NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

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

Date: 10/25/2016

Time Start-End: 2-3 PM Eastern

Attendees

NCCOE team and roles:	***Community Members:***
Jim McCarthy (Federal Lead)	Michael Smith, Dept. of Energy / Acacia Security
Dr. Michael Cohen (Presenter)	Samit Khare, SDG Corporation
David Weitzel	Leo Staples, Automation Federation
Tania Copper	Steve Pflantz, ISA
Mary Yang	Richard Donahue, Black and Veatch
Sarah Kinling	
Julie Steinke	

Agenda:

- NCCoE Energy Sector News
  - Grid Sec Conference
  - Upcoming NCCoE Planned Conferences
- Current Projects
  - Identity and Access Management (IdAM) Project Update
  - Situational Awareness (SA) Project Update
- Oil and Natural Gas Project Concepts
- Dr. Mike Cohen –Supply Chain Risk Management
- Oil and Natural Gas Use Case Development Discussion

Discussion:

NCCoE Energy Sector News

Grid Sec Conference:
On Tuesday October 18th, a four-hour workshop in Quebec City was held and approximately 50 people attended. The workshop discussions were centered around the NIST cybersecurity public offerings which is beneficial to all sectors such as cybersecurity framework, NIST SP 800-53, and NIST SP 800-82. Guest speakers included Energy COI members Bob Lockhart of UTC, Mike Prescher of Black and Veatch, and Mike Meason of Western Farmers Electric Cooperative. Mike Cohen presented on Supply Chain Risk Management which received a great deal of feedback regarding it becoming a possible Use Case.

Upcoming NCCoE Planned Conferences:

Upcoming conferences include the 11th Annual Cybersecurity Conference for the Oil & Natural Gas Industry on November 9th in Houston Texas. Dave Weitzel will represent the NCCoE as a panelist. As more conferences are added, the Energy COI will be informed.

Current Projects

Identity and Access Management (IdAM) Project Update:

IdAM is currently in draft form and all of the comments have been adjudicated. For those that have been following the project, the logo issue has been resolved and a potential release date of the IdAM in its final form is November 2016. The solution architecture has been included in slide five.

Situational Awareness (SA) Project Update:

Situational Awareness is a current project that the NCCoE Energy sector is working on. The final components of the build are in production and a draft has not been released at this time but is underway. The concept architecture is included in slide seven.

Oil and Natural Gas Project Concepts

The NCCoE strategy focuses on Oil and Natural Gas (ONG) but the Use Cases and solutions can be applied to all sectors within energy. The themes that were discussed on last month's call were Assets Inventory and Management, Information Sharing, and Supply Chain Risk Management which will be a topic of discussion during this call. We are also seeking ideas from the public.

As discussed on September's Energy COI call, ONG Information Sharing "Map and Match" and Identity Federation for ONG are still potential Use Cases. Energy COI members are encouraged to express their concerns and or ideas.

Supply Chain Risk Management: Dr. Michael Cohen

Based upon years of supply chain risk management studies, Mike Cohen informed the COI that there are opportunities for automating several portions of the SCRM Management process that could be a benefit to the energy sector. In the studies that Mike alluded to, it was found that supply chain threat is highest for nation's states and organized crime.

Supply chain risk is like all other critical infrastructure risks, it is a function of threat, vulnerability, and consequences. What makes supply chain risk somewhat unique is that the risk presents itself at every stage of the system development lifecycle (pictured at the bottom of slide 15). That implies in theory that there should be mitigations at every stage of the system development lifecycle. What makes SCRM so challenging, is that different companies and organizations own different stages of the lifecycle and no one organization or regulatory authority has oversite over the entire process. Over the last few years, a lot of SCRM guidance has been issued and initiatives have been launched. Guidance can be divided into energy related and non-energy related. The energy related guidance and initiatives include:

- FERC Order 829
- NERC Standard Drafting Team
- DoE
- ODNI's Recent Report

The non-energy related guidance and initiatives include:

- NIST SP 800-161
- US-CERT
- DHS
- DoD

The opportunities for automating energy supply chain risk management should not be viewed as limited to the electricity sub-sector despite some of the given examples, but are intended to cover the entire energy sector. Examples of potentially automated controls:

- NERC SCRM SDT
- US-CERT: TA16-250A
- DARPA Research Prototypes
- COTS Products

Recently developed prototypes include:

- MITRE/FFRDC LENS/SURE Research Prototype
- MITRE/FFRDC Requirements Analysis Tool (RAT) Prototype

In summary to review the landscape, NERC is actively developing SCRM standard to meet FERC's SCRM Order 829 and the NCCoE could be an observer to track the SCRM requirements we become qualified in the standard. Several NERC-mandated and NIST/US-CERT recommended security controls can be automated and provided as a tool suite to the energy provider community. Research prototypes for meeting some SCRM requirements have been developed by DARPA and FFRDCs and could be evaluated for possible inclusion in the build. Lastly, an NCCoE SCRM Use Case Build would be useful for both regulated BES and non-regulated Smart Grid industries but the decision is left to the Energy COI.

Questions/Comments:

Jim McCarthy to Energy COI: How does a provider or manufacturer control what their providers are doing?

***Mike Cohen Comments**:* One of the biggest challenges is how does a manufacturer control or ensure the integrity of the components they are putting into their systems. They don't have direct visibility into how their vendors are putting together their systems so one of the means for doing this would be through contractual mechanisms that would require that their vendors subscribe to a SCRM program that's at least as good as the manufacture's own program and perhaps allows autoing by the manufacture of the vendor's manufacturer process. You could pass this contractual requirement down the line until you have covered the entire supply chain.

Another answer given during the workshop is to send components or systems to a third party lab that would do testing of the components for hidden malware or malicious firmware to basically provide an underwriter lab guarantee that the components are good.

Jim McCarthy to Energy COI: Any other comments, concerns, or questions?

Energy COI Comments: Done right, what we're talking about would apply way beyond just the ONG sectors; certainly in waste water as some of the same systems are used. These lessons learned can be applied to their supply chain, often those groups don't have the technical people engaged and are relying solely on outsource folks to provide them with both technology, and technical support. Having standards like this would certainly make that sector much more secure.

Jim McCarthy to Energy COI: That's the reason why we are doing this as a whole. This is definitely something to consider as we want something applicable not only in this sector, but across as many sectors as possible or at least those that employ industrial control systems.

Dave Weitzel Comments: You are actually seeing an evolution here at NCCoE from industry specific Use Cases to broader projects so it is exactly a build on that. We are certainly seeing cross sectoral leverage of some of our current work products. We are also looking at how broad our projects can be with still appropriate focus to make sure that we are solving something. It would be great to use this opportunity.

Jim McCarthy to Energy COI: Any other comments, concerns, or questions?

Jim McCarthy concludes the Energy COI call at 2:58pm.

Action Items:

1) Jim McCarthy to stand up EPC sub-working group to develop the Supply Chain use case concept. Request for participation will be sent to entire EPC the week of 11/07/2016.