NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

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

Date: 12/20/2016

Time Start-End: 2-3 PM Eastern

Attendees

NCCOE Team and Roles:	***Community Members:***
Jim McCarthy (Federal Lead) Tania Copper (Outreach & Engagement Strategist)	Dan Phillips, FERC Margaret Scott, FERC

Agenda:

- NCCoE Energy Sector News
  - New NCCoE Planned Activities
- Energy Sector Project Updates
  - Identity and Access Management (IdAM) Project Update
  - Situational Awareness (SA) Project Update
  - Cybersecurity for Manufacturing Project Description
  - Supply Chain Use Case Development
  - Overall Year End Status
- EPC Open Discussion / Comments / Questions

Discussion: ***Please note that this is a year-end update call and is shorter in length.***

Energy Sector Project Updates

Identity and Access Management (IdAM) Project Update:
Work began on Identity and Access management (IdAM) in September 2014. The draft was released on August 25, 2015 and all comments were adjudicated by May, 2016. The document is pending final review by the Washington Executive Review Board (WERB) and contingent upon their feedback, the projected release of the final guide is January, 2017.

Situational Awareness (SA) Project Update:
The Situational Awareness guide is titled as SP 1800-7; it contains three parts:

- Part A – Executive Summary
- Part B – Architecture
- Part C – How-To Guide (step by step on installation, configuration and integration)

We are currently at "build complete" which means that the work of the NCCoE and UMd lab infrastructures are complete. The draft document has been submitted to the build team for review as they see it prior to it being released to the public for comment. The projected public draft release date is January, 2017.

Cybersecurity for Manufacturing Project Description:
Manufacturing is a new sector established at the NCCoE and is currently being run by the Energy sector team. These same industrial control systems (ICS) devices that are used to run the grid are also used to run manufacturing environments. The draft project description was released November 7, 2016. Due to the extensive feedback that has been received, the comment period was extended to December 22, 2016. The adjudication period is approximately 15-20 days and the final project description should be released by late January, or early February, 2017.

Supply Chain Use Case Development:
The NCCoE Energy Sector team is coordinating an effort to develop one or more use case ideas for a Supply Chain build in our labs. A Supply Chain Sub-work group was stood up and the first meeting was held on 12/16/2016. To begin a build, NCCoE management will need to approve of the use case ideas that are generated as a result of the meetings. The baseline criteria for the use case are as follows;

- Use case must solve a technology related Supply Chain issue for the Energy Sector. Additionally, this problem must be addressable by more than one commercially available Cybersecurity technology / capability.

- The scope of the use case must be manageable, in that Supply Chain issues typically contain more than one component related to policy, procedure and perhaps technology. NCCoE use cases solve Cybersecurity challenges through the use of technology, thus policy and procedure issues do not qualify for use case consideration.

EPC Open Discussion / Comments / Questions
Jim McCarthy to Energy COI: Are there any questions and or comments?

Energy COI Question: I know that at some point last year or perhaps this year, a different organization was meeting with critical manufacturers. Is this standup a completely different group that is being setup or is it a part of or derived from another organization?

Jim McCarthy to Energy COI: There has been no direct effort at this time to link the two. Also, as an EPC member, please feel free to suggest any type of relationship that you think would be beneficial to this group.

Energy COI Comments: From my perspective, as it relates to developing technology solutions, I think there are two areas that can be of focus for the team from an operational sense. They are:

- Verification of software integrity and authenticity
- Vendor remote access solutions

Jim McCarthy to Energy COI: Both suggestions were brought up on the Supply Chain SWG call that was held this past Friday. This is a very strong possibility. I agree with you; I see strong potential for device-to-device supply chain use cases.

Energy COI Comments: Another potential use case may be Cloud Virtualization. It's a Supply Chain type issue because if you want to take some of the operational functions and put them in the care of a third party, the question is how would one do that securely? It's kind of its own separate issue but can also be

Supply Chain because you want to make sure that if you're going to be doing that, you are employing the proper vendors and are avoiding redundant communication to allow that to happen given the constraints that they operate in.

Jim McCarthy to Energy COI: This is very valuable feedback that we will document and consider for presentation at the next Supply Chain SWG meeting (tentatively scheduled for mid-January).

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

Jim McCarthy concludes the Energy COI call at 2:53pm.