# Considerations in Migrating to Post-Quantum Cryptographic Algorithms

October 7, 2020

NCCoE

National Cybersecurity Center of Excellence

# Welcome to the NCCoE

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

NCCoE
NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

# Agenda

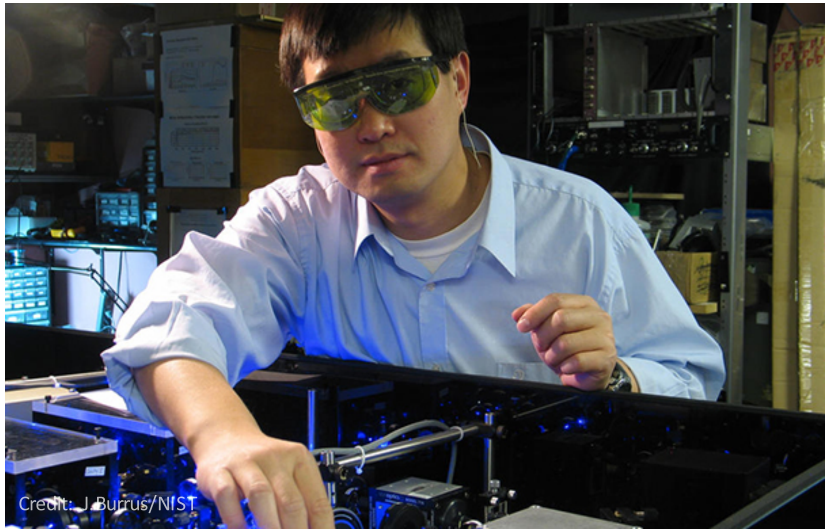
| | |
|---|---|
| **11:00 – 11:10 EDT** | **NIST and NCCoE Overview** |
| **11:10 – 11:25 EDT** | **Workshop Overview & Background** |
| **11:25 – 11:45 EDT** | **Status of NIST PQC Activity** |
| **11:45 – 11:55 EDT** | **Moderated Q&A** |
| **11:55 – 12:00 EDT** | *Break* |
| **12:00 – 1:00 EDT** | • **ETSI CYBER QSC WG, Migration to PQC**<br>• **Integration Challenges**<br>• **Customer Challenges**<br>• **Challenge Overview** |
| **1:00 – 1:10 EDT** | **Moderated Q & A** |
| **1:10 – 1:15 EDT** | *Break* |
| **1:15 – 2:30 EDT** | **Five/Ten Minute Participant Lightning Talks** |
| **2:30 – 2:45 EDT** | **Moderated Q & A** |
| **2:45 – 2:50 EDT** | **Next Steps/Wrap-up (NCCoE)** |

