National Cybersecurity Center of Excellence

The 3rd Annual Intelligence and National Security Forum

Jim McCarthy

NIST / NCCoE

05/11/2018

This presentation is unclassified in its entirety

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

NCCoE NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

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.

NIST Information Technology Laboratory

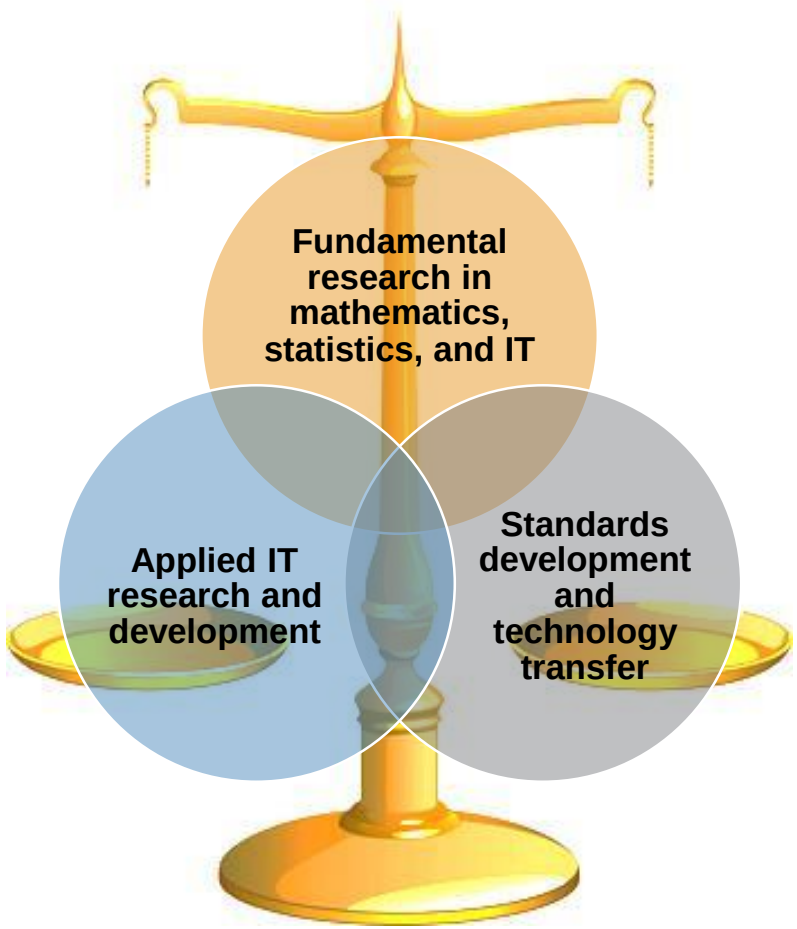
Cultivating Trust in IT and Metrology through measurements, standards and tests

ITL Programs

- Advanced Networking
- Applied and Computational Mathematics
- Cybersecurity
- Information Access
- Software and Systems
- Statistics

Collaborations with

- Industry
- Federal/State/Local Governments
- Academia



NIST Applied Cybersecurity Division (ACD)

Implements practical cybersecurity and privacy through outreach and effective application of standards and best practices necessary for the U.S. to adopt cybersecurity capabilities

ACD Programs

- Cybersecurity and Privacy Applications
- Cybersecurity Framework
- National Cybersecurity Center of Excellence
- National Initiative for Cybersecurity Education
- Privacy Engineering and Risk Management
- Trusted Identities Group

Mission

Accelerate adoption of secure technologies: collaborate with innovators to provide real-world, standards-based cybersecurity capabilities that address business needs

Engagement & Business Model

DEFINE

OUTCOME:
Define a scope of work with industry to solve a pressing cybersecurity challenge

ASSEMBLE

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

BUILD

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

ADVOCATE

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

SP 1800 Series

Volume A: Executive Summary

- High-level overview of the project, including summaries of the challenge, solution, and benefits

Volume B: Approach, Architecture, and Security Characteristics

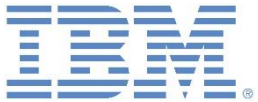
- Deep dive into challenge and solution, including approach, architecture, and security mapping to NIST Cyber Security Framework (CSF) and other relevant standards

Volume C: How-To Guide

- Detailed instructions on how to implement the solution, including components, installation, configuration, operation, and maintenance

