National Cybersecurity Center of Excellence

Increasing the adoption of standards-based cybersecurity technologies

Energy Provider Community Call
09/26/2017
AGENDA

 Agenda

➢ NCCoE Energy Sector Planned Activities

➢ Status of Energy Sector Projects

➢ Scoping Energy Sector Asset Management

➢ Manufacturing Update (New COI)

➢ EPC Open Discussion / Comments / Questions
NCCoE ENERGY SECTOR PLANNED ACTIVITIES

➢ 4th Annual Industrial Cybersecurity Conference USA Summit
   October 3 – 4, Sacramento, CA
   NCCoE Energy and Manufacturing Sector Project Overview

➢ GridSecCon 2017, October 17-20, St. Paul, MN
   Convergence of Cybersecurity Situational Awareness Capabilities for
   the Energy Sector

➢ Automation Federation: LOGIIC Executive Committee
   October 24 -25, Houston, TX
   NCCoE Energy and Manufacturing Sector Project Overview
Situational Awareness SP 1800-7 (a,b,c)

- Released public draft - 02/16/2017
- Comment period closed - 04/17/2017
- Final adjudications complete
- Final draft expected Fall / 2017

https://nccoe.nist.gov/projects/use_cases/situational_awareness
- **Energy Sector Asset Management (ESAM)**
  - Focuses on asset management capability for the Energy Sector
  - Will include electric utilities, oil and gas, and other sub-sectors
  - Additional focus given to remote and geographically dispersed assets
  - Received formal project approval 09/20/2017
  - Draft Project Description: Q1 FY 2017 (December 2017)
  - Scoping ideas with EPC
Manufacturing Behavioral Anomaly Detection Use Case:

- NIST Engineering Lab (EL) and Information Technology Lab (ITL)
- Will leverage existing EL Robotics and Process Control infrastructure
- Projected Draft Practice Guide Release Date: 04/2018
• Questions/comments
Contact Us

Jim McCarthy, Senior Security Engineer
Energy Sector Lead
James.McCarthy@nist.gov
301-975-0228

http://nccoe.nist.gov
301-975-0200
nccoe@nist.gov
Foundations

Collaborative Hub

The NCCoE assembles experts from businesses, academia, and other government agencies to work on critical national problems in cybersecurity. This collaboration is essential to exploring the widest range of concepts.

As a part of the NIST cybersecurity portfolio, the NCCoE has access to a wealth of prodigious expertise, resources, relationships, and experience.
OUTCOME: Define a scope of work with industry to solve a pressing cybersecurity challenge

OUTCOME: Assemble teams of industry orgs, govt agencies, and academic institutions to address all aspects of the cybersecurity challenge

OUTCOME: Build a practical, usable, repeatable implementation to address the cybersecurity challenge

OUTCOME: Advocate adoption of the example implementation using the practice guide