NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

EPC SUPPLY CHAIN SUB-WORKING GROUP MEETING – January 2017

Date: 1/13/2017

Time Start-End: 1:30-3 PM Eastern

Attendees

NCCOE Team and Roles:	***Community Members:***
Jim McCarthy (Federal Lead) Tania Copper (Outreach & Engagement Strategist)	Dan Rueckert, Sheffield Scientific Faisal Amin, Berkeley Research Group, LLC Jason Oberg, Tortuga Logic Jeff Foley, SIEMENS Jon Boyens, NIST Mark Kellaher, FERC Megan Aikman, FERC Michael Cohen, MITRE Mike Smith, Acacia Security Richard Donohoe, Berkeley Research Group, LLC Siv Houmb, IADC / SecureNok Steve Pflantz, ISA TJ Roe, Radiflow

Agenda:

- NCCoE Supply Chain SWG Goal
- Brief Review of 12/16/2016 Meeting for New Members
- Action Items from First Meeting
- Update on NERC-CIP SCRM Compliance Draft
- Set Target Dates for NCCoE
- Open Discussion

SWG Goal

The overall goal of this sub-working group is to identify one or more technology based use cases for Supply Chain 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 NCCoE management to determine whether or not this meets the criteria to become a use case.

December 2016 Meeting Review for New Members

The following items were decided/discussed at the Supply Chain discussion that was held on 12/16/2016:

- SWG meetings will be held on as needed basis until use cases identified: the next call was to take place a month from 12/16/2016, due to the Holidays.

- NCCoE will handle all communications among SWG members: Jim McCarthy and Tania Copper will distribute written communication to the SWG members as pertinent information is received. This is will be done by way of email using the GovDelivery platform.

- No real need for specialized roles: each member of the sub-working group is considered to be a thought leader and can decide how involved they would like to be in each discussion. While participation and engagement are welcomed, it is not mandatory.

- Orient use case discussion to technology challenges in pending NERC guidance

- Consideration given to tech issues identified in future "procurement language"

- All encouraged to expand participation in this SWG: SWG members are encouraged to spread awareness and invite anyone that they deem an asset to the group and discussions.

Action items from the first Supply Chain SWG meeting that was held on 12/16/2016

During December's call, members of the Supply Chain SWG expressed interest in having tech providers, integrators and collaborators join future calls. This request was addressed by inviting companies who have contributed significantly to one or more NCCoE practice guide(s), particularly in the Energy Sector. SWG members are encouraged to provide the information of any additional companies that they would like to participate in future calls.

NERC-CIP Supply Chain Compliance update

The following information is a brief update on the pending NERC-CIP SCRM Compliance Requirement as understood by the NCCoE:

- The document has been titled NERC CIP-013-1 Cyber Security Supply Chain Risk Management (SCRM)
- It addresses FERC Order 829: a reliability standard that addresses Supply Chain Risk Management for Industrial Control System hardware, software, and computing and networking services associated with bulk electric system operations
- The draft release is set for January 2017, with a 45-day comment period that will include a voting ballot
- The NERC Board adoption will occur in August 2017
- The NERC-CIP Supply Chain Compliance Requirement will address the following cybersecurity technology capabilities
    - Software Assurance and Authenticity
    - Vendor Remote Access

Target Dates for NCCoE

The goal of the Supply Chain SWG is to collaborate and develop initiatives that can be presented to NCCoE management to determine if one or more can become a Use Case(s). The following target dates have been set:

- Host another SWG call in **January** to narrow the scope and lock in a few ideas regarding cybersecurity issues plaguing the Supply Chain community (set for 01/27/2017).
- Present the use cases to NCCoE management by the end of **February**

Open Discussion

Jim McCarthy to Supply Chain SWG Member (Tortuga Logic): this company's technology is very interesting as it relates to the Supply Chain initiative, please provide the group with a bit of background on your company.

SWG Member Comments (Jason Oberg, CEO, Tortuga Logic): Tortuga Logic provides software and services to identify security vulnerabilities in integrated circuit designs. Based in San Diego and formed in 2013, Tortuga Logic spawned out of decades of research performed at both UC San Diego and UC Santa Barbara. Tortuga Logic can address supply chain issues that occur during the design and verification of integrated circuit or FPGA designs before manufacturing. The software products identify vulnerabilities in the integrated circuits themselves and also in the way the low level software (boot- and micro-code) interacts with the integrated circuit.

Additional Questions/Comments:

Jim McCarthy to Supply Chain SWG: Any other comments, concerns, or questions?

Mike Cohen Comments: I'm proposing to demonstrate an operational research prototype (not yet a COTS Product) that we developed at MITRE for evaluating vendors. It's called
LENS: Leveraging Non-traditional Supply Chain Analyses for Anomaly Detection.

The premise of the prototype tool is that a prime contractor or systems integrator is assessing bids from multiple vendors to supply a certain component of an energy system. The prime contractor or system integrator wants to include in their overall vendor evaluation an assessment of how well each vendor carries out its SCRM due diligence in developing the component it is bidding on to offer.

The prototype implements processes and metrics for defining vendor trust assessment measures to assess trust on vendors in an energy system supply chain that can then be used during acquisition and procurement.

We propose to give a live demo to Jim at NCCoE and then if he thinks it fits within the scope of the types of Use Cases he's looking for give a Meeting Place demo to the entire SWG.

Action Items:

1) Schedule the next Supply Chain SWG call for January 27, 2017
2) Include Jon Boyens of NIST on a future call as a presenter
3) SWG members to present ideas on procurement during next meeting

Jim McCarthy concludes the Supply Chain SWG call at 2:29pm.