NIST National Cybersecurity Center of Excellence

Project Portfolio Webinar

February 19, 2026

This webinar is being recorded

NIST | NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

nccoe.nist.gov

Welcome

Goal:
Provide an overview of the NCCoE and our work, including more detail on our research portfolio, and a spotlight on a selection of our projects.

Today's webinar will use Slido to capture feedback throughout the session.

Scan using your mobile phone's camera app

OR

Follow this link (posted in the Zoom chat)

https://app.sli.do/event/eAZtvnhJC28BDyvzbcjPuz

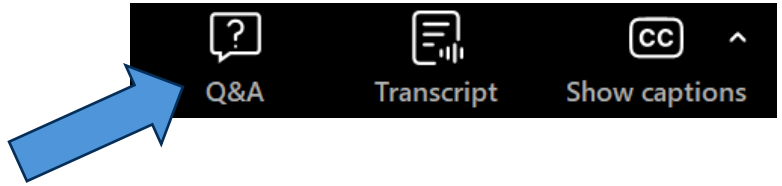
Agenda

Topic	Speaker(s)
Overview of the NCCoE	Cheri Pascoe
Project Portfolio Overview	Cheri Pascoe
Pillar Overview	Jon Davis
Project Spotlight: Migration to Post-Quantum Cryptography (PQC)	Bill Newhouse
Project Spotlight: Secure Software Development (DevSecOps)	Alper Kerman
Project Spotlight: Identity and Authorization of Software Agents	Bill Fisher
Project Spotlight: Transit CSF Profile	Chee Tang
Q&A / Wrap Up	Jon Davis

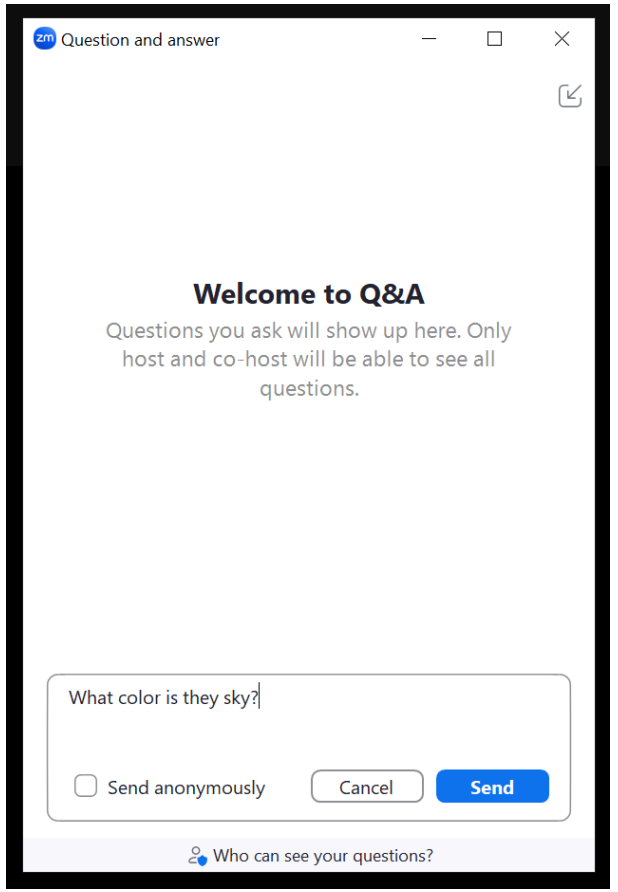
Submitting Questions

Please use the Q&A function to enter your questions.

We will do our best to answer your questions during the Q&A session at the end of the webinar.



1. To open the Q&A function, select “Q&A” on the bottom panel



2. Type your question in the text box and click Send

Speaker Introduction:

Cherilyn Pascoe
Director, NCCoE

NIST Strategy for American Technology Leadership in the 21st Century

NIST NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

NIST is committed to advancing American innovation and industrial competitiveness through **four interdependent strategic priorities:**

Accelerate innovation in critical emerging technologies of the future

Accelerate the commercial adoption of U.S. innovations

Bolster American leadership in standards

Build 21st century research infrastructure to unleash CET innovation

About the NCCoE

The NIST National Cybersecurity Center of Excellence (NCCoE) is a **collaborative hub convening experts from industry, government, and academia** to solve organizations' most pressing cybersecurity challenges.

