National Cybersecurity Center of Excellence

Increasing the deployment and use of standards-based security technologies

Healthcare Community of Interest Webinar

October 30, 2017

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

NCCoE
NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

Agenda

- HIT Intro: 5 mins
- NCCoE Overview: 5 mins
- Picture Archiving & Communication Systems (PACS): 30 mins
- Wireless Infusion Pumps (WIP): 15 mins
- Q&A: 5 mins

NCCoE
NATIONAL CYBERSECURITY
CENTER OF EXCELLENCE

NCCoE 101

Mission

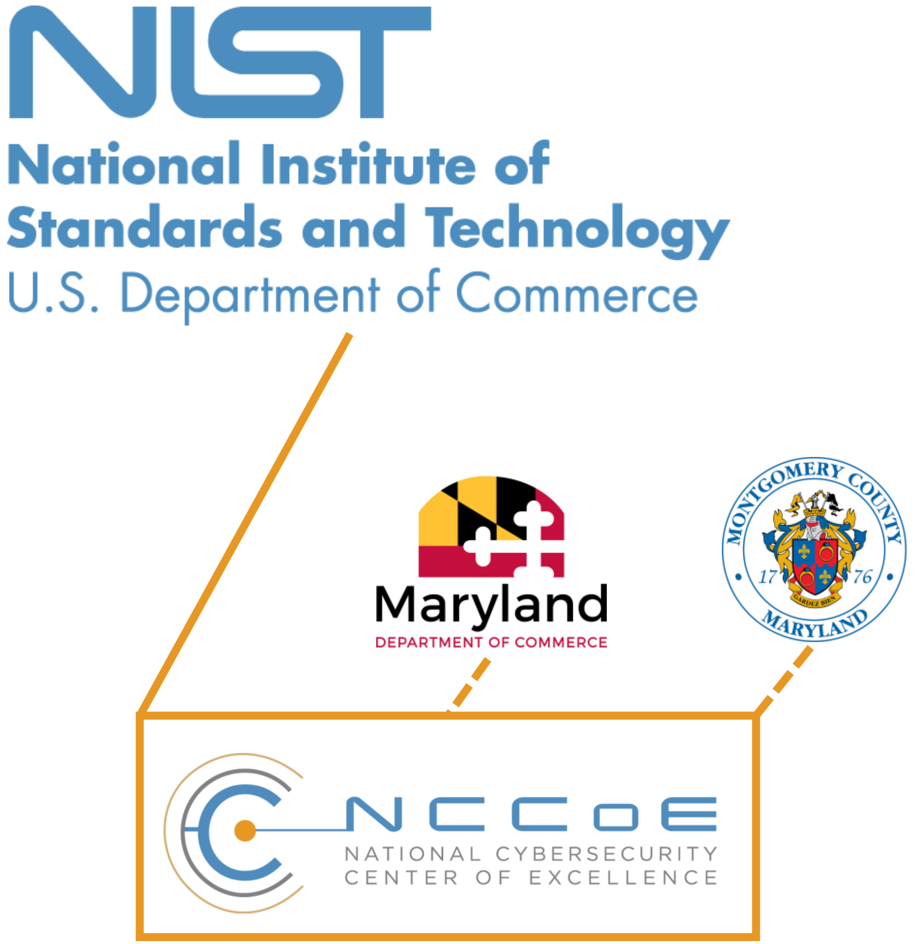
Accelerate adoption of secure technologies: collaborate with innovators to provide real-world, standards-based cybersecurity capabilities that address business needs

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
National Institute of Standards and Technology
U.S. Department of Commerce
Maryland
DEPARTMENT OF COMMERCE
MONTGOMERY COUNTY
17 76
MARYLAND
NCCoE
NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

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

Engagement & Business Model

DEFINE

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

1. **Conduct market research**
   - Explore and identify pressing cybersecurity challenges
   - Understand business needs and drivers
2. **Assess and document project scope and impact**
   - Meet with industry and industry organizations to further define cybersecurity challenges from technical and business perspectives
3. **Draft project description**
   - Define and refine specific challenge to address
   - Publish a draft project description with high-level architecture for public comment

