NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

EPC SUPPLY CHAIN SUB-WORKING GROUP MEETING – January 2017

Date: 1/27/2017

Time Start-End: 2-3 PM Eastern

Attendees

NCCoE Team and Roles:	*Community Members:*
Jim McCarthy (Federal Lead) Tania Copper (Outreach & Engagement Strategist)	AJ Nicolosi, SIEMENS Dan Rueckert, Sheffield Scientific Isiah Jones, FERC Jason Oberg, Tortuga Logic Jon Boyens, NIST Mike Cohen, MITRE Siv Houmb, IADC/SecureNok Solomon Karchefsky, FERC Steve Pflantz, ISA Todd Wedge, SIEMENS

Agenda:

- Review of 01/13/2017 Meeting
- Jon Boyens, NIST: Other SCRM Initiatives & Supply Chain Updates in Cybersecurity Framework (CSF) v1.1 draft
- Potential Use Cases - Topics
- Development of Use Case Ideas - Open Discussion
- Action Items for Next Meeting

Review of 01/13/2017 Meeting

- Briefly discussed pending NERC-CIP supply chain guidance
- Agreed that the "technology "areas identified in NERC-CIP guidance will serve as at least one guideline for use case ideas:
- Members provided use case ideas regarding procurement language:
- Tortuga Logic's Jason Oberg provided overview of Supply Chain product:

Jon Boyens, NIST

Below is the Energy Sector Supply Chain Risk Management (SCRM) activities timeline:

- **May 2012**: ES-C2M2 Version 1, Supply Chain and External Dependencies Management Domain
- **February 2014**: ES-C2M2 Version 2, O&G C2M2, C2M2, Supply Chain and External Dependencies Management Domain
- **April 2014**: Cybersecurity Procurement Language for Energy Delivery Systems
- **April 2015**: UTC Supply Chain Risk Management for Utilities – Roadmap for Implementation
- **September 2015**: EEI Cyber Supply Chain Principles
- **January 2016**: FERC Supply Chain Risk Management Conference on Supply Chain Risk Management
- **July 2016**: FERC expresses and interest in supply chain management standard
- **July 2016**: Final Rule: FERC directs NERC to develop a new or modified standard: (1) software integrity and authenticity; (2) vendor remote access; (3) information system planning; and (4) vendor risk management and procurement controls.

Draft CSF V1.1, Framework Core:

Upon the release of Framework Draft Version 1.1, there are three main areas that we put into SCRM. The background on this is during the development of the Framework between February 2013 and the final release in 2014, we had approximately six workshops around the country and the number one problem that we heard back specifically from owners and operators was SCRM issues. We did not address SCRM directly inside the first version of the framework for many reasons, primarily because just the framework alone was fairly contentious and we were concerned that it would not remain voluntary but that it would become regulatory. Since its release, I have been innovating with comments from industry saying how there are gaps, a main one being the fact that we did not address hardware integrity which was a pretty big oversight from a technical perspective which is why we tackled it in 1.1.

Supply Chain Risk Management (ID.SC): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has in place the processes to identify, assess and manage supply chain risks.	**ID.SC-1**: Supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders.
	ID.SC-2: Identify, prioritize and assess suppliers/providers of critical information systems, components and services using a supply chain risk assessment process.
	ID.SC-3: Suppliers/providers are required by contract to implement appropriate measures designed to meet the objectives of the Information Security program or Supply Chain Risk Management Plan.
	ID.SC-4: Suppliers/providers are monitored to confirm that they have satisfied their obligations as required. Reviews of audits, summaries of test results, or other equivalent evaluations of your suppliers/providers are conducted.
	ID.SC-5: Response and recovery planning and testing are conducted with critical suppliers/providers.
Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information	**PR.DS-1**: Data-at-rest is protected
	PR.DS-2: Data-in-transit is protected
	PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition
	PR.DS-4: Adequate capacity to ensure availability is maintained
	PR.DS-5: Protections against data leaks are implemented
	PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity
	PR.DS-7: The development and testing environment(s) are separate from the production environment
	***PR.DS-8**: Integrity checking mechanisms are used to verify hardware integrity.*

Draft CSF v1.1, Framework Implementation Tiers:

Cyber Supply Chain Risk Management

Tier 1 - Partial: An organization may not understand the full of cyber supply chain risks or have the processes in place to identify, assess and mitigate its cyber supply chain risks.

