NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

EPC SUPPLY CHAIN SUB-WORKING GROUP MEETING – DECEMBER 2016

Date: 02/24/2017

Time Start-End: 2-3 PM Eastern

Attendees

NCCOE Team and Roles:

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

Community Members:

Dan Phillips, FERC
Tim Clancy, Arch Street LLC
Celia Paulsen, NIST
Isiah Jones, FERC
Steve Pflantz, ISA
Pete Tseronis, Dots & Bridges
Fred Hintermister, NERC
Dario Lobozzo, Guidepost Solutions
Michael Cohen, MITRE
Dan Rueckert, Sheffield Scientific
Siv Houmb, IADC / SecureNok
Patricia Eke, FERC

Agenda:

- Discuss potential use cases
- Identify additional use cases that have since been submitted

SWG Goal

The goal of the NCCoE sub-working group is to identify one or more technology based use cases for Supply Chain (SC) Risk Management. This has to be based on a challenge that is prevalent in the Energy sector at this point in time but can also readily overlap into other sectors, such as Manufacturing. The use case selection guidelines are;

- Must solve a technology based supply chain challenge utilizing a set of cybersecurity tools and or capabilities. This is one of NCCoE's basic tenets as we cannot take on a use case that a technology provider and/or vendor can solve on their own. Our goal is to take a set of commercially available tools and technologies that currently exist to solve the problem at hand.

- Must be technology based as we are not exploring policy, procedure, research or process. The goal is to create something that can be introduced to industry within about a year.

- The use case must be industry driven. This is done by having the participants of the Supply Chain sub-working group weigh in on what the main concerns of the sector are, as they relate to Supply Chain. Once the need has been identified, the proposal is then taken to management to determine whether or not this meets the criteria to become a use case.

Jim McCarthy to SWG: Here are some details about the potential use cases for the Supply Chain sub working group (SWG) to consider. Siv's first idea is for Supply Chain Coordinated Incident Response, focusing on drilling rigs. Drilling rigs house various control systems, such as Drilling Control Systems (DCS), Blowout Prevention (BOP) control systems, Mud control systems, etc., and these systems are usually comprised of equipment and software from multiple vendors. It is also usually the case that these multiple vendors have Service Level Agreements (SLAs) to maintain their part of the systems of systems. coordinated incident response would need to handle the various layers in the supply chain, but also their interrelations and interests such as decision power, goals and objectives. Additionally, this coordinated cross supply chain incident response would have to happen in real-time, as time could be paramount to avoid major catastrophes. What is needed is a cross supply chain real-time decision support system. Her second idea is focused on asset management, which is a challenge for everyone. Titled Maintaining Operational Cybersecurity Across Supply Chain, this use case calls for a cross supply chain cybersecurity assurance tool or framework comprised of asset management, software management, cybersecurity requirements verifications. Any comments?

Siv Houmb's use case ideas are available at:
https://nccoe.nist.gov/sites/default/files/ONG%20Use%20Case.pdf

SWG comment: there's a need to look at asset management, along with the acquisition language and voluntarily compelled response capabilities of vendors on the SC. There's a need to know who to contact in such incidents. We think her number two idea is important. We like idea #2.

SWG comment: we need to participate in a solution communications channel of trust. Reporting vulnerabilities has grown mundane. How to gain incident response in the supply chain is important.

SWG comment: what we could create as a group is a guideline of topics that holds manufacturers to account for operational technologies. If using hardware, software or firmware when was your code third-party verified? How often are you reporting issues? It would be helpful to have a guide for how to manageably convey information about what they are pursuing, whether its secure?

SWG comment: Coordinating data that traverses the supply chain is brought up a great deal in Internet of Things. IoT and SC are both virtual and multiple vendors and partners' hardware and software are involved. Data integrity must be created, maintained. It's important to understand and maintain data integrity to mitigate risks in the future.

Mike Cohen to SWG: This use case idea involves three use cases related to systems acquisition, manufacturing and systems users. All three form a single system, and an overarching use case. What's needed is a tool for all three components, an integrated Supply Chain RM tool suite. That would take all three phases of the software delivery lifecycle into account. NCCOE would be building an integrated tool suite across the three phases. Review Mike's use cases at the following link: https://nccoe.nist.gov/sites/default/files/SCRM%20Use%20Cases%20based%20on%20the%20SDLC.pdf

Dan Rueckert to SWG: I like the idea of validating acceptance of equipment because early in smart grid era we were forced to reject meters. Ultimately, if you have vulnerabilities its important to share them with us, not wait until after we face a cybersecurity event. Dan shared his idea for a use case as well. Read more about his idea at https://nccoe.nist.gov/sites/default/files/DRAFT-20170214-1030-SystemAndServicesAcquisition-v20170209.pdf

SWG comment: Will send a draft of use cases for further discussion in the future.

Jim to SWG: Let's refine the ideas we have on the table today. Also important to note there is no time limit to submit ideas for use cases. Right now, this SC SWG could focus on data integrity, IDAM and/or situational awareness in supply chain management. All are interrelated.

SWG comment: I like Mike's use case approach, we need to be applying applicable lessons and technology to another vertical sector, from nuclear and defense to Underwriters Labs and ISA. Building a solution for SC that includes integrators and manufacturers who are putting stuff on the grid makes sense.

Jim to SWG: Meeting time may be subject to change. Next call likely in one month. We appreciate the input and especially the use case ideas.

-end-