# National Institute of Standards and Technology

# NIST Mission

To promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life

©Robert Rathe

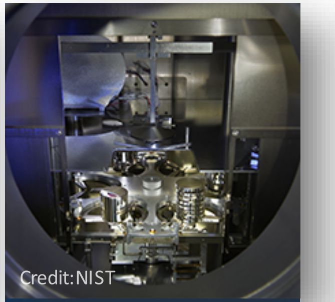

Credit: J.Burrus/NIST

©Nicholas McIntosh Photography

# Laboratory Programs

Credit:NIST

Material Measurement Laboratory



Credit:NIST

Physical Measurement Laboratory

Credit:Shutterstock/ Dmitry Kalinovsky

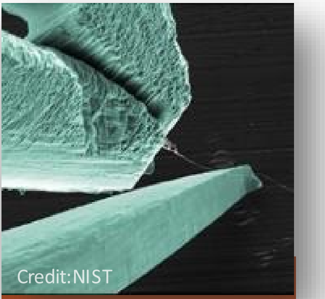
Engineering Laboratory

Credit:Shutterstock

Information Technology Laboratory

Credit: Shutterstock/Italianestro

Communication Technology Laboratory



Credit:NIST

Center for Nanoscale Science and Technology

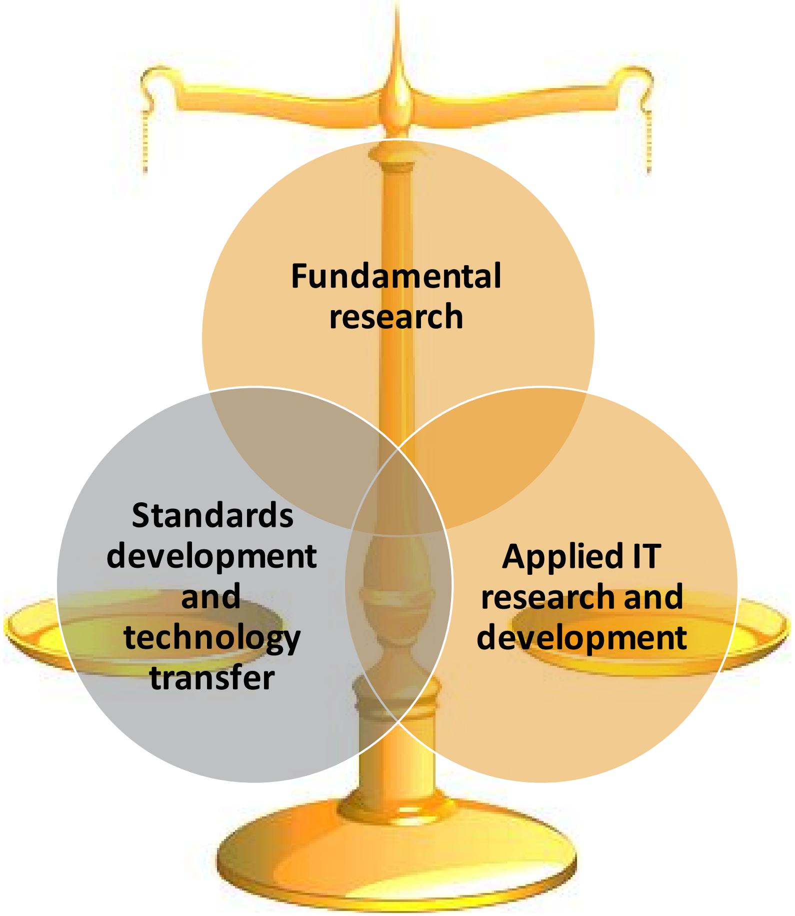
Credit:NIST

NIST Center for Neutron Research

# Information Technology Laboratory – itl.nist.gov

*Cultivating Trust in IT and Metrology*

## Cybersecurity Program


Fundamental research
Standards development and technology transfer
Applied IT research and development

### Standards and Guidelines Development – csrc.nist.gov

- Cryptographic Development – AES, SHA-3, PQC, etc.
- Cryptographic Validation – FIPS 140-3
- Risk Management Framework – Cybersecurity Framework, FISMA, SP 800-53, SP 800-171, etc.
- Technology Guidelines – Virtualization, Containers, Security Automation, etc.
- Framework for cybersecurity, privacy, workforce, and secure software development
- Identity Management

