National Cybersecurity Center of Excellence

Increasing the deployment and use of standards-based security technologies

Briefing to ITEA Cyber Workshop
29 March 2017

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

NCCoE
NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

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

ENGAGEMENT & BUSINESS MODEL

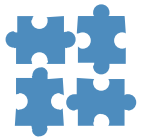
DEFINE + ARTICULATE	ORGANIZE + ENGAGE	IMPLEMENT + TEST	TRANSFER + LEARN
Describe the business problem	Partner with innovators	Build a reference design	Guide stronger practices
ACTION	**ACTION**	**ACTION**	**ACTION**
Identify and describe business problem	Publish project use cases and solicit responses	Build reference design	Collect documents
Conduct market research	Select partners and collaborators	Test reference design	Tech transfer
Vet project and use case descriptions	Sign CRADA	Identify gaps	Document lessons learned
OUTCOME	**OUTCOME**	**OUTCOME**	**OUTCOME**
Define business problems and project descriptions, refine into specific use case	Collaborate with partners from industry, government, academia and the IT community on reference design	Practical, usable, repeatable reference design that addresses the business problem	Set of all material necessary to implement and easily adopt the reference design

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

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



Modular

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

Usable

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

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

Open and transparent

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

NATIONAL CYBERSECURITY EXCELLENCE PARTNERS

NCEPs provide ongoing support (HW, SW, personnel) to Practice Guide development and NCCoE mission support

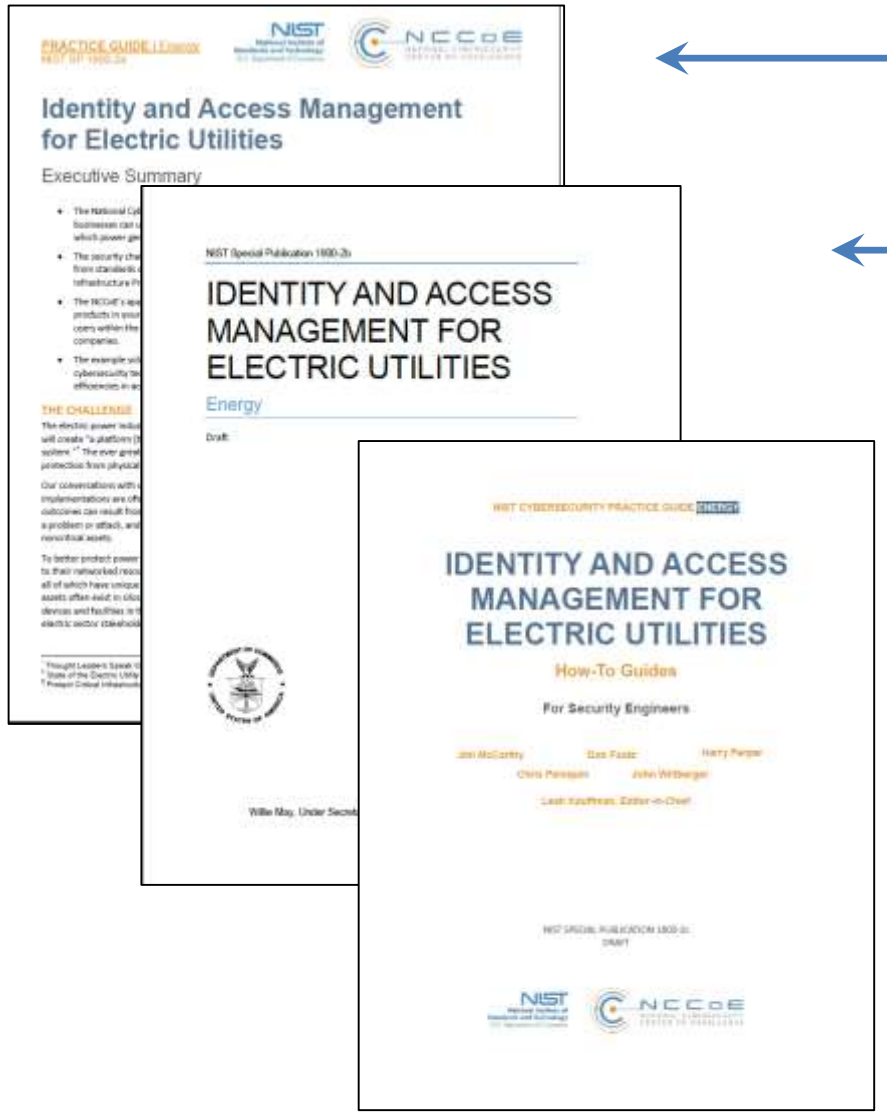
Over Twenty Labs dedicated to industry and technical challenges including:

