National Cybersecurity Center of Excellence (NCCoE)
Energy Sector

Energy Provider Community of Interest

30 May 2017

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

NCCoE
NATIONAL CYBERSECURITY
CENTER OF EXCELLENCE

Agenda

- NCCoE Energy Sector Planned Activities
- Status of Energy Sector (and related) Projects
- Guest Speaker: Clint Bodungen, Kaspersky Lab N.A.
- EPC Open Discussion / Comments / Questions

NCCOE ENERGY SECTOR PLANNED ACTIVITIES

- **Energy Exchange 2017, August 15 – 17, Tampa, FL**
  Unpacking the IoT, Cloud, and Cyber Security Framework

- **GridSecCon 2017, October 17-20, St. Paul, MN**
  Abstract Submitted: ***Convergence of Cybersecurity Situational Awareness Capabilities for the Energy Sector***
  Proposed Panelists: NCCoE Energy Sector Team, UMd, PNNL, Dots and Bridges, LLC

- **RSA Charge 2017, October 17-19, Dallas, TX**
  SP-1800-7: Energy Sector Situational Awareness Practice Guide

ENERGY SECTOR PROJECT STATUS

- **Situational Awareness SP 1800-7 (a,b,c)**
  - Released public draft - 02/16/2017
  - Comment period closed- 04/17/2017
  - Selected internal and external reviewers for final document
  - https://nccoe.nist.gov/projects/use_cases/situational_awareness

- **Energy Sector Asset Management (Supply Chain)**
  - Derived from work performed on NCCoE Supply Chain Sub-working group
  - Focus on asset management capability for Energy Sector
  - Will give strong consideration to remote and geographically dispersed assets
  - NCCoE Business Case study underway as of 05/12/2017

ENERGY SECTOR PROJECT STATUS

- **Cybersecurity for Manufacturing**
  - Behavioral Anomaly Detection (BAD)
  - Federal Register Notice - 03/23/2017
  - Requested Collaborative Research and Development Agreements (CRADAs) with five tech vendors thus far
  - Three have accepted: GuardX, SecureNok, and Security Matters
  - Initial capabilities meetings currently being held with CRADA collaborators
  - Reference Architecture – early August, 2017
  - https://nccoe.nist.gov/projects/use_cases/capabilities-assessment-securing-manufacturing-industrial-control-systems

GUEST SPEAKER

- **Clint Bodungen, Senior Researcher, Critical Infrastructure Threat Analysis, Kaspersky Lab N.A.**
  - **Product Overview: SimICS**
  - **Author: “Hacking Exposed, Industrial Control Systems”**

EPC OPEN DISCUSSION

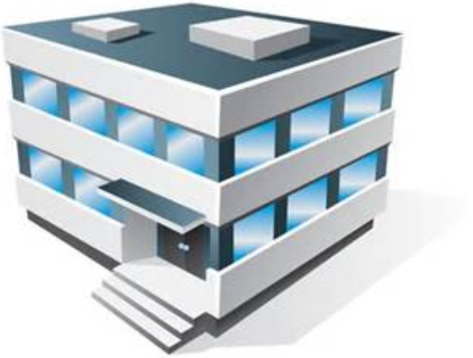
- Questions/comments

CONTACT US

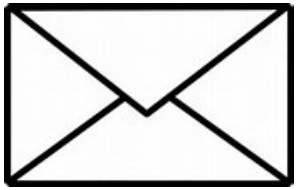
301-975-0200

http://nccoe.nist.gov/forums/energy

energy_nccoe@nist.gov



9700 Great Seneca Hwy,
Rockville, MD 20850



100 Bureau Drive, Mail Stop 2002,
Gaithersburg, MD 20899

Thank You

STRATEGY

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

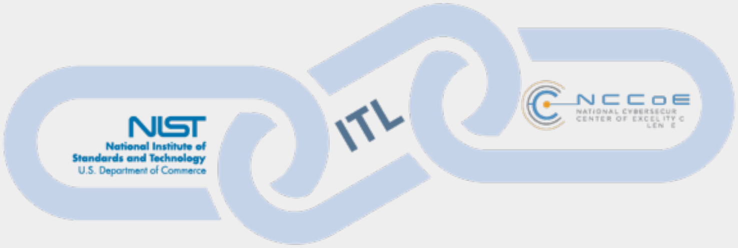
Enable companies to rapidly deploy commercially available cybersecurity technologies by reducing technological, educational and economic barriers to adoption