Engagement & Business Model

ASSEMBLE

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

1. **Assemble Community of Interest (COI)**
   - Invite corporations and individuals with relevant knowledge, experience, and interest in shaping the project
   - Collaborate with COI to refine the final project description
2. **Seek innovative technology vendors**
   - Identify capabilities needed for the reference design
   - Publish a Federal Register Notice (FRN) inviting technology vendors to participate in the project build team
3. **Assemble project build team**
   - Technology vendors sign a Cooperative Research and Development Agreement (CRADA) to join build team and become technology collaborators
   - Technology collaborators contribute hardware, software, and expertise

Engagement & Business Model

BUILD

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

1. **Refine reference design**
   - Refine reference design based on the commercially available vendor technologies
   - Vet reference design with COI
2. **Build example implementation**
   - Integrate technologies into example implementation
   - An example implementation is a modular, easily adaptable set of instructions
3. **Engage industry and refine example implementation**
   - Demo example implementation for comment
   - Conduct outreach and engagement to industry and stakeholders

Engagement & Business Model

ADVOCATE

OUTCOME:
Advocate adoption of the example implementation using the easy-to-understand practice guide

1. **Publish SP 1800**
   - SP 1800 Practice Guides are free publications that encourage and instruct businesses to adapt the example implementation to their own environment
   - Available for download at https://nccoe.nist.gov, practice guides include three volumes of varying technical complexity

2. **Engage industry and seek feedback**
   - Each draft practice guide has a public comment period
   - Comments are reviewed and incorporated into final SP 1800 Practice Guide publication

3. **Encourage adoption of secure technologies**
   - Through outreach and engagement with industry, demonstrate how the example implementation can help solve the cybersecurity challenge

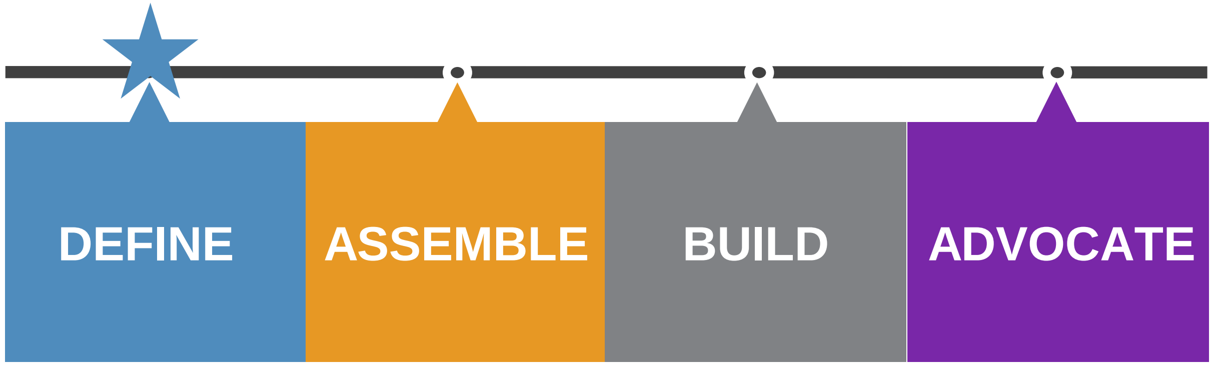
NCCoE
NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

Securing Picture Archiving & Communication Systems (PACS)

Securing Picture Archiving & Communication Systems (PACS)

Current Status/Next Steps

- Developing Draft Project Description
- **Nov 2017:** Publish Draft Project Description for public comment
  - 30-day comment period
  - NCCoE HIT Team will review comments and update project description
- **Jan 2018:** Publish revised Project Description by Federal Register Notice (FRN)
- Collaborators respond to FRN by submitting Letter of Interest (LOI)