### National Cybersecurity Center of Excellence (NCCoE) – nccoe.nist.gov

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

DEFINE

ASSEMBLE

BUILD

ADVOCATE

Collaboration with Industry, Federal/State/Local Governments, and Academia

# Introduction to NCCoE

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

NCCoE
NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

# NCCoE Mission

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

# NCCoE 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

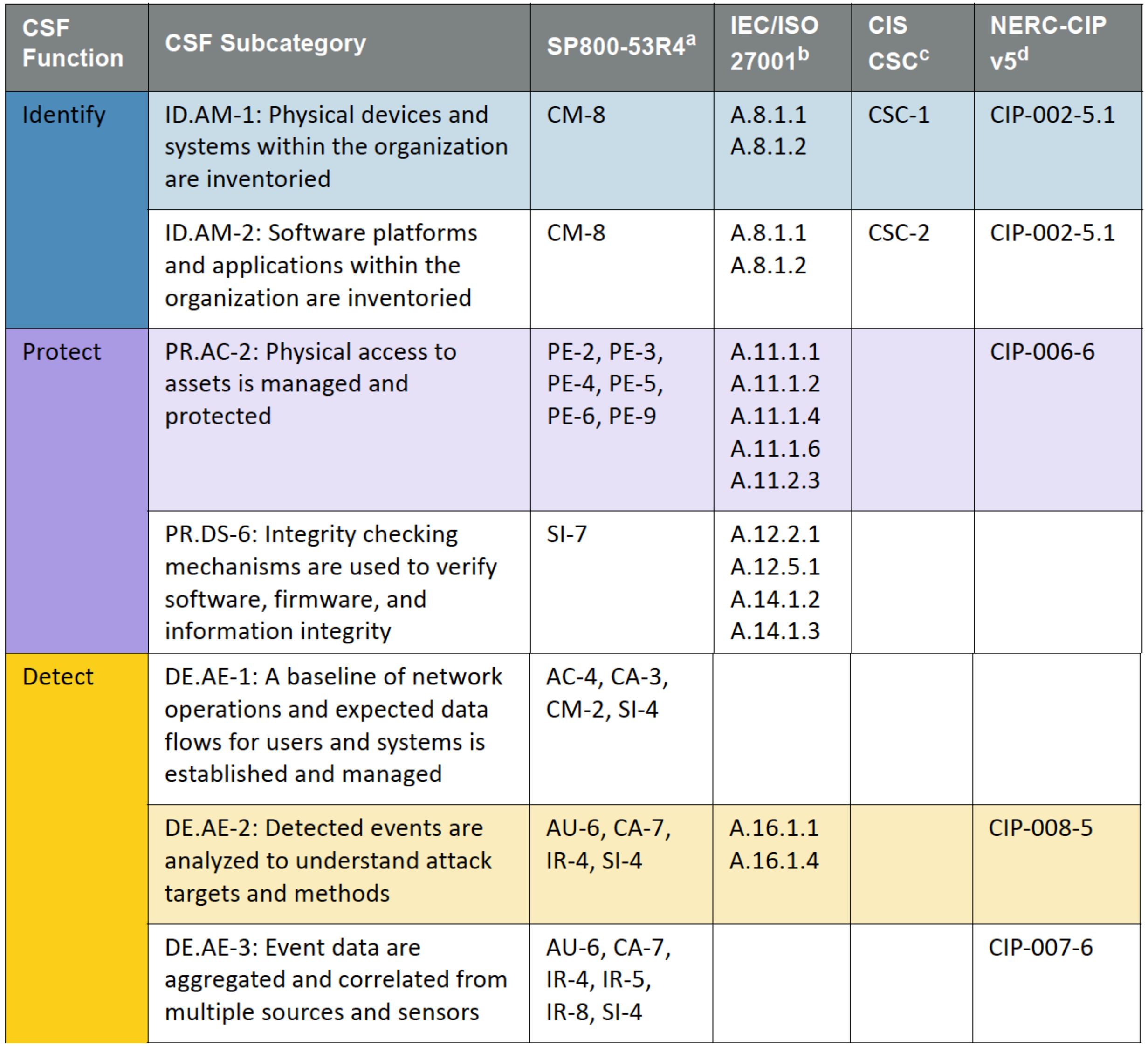
## BUILD 〉

**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:
# Cybersecurity Practice Guides



| 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<br>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<br>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<br>A.11.1.2<br>A.11.1.4<br>A.11.1.6<br>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<br>A.12.5.1<br>A.14.1.2<br>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<br>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 |

- 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 the Cybersecurity Framework and other relevant standards
- Volume C: How-To Guide
  - Detailed instructions on how to implement the solution, including components, installation, configuration, operation, and maintenance