CSF Function	CSF Subcategory	SP800-53R4[a]	IEC/ISO 27001[b]	CIS CSC[c]	NERC-CIP v5[d]
Identify	ID.AM-1: Physical devices and systems within the organization are inventoried	CM-8	A.8.1.1 A.8.1.2	CSC-1	CIP-002-5.1
	ID.AM-2: Software platforms and applications within the organization are inventoried	CM-8	A.8.1.1 A.8.1.2	CSC-2	CIP-002-5.1
Protect	PR.AC-2: Physical access to assets is managed and protected	PE-2, PE-3, PE-4, PE-5, PE-6, PE-9	A.11.1.1 A.11.1.2 A.11.1.4 A.11.1.6 A.11.2.3		CIP-006-6
	PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity	SI-7	A.12.2.1 A.12.5.1 A.14.1.2 A.14.1.3		
Detect	DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed	AC-4, CA-3, CM-2, SI-4			
	DE.AE-2: Detected events are analyzed to understand attack targets and methods	AU-6, CA-7, IR-4, SI-4	A.16.1.1 A.16.1.4		CIP-008-5
	DE.AE-3: Event data are aggregated and correlated from multiple sources and sensors	AU-6, CA-7, IR-4, IR-5, IR-8, SI-4			CIP-007-6

National Cybersecurity Excellence Partnership



NCCoE Tenets

Standards-based

Apply relevant industry standards to each security implementation; demonstrate example solutions for new standards

Modular

Develop components that can be easily substituted with alternates that offer equivalent input-output specifications

Repeatable

Provide a detailed practice guide including a reference design, list of components, configuration files, relevant code, diagrams, tutorials, and instructions to enable system admins to recreate the example solution and achieve the same results

Commercially available

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

Usable

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

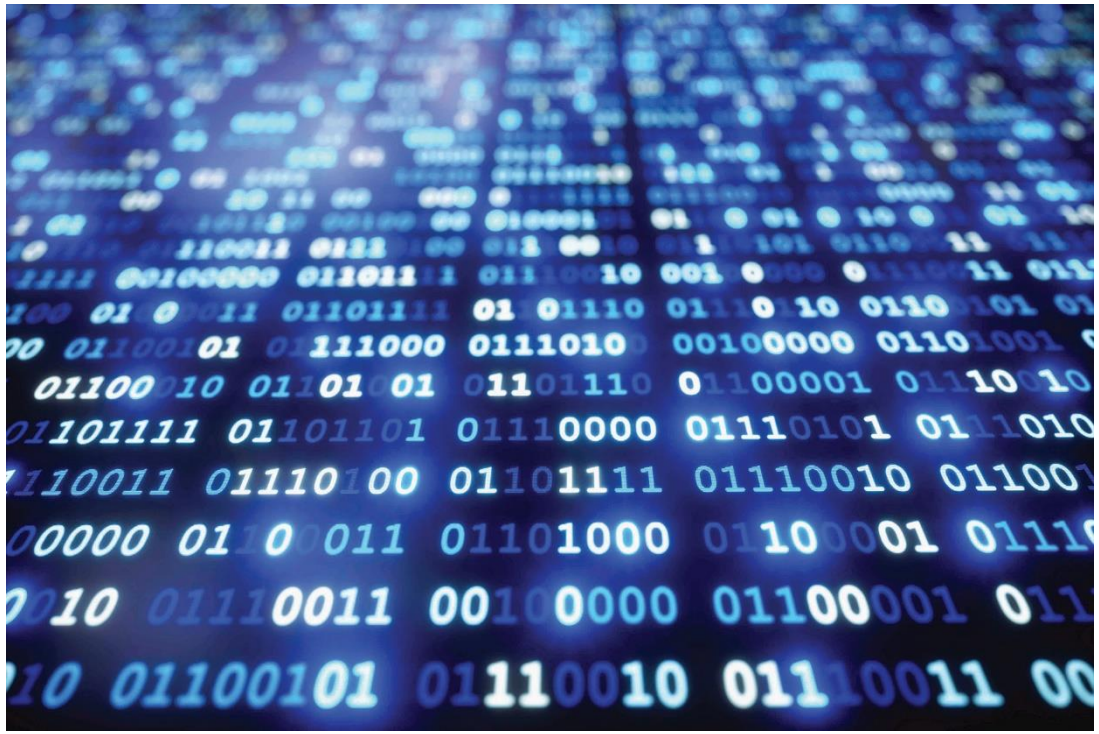
Open and transparent

Use open and transparent processes to complete work; seek and incorporate public comments on NCCoE publications

Portfolio

- Attribute Based Access Control (SP 1800-3)
- Consumer/Retail: Multifactor Authentication for e-Commerce
- Data Integrity: Recovering from a Destructive Malware Attack
- Derived Personal Identity Verification Credentials
- DNS-Based Email Security (SP 1800-6)
- Energy: Identity and Access Management (SP 1800-2)
- Energy: Situational Awareness (SP 1800-7)
- Financial Services: Access Rights Management
- Financial Services: IT Asset Management (SP 1800-5)
- Healthcare: Securing Electronic Health Records on Mobile Devices (SP 1800-1)
- Healthcare: Securing Wireless Infusion Pumps (SP 1800-8)
- Hospitality: Securing Property Management Systems
- Manufacturing: Capabilities Assessment for Securing Manufacturing Industrial Control Systems
- Mobile Device Security (SP 1800-4)
- Privacy-Enhanced Identity Federation
- Public Safety/First Responder: Mobile Application Single Sign-On
- Secure Inter-Domain Routing
- Transportation: Maritime: Oil & Natural Gas
- Trusted Geolocation in the Cloud (NISTIR 7904)