GOAL 3

ACCELERATE INNOVATION

Empower innovators to creatively address businesses' most pressing cybersecurity challenges in a state-of-the-art, collaborative environment

FOUNDATIONS

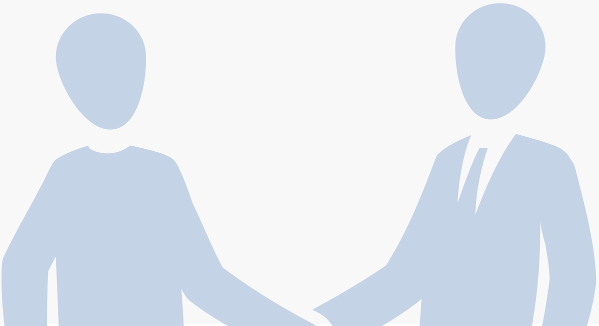

NIST
National Institute of Standards and Technology
U.S. Department of Commerce
ITL
NCCoE
NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

NIST ITL

The NCCoE is part of the NIST Information Technology Laboratory and operates in close collaboration with the Computer Security Division. As a part of the NIST family, the center has access to a foundation of prodigious expertise, resources, relationships and experience.

PARTNERSHIPS

Established in 2012 through a partnership between NIST, the State of Maryland and Montgomery County, the NCCoE meets businesses' most pressing cybersecurity needs with reference designs that can be deployed rapidly.



NIST CYBERSECURITY THOUGHT LEADERSHIP

- Cryptography
- Identity management
- Key management
- Risk management
- Secure virtualization
- Software assurance
- Security automation
- Security for cloud and mobility
- Hardware roots of trust
- Vulnerability management
- Secure networking
- Usability and security

STAKEHOLDERS

SPONSORS

Advise and facilitate the center’s strategy

- White House
- National Institute of Standards and Technology
- U.S. Department of Commerce
- U.S. Congress
- Montgomery County
- State of Maryland

TEAM MEMBERS

Collaborate to build real-world cybersecurity capabilities for end users

- NCCoE
- National Cybersecurity FFRDC*
- Tech firms
- Industry
- Academia
- Government
- Project managers
- Project-specific collaborators
- National Cybersecurity Excellence Partners (NCEP)

**Sponsored by NIST, the National Cybersecurity Federally Funded Research & Development Center (FFRDC) is operated by the MITRE Corporation*

END USERS

Work with center on use cases to address cybersecurity challenges

- Business sectors
- Individuals
- Academia
- Government
- Cybersecurity IT community
- Systems integrators

ENGAGEMENT & BUSINESS MODEL

DEFINE + ARTICULATE

Describe the business problem

Define business problems and project descriptions, refine into a specific use case

ORGANIZE + ENGAGE

Partner with innovators

Collaborate with partners from industry, government, academia and the IT community on reference design

IMPLEMENT + TEST

Build a usable reference design

Practical, usable, repeatable reference design that addresses the business problem

TRANSFER + LEARN

Guide users to stronger cybersecurity

Set of all material necessary to implement and easily adopt the reference design

BENEFITS

Cybersecurity solutions that are:

based on standards and best practices

usable, repeatable and can be adopted rapidly

modular, end-to-end and commercially available

developed using open and transparent processes

matched to specific business needs and bridge technology gaps

MODEL

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 the 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)