EPC Comment: Many utilities, especially ONG utilities, have aged (80%) infrastructure, and getting funds for ONG security is difficult. Helping ONG organizations understand cyber risk and its relationship to business risk would help them allocate funds. How do you identify the basic top 10 cyber priorities in C-suite language?

  - Dave Weitzel: There has been some great research through the years (I3P) on enterprise-side risk management
- Jim McCarthy: Is there both a need and enough trust/cooperation among utilities to share sensitive cybersecurity information?
  - EPC Comment: Yes, there is an increasing desire to have access to shared information. STIX and TAXI are being used. Sharing may not currently include all details of an incident, but the main points are being shared. Having a standard format for information sharing would make a significant difference for utilities Cybersecurity programs