Project Status

Developing Draft Project Description

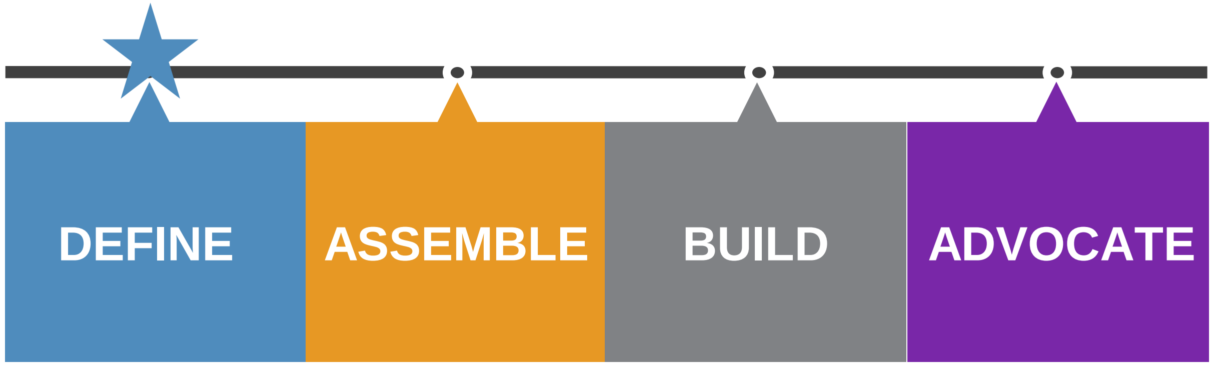
Collaborate with Us

- Join COI calls, contribute ideas, and share expertise
- Email hit_nccoe@nist.gov to join the Community of Interest for this project

Securing Picture Archiving & Communication Systems (PACS)

Next Steps

- Collaborators sign Cooperative Research and Development Agreement (CRADA)
- NCCoE forms Build Team
- Collaborators work with NCCoE to install and configure the products
- NCCoE writes and publishes NIST 1800-series Practice Guide
  - Collaborators provide comments on draft document before it is posted to the web site
  - Free publication and available for download from the NCCoE web site



Project Status

Developing Draft Project Description

Collaborate with Us

- Join COI calls, contribute ideas, and share expertise
- Email hit_nccoe@nist.gov to join the Community of Interest for this project

NCCoE
NATIONAL CYBERSECURITY
CENTER OF EXCELLENCE

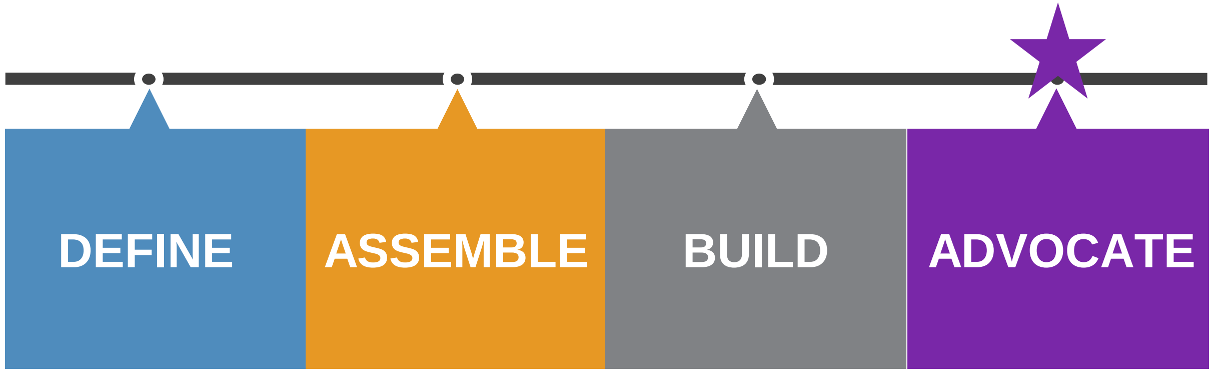
Securing Wireless Infusion Pumps *In Healthcare Delivery Organizations* (SP 1800-8)

Securing Wireless Infusion Pumps: (SP1800-8)

In Healthcare Delivery Organizations

Overview

- Background & Build Team
- Guiding Standards and References
- Risk-based approach and NIST CSF centric
  - Risk Assessment and Mitigation
  - Security Characteristics and Controls Mapping
  - Technologies / Products and Controls Mapping
  - Reference Architecture
  - Security Characteristics Analysis
  - Functional Evaluation
- Life Cycle Cybersecurity Issues / Future Build Considerations



Project Status

Draft Practice Guide, SP 1800-8 released May 8, 2017

Collaborate with Us

- Read SP 1800-8: Securing Wireless Infusion Pumps
- Email hit_nccoe@nist.gov to join the Community of Interest for this project