Tier 2 - Risk Informed: The organization understands the cyber supply chain risks associated with the products and services that either supports the business mission function of the organization or that are utilized in the organization's products or services. The organization has not formalized its capabilities to manage cyber supply chain risks internally or with its suppliers and partners and performs these activities inconsistently.

Tier 3 - Repeatable: An organization-wide approach to managing cyber supply chain risks is enacted via enterprise risk management policies, processes and procedures. This likely includes a governance structure (e.g. Risk Council) that manages cyber supply chain risks in balance with other enterprise risks. Policies, processes, and procedures are implemented consistently, as intended, and continuously monitored and reviewed. Personnel possess the knowledge and skills to perform their appointed cyber supply chain risk management responsibilities. The organization has formal agreements in place to communicate baseline requirements to its suppliers and partners.

Tier 4 - Adaptive: The organization can quickly and efficiently account for emerging cyber supply chain risks using real-time or near real-time information and leveraging an institutionalized knowledge of cyber supply chain risk management with its external suppliers and partners as well as internally, in related functional areas and at all levels of the organization. The organization communicates proactively and uses formal (e.g. agreements) and informal mechanisms to develop and maintain strong relationships with its suppliers, partners, and individual and organizational buyers.

Potential Use Cases - Topics

We are not confined to what NERC-CIP has in their guidance, but it would be nice to have Use Cases to comport to what they are planning to do as we are using this as a guideline. We can readily identify a couple of Use Cases that cover the below topics:

NERC-CIP Compliance

- Software Assurance
- Software Authenticity
- Vendor Remote Access

SDLC Based (provided by Mike Cohen, MITRE)

I developed my proposed Use Cases by parsing the system development life cycle, I parsed the SDLC into the below three phases:

- System Acquisition Use Case: a tool suite that specifies the SCRM requirements that must be met for both the system being acquired and the manufacturer/system integrator who supplies the system
- Manufacturer/System Integrator Use Case: a tool suite that checks all components being assembled into the system for both unintended and intentional SCRM vulnerabilities

- System User Use Case: a tool suite for use during user acceptance testing, initial and ongoing operations, maintenance and upgrade, and final system disposal.

Oil and Gas Sector (Drilling Platforms) Supply Chain Concerns (provided by Siv Houmb, Secure-Nok/IADC)

Outlining the Drilling Supply Chain (DSP): In the DSP you have an operator that usually provides the requirements certification for drilling systems access. They do not typically own the drilling access so the most common way is for them to lease from a drilling contractor who owns various types of onshore and offshore drilling access. Drilling contractors usually don't make any systems themselves, so they purchase them from multiple vendors who buy from other vendors that are comprised of systems and hardware pieces from a third layer of vendors. It gets a little complicated both in the terms of the design phase and day-to-day operations as it relates to the cybersecurity of remote access and the site acceptance test (SAT).

The two biggest challenges for oil and gas (ONG) are:

- Identity management and access controls
  - As it relates to the current status of shared username and password, we would like to get to a stage where we could do some kind of working role task related identity management and then tie the access control to the work floor and all of the vendors that have access.

- Supply Chain coordinated incident response
  - If someone were to manipulate the blowout preventer system (BOP) or the Mud system which are very critical, you could be in a situation where you would have to act in coordination. At this time, we do not have any way to do that.

Additional Questions/Comments:

Jim McCarthy to Supply Chain SWG: The best way to move forward is to take what we have thus far and vet all the use cases proposals out to the community at large.

SWG agrees unanimously.

Action Items:

1) Provide the SWG with Jon Boyens contact information
2) Collect all use case ideas and submit to Energy Provider Community (EPC) Supply Chain Sub Working Group (SWG)
3) Schedule the next SWG call to review all proposals (tentative for 02/24/2017.
4) Jon Boyens to forward results from a previous workshop on Supply Chain technologies which will be shared with the SWG

Jim McCarthy concludes the Supply Chain SWG call at 2:58pm.