- Health and IT
- Energy
- Mobile Device Security
- Financial Services
- Derived - PIV

Capabilities Including:

- Real-world components (Infusion Pumps, Access Controllers, Automobiles, etc.)
- VMs that can emulate dozens of nodes within an enterprise
- Vendor security products (through NCEPs and CRADA partners)
- Ability to VPN into labs to conduct analysis, demonstrations
- Consumer IoT devices

ANATOMY OF A PRACTICE GUIDE



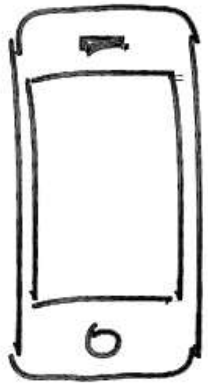
- Executive Summary
  - Overview of reference solution and key elements
- Approach, Architecture, and Security Characteristics
  - Problem context
  - Architecture solution
  - Security standards and controls mapping
  - ***Risk Assessment***
  - ***Functional Evaluation***
- How To Guide
  - Details on product installation, step-by-step instructions to support recreation of reference solution

- Financial Services
  - IT Asset Management (SP 1800-5)
  - Access Rights Management (Spring 2017)
- Energy
  - Identity and Access Management (SP 1800-2)
  - Situational Awareness (SP 1800-7)
- Health IT
  - Electronic Health Records (SP 1800-1)
  - Infusion Pumps (Spring 2017)
- Consumer / Retail
  - MFA for Card-not-present / e-commerce transactions
  - Secure handling of consumer PII and non-credit card data
- Transportation
  - Securing Law Enforcement Vehicles
  - Cybersecurity profile for bulk liquid transport (Fall 2016)
- Mobile Device Security (SP 1800-4)
- Data Integrity (Ransomware) (Summer 2017)
- DNS-based Secured Email (SP 1800-6)
- Derived Personal Identity Verification (PIV)
- Attribute Based Access Control (SP 1800-3)

- The NCCoE can help your organization:
  - Solve current cybersecurity challenges with commercially available technology
  - Develop a defense strategy for preventing tomorrow's problems
  - Apply standards from NIST and other relevant standards-setting organizations
  - Produce results quickly and efficiently
  - Connect best practices and lessons learned from across government and industry without additional research time

- The NCCoE can provide:
  - Deep industry-facing cyber expertise with a unique perspective
  - Full spectrum government service – civilian and defense
  - Access to NIST and the National Cybersecurity FFRDC
  - State-of-the-art facilities and equipment

- USM is a Partner in the execution of the NCF
- Direct Support to NCCoE Projects
  - Energy Grid Instrumentation (UMCP)
  - Health IT Survey (UMBC)
- Intern Support
  - Multiple students from UMCP ACES Program in FY16
- Technical Integration
  - Onsite technical integrator to coordinate efforts across USM and our Academic Affiliates Council
- Academic Affiliates Council
  - Provides outreach to other universities who can support NCCoE work
  - MITRE funded R&D

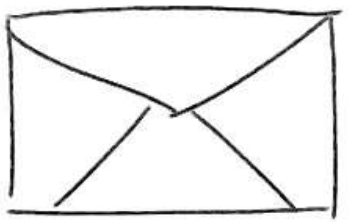


301-975-0200

nccoe@nist.gov

Participate

http://nccoe.nist.gov



100 Bureau Dr, M/S 2002
Gaithersburg, MD 20899