# 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

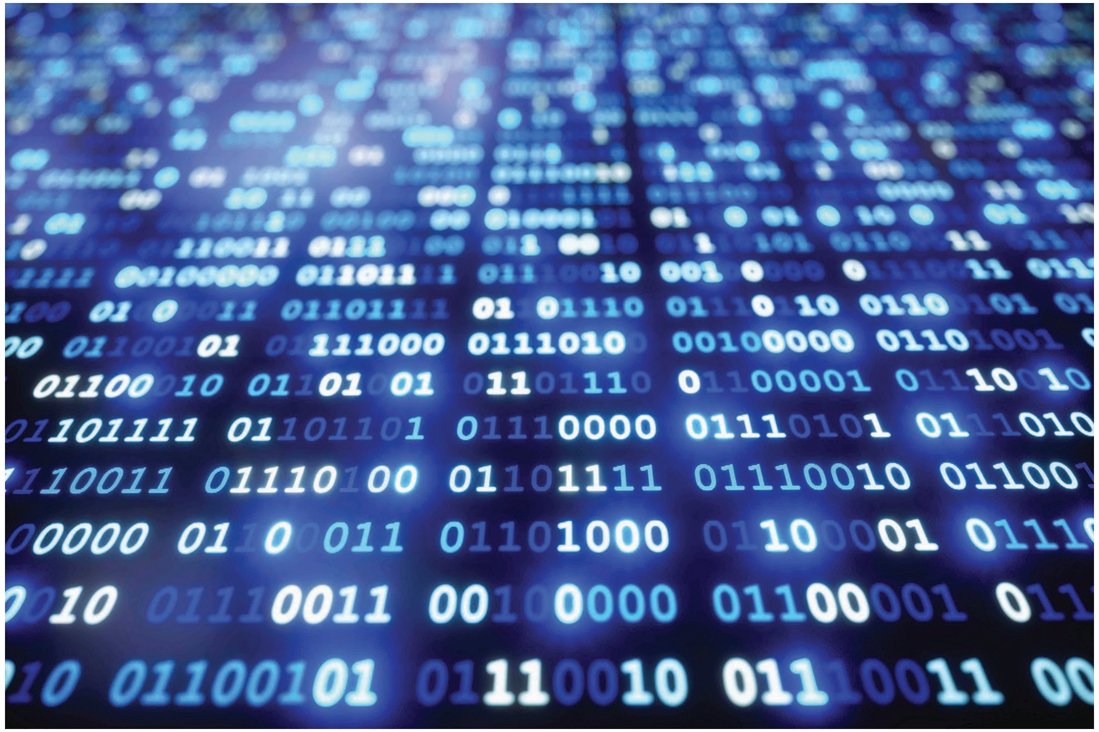
### Usable

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

# Sector-Based Projects



- Commerce/Retail (SP 1800-17)
- Energy (SP 1800-2 & SP 1800-7)
- Financial Services (SP 1800-5 & SP 1800-9 & SP 1800-18)
- Healthcare (SP 1800-1 & SP 1800-8)
- Hospitality
- Manufacturing
- Public Safety/First Responder (SP 1800-13)
- Transportation

# Cross-Sector Projects

- Attribute Based Access Control (SP 1800-3)
- Data Integrity (SP 1800-11)
- Derived PIV Credentials (SP 1800-12)
- DNS-Based Secured Email (SP 1800-6)
- Mitigating IoT-Based DDoS (SP 1800-15)
- Mobile Device Security (SP 1800-4 & SP 1800-21)
- Secure Inter-Domain Routing (SP 1800-14)
- TLS Server Certificate Management (SP 1800-16)
- Trusted Geolocation in the Cloud (SP 1800-19)

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

NCCoE
NATIONAL CYBERSECURITY
CENTER OF EXCELLENCE

# Thank you!