Sector-Based Projects



- Commerce/Retail
- Energy
- Financial Services
- Health Care
- Hospitality
- Manufacturing
- Public Safety/First Responder
- Transportation

Energy Sector

Projects

Identity and Access Management **(SP 1800-2)**

Situational Awareness **(SP 1800-7)**

Join our Community of Interest

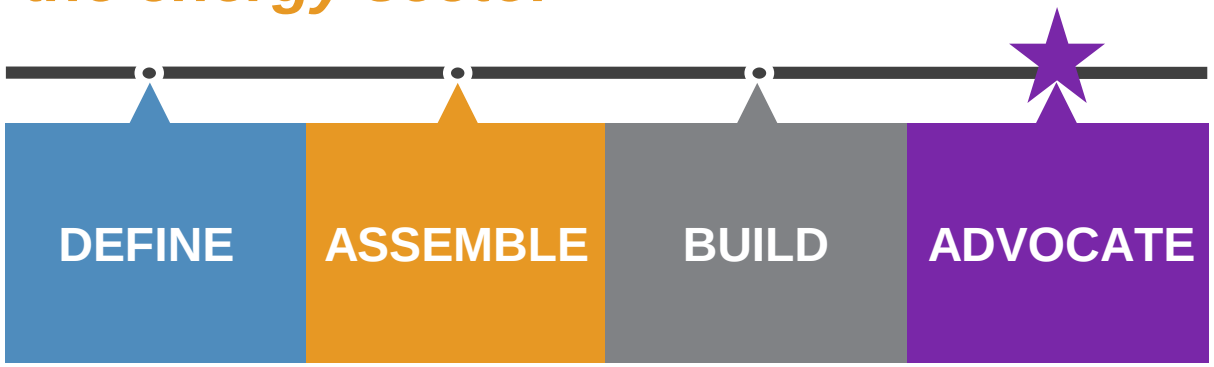
Email us at energy_nccoe@nist.gov

Identity and Access Management: SP 1800-2

Securing networked infrastructure for the energy sector

Overview

- Electric companies need to be able to control access to their networked resources
- Identity and Access Management (IdAM) implementations are often decentralized and controlled by numerous departments within a company
- The IdAM Practice Guide shows how an electric utility can implement a converged IdAM platform to provide a comprehensive view of all users within the enterprise across all silos, and the access rights they have been granted



Project Status

Revising practice guide to publish final SP 1800-2

Collaborate with Us

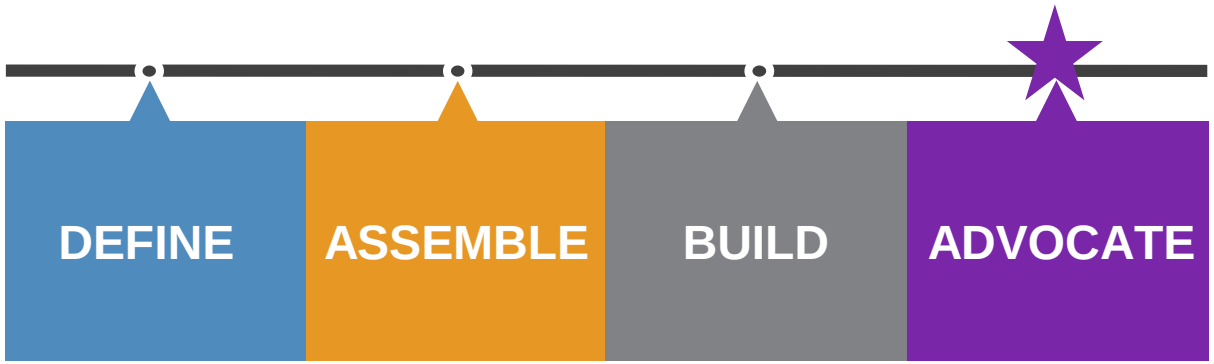
- Download NIST SP 1800-2, Identity and Access Management for Electric Utilities
- Email energy_nccoe@nist.gov to join the Community of Interest for this project

Situational Awareness: SP 1800-7

Improving security for electric utilities

Overview

- Energy companies rely on operational technology to control the generation, transmission, and distribution of power
- A network monitoring solution that is tailored to the needs of control systems would reduce security blind spots
- This project explores methods energy providers can use to detect and remediate anomalous conditions, investigate the chain of events that led to the anomalies, and share findings with other energy companies



