

NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

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

Date: 1/31/2017

Time Start-End: 2-3 PM Eastern

Attendees

NCCoE Team and Roles:

Jim McCarthy (Federal Lead)
Tania Copper (Outreach & Engagement Strategist)

Community Members:

Margaret Scott, FERC
Mike Cohen, MITRE
Mike Prescher, Black and Veatch
Mike Smith, Acacia Security
Tim Clancy, Arch Street LLC

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
 - NCCoE Cybersecurity for Manufacturing
 - Supply Chain Use Case Development
- EPC Open Discussion / Comments / Questions

NCCoE Energy Sector News

New NCCoE Planned Activities

LOGIIC Executive Committee Meeting (Linking the Oil & Gas Industry to Improve Cybersecurity) 02/07/17 – 02/08/17 in Houston, TX

- Part of Automation Federation
- Presenting NIST Cybersecurity portfolio at 5pm EST, 02/07, via conference call

Purpose: Jim McCarthy will be giving an overview of the NCCoE to determine if there is any potential partnership or linking in terms of Use Cases between the LOGIIC participants and the NCCoE, as we are actively seeking an initiative in OnG.

**ICRMC
(International Cyber Risk Management Conference)
03/02/17- 03/03/17 in Toronto, ON**

Purpose: This conference contains interested parties from the energy sector in addition many individuals representing various sectors and industries.

**OSIsoft Annual User Conference
03/20/17 – 03/23/17 in San Francisco, CA**

- Presenting NIST Cybersecurity portfolio with focus on OSIsoft’s PI Historian use in SA build

Purpose: We the have used the OSIsoft PI system in the Situational Awareness Use Case as part of our build, Jim McCarthy has been invited to speak at an IT Industrial Track.

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 logos will be included in all Practice Guides and the projected release date is February 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 was submitted to the build team for review on December 23, 2016 and there has been a bit of re-work but no material changes were requested. The projected public draft release date is the week of February 13, 2017 at which time the NCCoE will make an announcement and all communities will be notified.

[Cybersecurity for Manufacturing Project Description:](#)

Manufacturing is a new sector established at the NCCoE and is currently being run by the Energy sector team. This is a four-part series which will initially focus on Behavioral Anomaly Detection. The draft project description was released November 7, 2016, and due to the extensive feedback that was received, the comment period was extended to December 22, 2016. We are currently completing comment adjudication and the final project description should be released in 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.

The third Supply Chain SWG meeting was held on January 27, 2017, we received significant feedback regarding Use Case. The goal is to have at least one or more Use Cases by March 2017.

EPC Open Discussion / Comments / Questions

Jim McCarthy to Energy COI: Are there any questions and or comments?

Energy COI Question: Do you have any vendors lined of up for the Behavioral Anomaly Detection initiative?

Jim McCarthy to Energy COI: We have a lot of vendors who are aware that we are doing something in manufacturing and have expressed interest in participating, but we do not have anyone chosen specifically yet.

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

Jim McCarthy concludes the Energy COI call at 2:30pm.