
NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

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

Date: 3/28/2017

Time Start-End: 2-3 PM Eastern

Attendees:

NCCoE Team and Roles:

Jim McCarthy (Federal Lead)

Barbara DePompa (Outreach & Engagement)

Steve Pflantz, ISA
Ron Beck, Central Lincoln PUD
Rich Donahoe, Berkeley Research Group
John Abeles System One
Michael Cohen, MITRE
Mike Smith, DoE
Siv Houmb, IADC / SecureNok
Isiah Jones, FERC
Kevin Comfort, Entergy Corp.
Mike Prescher, Black and Veatch

Agenda

- NCCoE Energy Sector Planned Activities
- Status of Energy Sector (and related) Projects
- Supply Chain Use Case Proposal
- EPC Open Discussion / Comments / Questions

Jim McCarthy to Energy COI: Upcoming events for NCCoE's Energy sector. These are events Jim will attend:

- Second Annual Intelligence and National Security Forum 04/20/2017, Tyson's Corner, VA
- American Council for Technology (ACT) and Industry Advisory Council (IAC), Cybersecurity Community of Interest Monthly Meeting, 04/28/2017, will speak at this cybersecurity event in Washington D.C.

Jim McCarthy to Energy COI: As the lead for the energy and manufacturing sectors here's the status of my four primary projects, along with their various phases of development.

Energy Sector project status

- **Situational Awareness SP 1800-7 (a,b,c)**
 - Released public draft - 02/16/2017
 - Comment period open until - 04/17/2017 – Please make your comments, or let me know if you need more time to respond. The deadline for comments may be extended.
 - https://nccoe.nist.gov/projects/use_cases/situational_awareness
- **Identity and Access Management SP 1800-2 (a,b,c) – draft published in Aug. 2015, can be read at the URL below.** This practice guide is about a converged provisioning mechanism to change access rights on IT, OT and physical access control systems.
 - Projected release of final – Spring 2017
 - https://nccoe.nist.gov/projects/use_cases/idam
- **NCCoE Supply Chain (SC) Sub Working Group (SWG) –** On our last call, 2/24, it was decided that a potential first use case proposal would include a combination of 1) an SDLC-based use case idea from Mike Cohen and 2) Maintaining Operational Cybersecurity Across Supply Chain, with an emphasis on Asset Management, from Siv Houmb.
 - Last call was held on 02/24/2017
 - Drafted Use Case Proposal on 3/17/17 that incorporates several elements of ideas generated by SWG members
 - SWG Action – Please provide comments by April 7, 2017
 - Will present this use case idea to NCCoE management team in April for approval.
- **Cybersecurity for Manufacturing**
 - Behavioral Anomaly Detection (BAD)
 - Final project description (PD) - 03/2017—we have emulated a manufacturing environment with robotic arms and a chemical processing environment as well.
 - Federal Register Notice - 03/2017—We have put out a call for collaboration for any vendors who wish to participate in NCCoE’s manufacturing project, to submit a letter of interest.
 - https://nccoe.nist.gov/projects/use_cases/capabilities-assessment-securing-manufacturing-industrial-control-systems

Jim McCarthy to Energy COI: Now we can go over the proposed use case idea developed by the Supply Chain Sub-Working Group (SC-SWG). The letter was read aloud at the meeting.

Sent via GovDelivery on March 17, 2017, here is the Draft Supply Chain Cybersecurity Use Case Proposal by the NCCoE Supply Chain (SC) Sub-Working Group (SWG)

In December 2016, the NCCoE Energy Sector team solicited members of the Energy Provider Community (EPC) to participate in the development of a Cybersecurity Supply Chain use case. Numerous calls have been held and use case ideas have been submitted by our participants. The criteria for a viable NCCoE use case are as follows:

- Must solve a technology based supply chain challenge utilizing a set of commercially available cybersecurity tools and or capabilities.
- Must take into consideration existing standards and/or best practices (if applicable).
- The use case must be industry driven. This is done by having the participants of the SCSWG group weigh in on what the main concerns of the sector are, as they relate to Supply Chain issues.

The NCCoE SC SWG's most recent call was held on Friday, 02/24/2017. It was decided that our first use case proposal would include a combination of the 1) SDLC based use case idea (Mike Cohen) and 2) Maintaining Operational Cybersecurity Across Supply Chain, with an emphasis on Asset Management (Siv Houmb). It is believed a single use case highlighting numerous supply chain Cybersecurity capabilities is feasible, and would also take into account the technology components of the proposed draft NERC-CIP guidance focusing on vendor remote access to BES systems, software integrity, and software authenticity.

NCCoE SC SWG Draft Use Case Proposal for Review

Title: Operational Supply Chain Cybersecurity throughout the System Development Lifecycle

Sector: Energy Sub-sector(s): Utilities, Oil and Gas (Drilling)

Supply Chain Risk Management (SCRM) presents challenges to many industries and sectors. The NCCoE, in collaboration with Energy Sector security experts, proposes a comprehensive SCRM Cybersecurity use case that addresses multiple phases of the System Development Life Cycle (SDLC). There is no single Cybersecurity capability that can resolve all the technology based challenges in SCRM. Rather, a use case that introduces numerous Cybersecurity capabilities, or, "an integrated tool suite" to address Cyber risks in various SDLC phases seems appropriate.

Use case scoping will include:

- Identifying appropriate SDLC phases 1) Acquisition 2) Manufacturing 3) System Deployment (Users)
- Identifying cybersecurity capabilities 1) Asset Management (ICS/IT/) 2) Cybersecurity Visualization tools 3) Remote Access (vendor/contractor/employee) 4) Software Integrity (code vulnerabilities) 5) Software authenticity (validation)

Jim McCarthy to Energy COI: Please review the supply chain use case letter, and feel free to provide comments, and elaborate on this proposed use case idea. We will host an SC SWG conference call on April 10 to discuss and refine this proposed use case idea. [NCCoE Supply Chain SWG Draft Use Case Proposal](#)

Jim McCarthy to Energy COI: Separately, the NCCoE is also interested in gathering your input and feedback on the possibility of a use case on IT asset management for the Energy sector, similar to a practice guide that has been published previously for financial sector audiences. For greater detail, please feel free to review the current financial sector ITAM practice guide at:

https://nccoe.nist.gov/projects/use_cases/financial_services_sector/it_asset_management.

Energy COI questions/comments: Multiple attendees responded affirmatively to the possibility of an ITAM guide for the energy sector. There's a need to better track both physical and virtual assets. We would be interested in a solution aimed at IT asset management for the energy sector.

Jim McCarthy to Energy COI: That's great feedback. We will reach out further about this possible use case idea in the near future then. Look for more about this idea soon.

Call ended at 2:42pm