Project Status

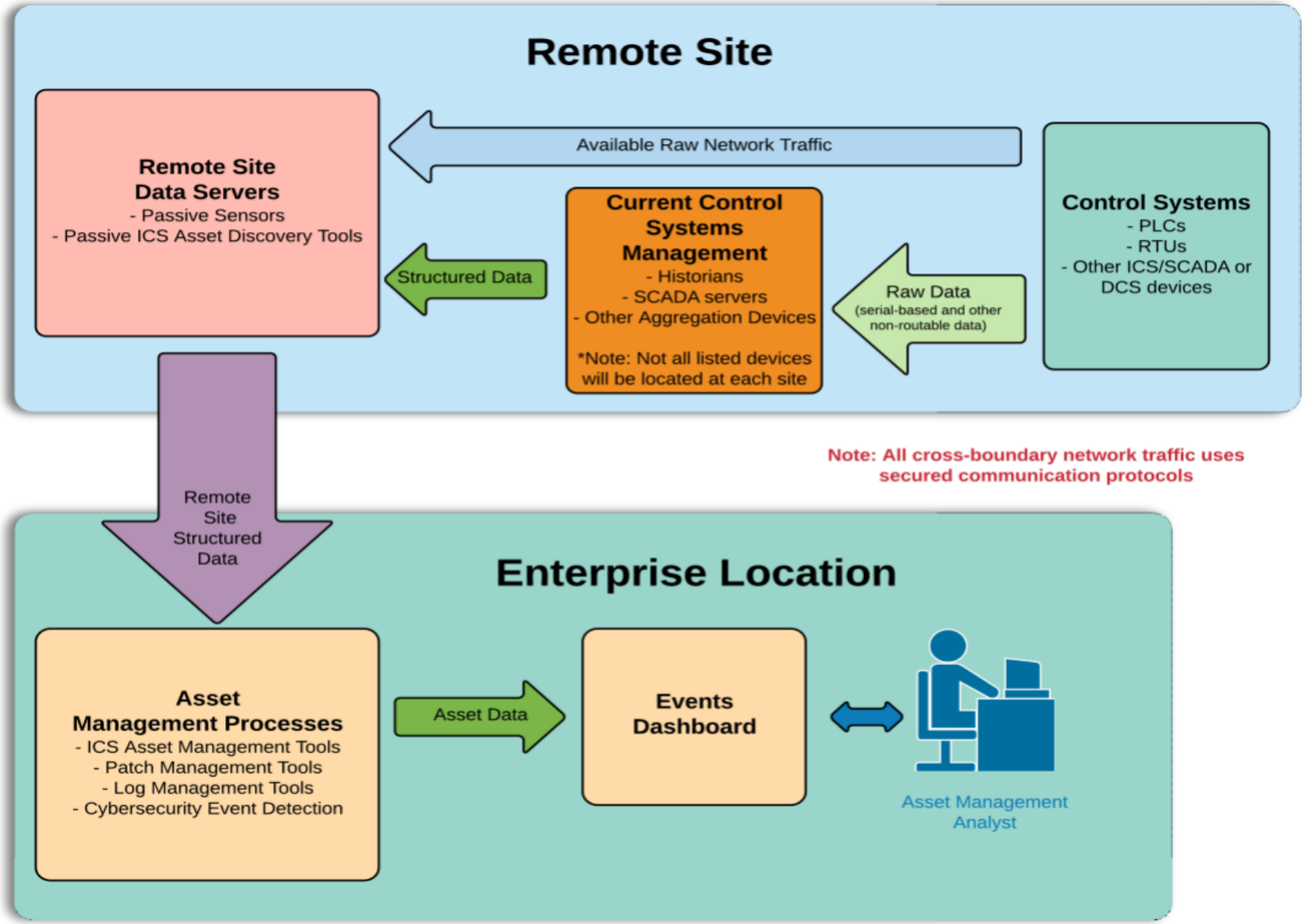
Accepting public comments on draft Practice Guide SP 1800-7 through April 17, 2017

Collaborate with Us

- Read SP 1800-7 Situational Awareness for Electric Utilities Practice Guide Draft
- Email energy_nccoe@nist.gov to join the Community of Interest for this project

- **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
  - Collaborator selection completed: May, 2018
  - Build Architecture: July, 2018
  - Draft ESAM Practice Guide Public Release: March, 2019

ESAM CONCEPTUAL ARCHITECTURE



University of Maryland

UNIVERSITY OF
MARYLAND

MANUFACTURING

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: 06/2018
- https://nccoe.nist.gov/sites/default/files/library/project-descriptions/mf-ics-1-project-description-final.pdf

Questions?

Jim McCarthy, Senior Security Engineer

James.McCarthy@nist.gov

301-975-0228

http://nccoe.nist.gov

301-975-0200

nccoe@nist.gov