National Cybersecurity Center of Excellence (NCCoE)

Energy Sector Supply Chain SWG

Energy Provider Community of Interest

27 January 2017
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
01/13/2017 Meeting Summary

- 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

- Overview of other SCRM Initiatives
- Cybersecurity Framework (CSF) v 1.1 draft - Supply Chain Updates
<table>
<thead>
<tr>
<th>Date</th>
<th>Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>May 2012</td>
<td>ES-C2M2 Version 1, Supply Chain and External Dependencies Management Domain</td>
</tr>
<tr>
<td>February 2014</td>
<td>ES-C2M2 Version 2, O&amp;G C2M2, C2M2, Supply Chain and External Dependencies Management Domain</td>
</tr>
<tr>
<td>April 2014</td>
<td>Cybersecurity Procurement Language for Energy Delivery Systems</td>
</tr>
<tr>
<td>April 2015</td>
<td>UTC Supply Chain Risk Management for Utilities – Roadmap for Implementation</td>
</tr>
<tr>
<td>July 2016</td>
<td>FERC expresses and interest in supply chain management standard</td>
</tr>
<tr>
<td>September 2015</td>
<td>EEI Cyber Supply Chain Principles</td>
</tr>
<tr>
<td>January 2016</td>
<td>FERC Supply Chain Risk Management Conference on Supply Chain Risk Management</td>
</tr>
<tr>
<td>July 2016</td>
<td>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.</td>
</tr>
</tbody>
</table>
Determine cybersecurity requirements for suppliers/partners.

Enact cybersecurity requirements through formal agreement (e.g. contracts).

Communicate to suppliers/partners how those cybersecurity requirements will be verified and validated.

Verify cybersecurity requirements are met through a variety of assessment methodologies.

- Use Target Profile by organization to express cybersecurity risk management requirements to supplier/partner.
- Use by supplier/partner to express its cybersecurity state through a Current Profile to report results.

OT e.g. Subcategory selection (ID.BE-4, ID.SC-3, ID.SC-4, ID.SC-5, PR.DS-4, PR.DS-6, PR.DS-7, PR.DS-8, PR.IP-1, DE.AE-5, etc.).
### 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. |
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.
Cyber Supply Chain Risk Management Cont’d

**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.
NERC-CIP Compliance

- Software Assurance
- Software Authenticity
- Vendor Remote Access

SDLC Based (provided by Mike Cohen, MITRE)

- **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.
Procurement Language Related

Rich Donohue, BRG, has some procurement based supply chain language (per SWG call on 01/13) that includes discussion of technical controls

Oil and Gas Sector (Drilling Platforms) Supply Chain Concerns

Siv Houmb, CTO, Secure-Nok & IADC Cybersecurity Committee Lead
OPEN DISCUSSION

- Questions
- Action Items
- Schedule Next Meeting
ABOUT THE NCCOE
Information Technology Laboratory

MARYLAND OF OPPORTUNITY.

Department of Business & Economic Development
Goal

The purpose for establishing the NCCoE Supply Chain (SC) SWG is to identify one or more technology based use cases for Supply Chain Risk Management.

- Use case must solve a technology based SC challenge by utilizing a set of Cybersecurity tools and/or capabilities
- Use case should comport to existing or pending industry compliance standards
- Must be industry driven
WHO WE ARE AND WHAT WE DO

VISION
ADVANCE CYBERSECURITY
A secure cyber infrastructure that inspires technological innovation and fosters economic growth

MISSION
ACCELERATE ADOPTION OF SECURE TECHNOLOGIES
Collaborate with innovators to provide real-world, standards-based cybersecurity capabilities that address business needs

GOAL 1
PROVIDE PRACTICAL CYBERSECURITY
Help people secure their data and digital infrastructure by equipping them with practical ways to implement standards-based cybersecurity solutions that are modular, repeatable and scalable

GOAL 2
INCREASE RATE OF ADOPTION
Enable companies to rapidly deploy commercially available cybersecurity technologies by reducing technological, educational and economic barriers to adoption

GOAL 3
ACCELERATE INNOVATION
Empower innovators to creatively address businesses’ most pressing cybersecurity challenges in a state-of-the-art, collaborative environment
The NCCoE seeks problems that are:

- Broadly applicable across much of a sector, or across sectors
- Addressable through one or more reference designs built in our labs
- Complex enough that our reference designs will need to be based on a combination of multiple commercially available technologies

Reference designs address:

- Sector-specific use cases that focus on a business-driven cybersecurity problem facing a particular sector (e.g., health care, energy, financial services)
- Technology-specific building blocks that cross sector boundaries (e.g., roots of trust in mobile devices, trusted cloud computing, software asset management, attribute based access control)
Standards-based
Apply relevant local, national and international standards to each security implementation and account for each sector’s individual needs; demonstrate reference designs for new standards

Modular
Develop reference designs with individual components that can be easily substituted with alternates that offer equivalent input-output specifications

Repeatable
Enable anyone to recreate the NCCoE builds and achieve the same results by providing a complete practice guide including a reference design, bill of materials, configuration files, relevant code, diagrams, tutorials and instructions

Commercially available
Work with the technology community to identify commercially available products that can be brought together in reference designs to address challenges identified by industry

Usable
Design usable blueprints that end users can easily and cost-effectively adopt and integrate into their businesses without disrupting day-to-day operations

Open and transparent
Use open and transparent processes to complete work, and seek and incorporate public comments on NCCoE documentation, artifacts and results