Mission:

Accelerate the adoption of secure technologies.

A U.S. Cybersecurity Innovation Hub

NIST | NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

Over 180 collaborative agreements providing technology and expertise to support our work

The NCCoE's Impact

Strengthen U.S. Cybersecurity

Provide practical guides to help organizations implement standards-based, repeatable, and scalable solutions

Drive Standards Adoption & Innovation

Reveal opportunities to improve standards to better address real-world challenges

Improve Technology

Help vendors strengthen products' security and interoperability by building actual demonstrations

Foster Public-Private Innovation

Convene cybersecurity experts from industry, academia, and government to develop integrated solutions

NCCoE Project Portfolio

Provides an overview of the NCCoE and our work, including:

- Our four strategic pillars
- Active research projects
- Opportunities to provide input and get involved

Overview

Our Mission: Accelerate the Adoption of Secure Technologies

At the National Cybersecurity Center of Excellence (NCCoE), we collaborate with top cybersecurity experts and industry leaders to demonstrate practical ways to address the nation's most pressing cybersecurity challenges.

Advancing Cybersecurity Collaboration + Innovation

The NCCoE serves as a U.S. cybersecurity innovation hub for the technologies, standards, and architectures for today's cybersecurity landscape.

Through our collaborative testbeds and hands-on work with industry, we build and demonstrate practical architectures to address real-world implementation challenges, strengthen emerging standards, and support more secure, interoperable commercial products.

Our trusted, evidence-based guidelines show how organizations can reduce cybersecurity risks and confidently deploy innovative technologies aligned with secure standards.

Our work is:

- **Collaborative:** We partner with more than 180 organizations who contribute technology and expertise.
- **Practical:** We build testbeds based on real use cases using commercial technology.
- **Standards-Based:** We apply relevant NIST and industry standards to each security implementation.
- **Open and Transparent:** NCCoE resources are free and open for public comment.
- **Neutral:** We provide neutral, unbiased results from our testbeds showing how to use technology securely.
- **Impactful:** We align our projects to national priorities and industry needs.

This project portfolio provides an overview of active, new, and concluding NCCoE projects organized around four strategic pillars. It also describes opportunities for cybersecurity vendors and practitioners to provide input to help us validate priorities and keep the NCCoE's work focused on the cybersecurity challenges that matter most.

NCCoE by the Numbers:

22	180+	250+	700+
Active Projects	Active, Formal Collaborators	Cybersecurity Publications	Products Demonstrated

Project Spotlight: Implementing Zero Trust

This year, we concluded the NCCoE's zero trust architecture project with the publication of NIST Final SP 1800-35, *Implementing a Zero Trust Architecture*, offering organizations practical, actionable guidelines to design and implement zero trust architectures.

Since organizations have limited resources, we provide multiple examples—in this case, 19 real-world demonstrations in collaboration with 24 vendors—showing how to gradually evolve towards zero trust with existing infrastructures.

Our guidelines are used across the public and private sectors to inform organizations' cybersecurity architectures. Several federal agencies have adopted solutions based on our demonstrations—and our guidelines are shared widely by third parties.

Our work to promote zero trust continues through other projects, including our new DevSecOps project. All of this supports our goal to help organizations be more resilient and adapt to evolving cyber threats.

2

NIST NCCoE Project Portfolio

View the NCCoE Project Portfolio

How We Select Projects

- National Priorities
- NIST Mission and Available Resources
- NCCoE Mission Alignment
- Industry Signals

Our Pillars

NIST | NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

Data Protection

Cryptography, Identity, and Privacy

Trusted Enterprise

Foundational Infrastructure & Hardware Roots of Trust

Cybersecurity & Artificial Intelligence

Cybersecurity of AI Tools & AI for Cybersecurity

Resilient Embedded Systems

Cybersecurity of OT/ICS & IoT

Project Portfolio (as of January 2026)

NIST | NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

Data Protection

ACTIVE:

- **Digital Identities through Mobile Driver's Licenses**
- **Migration to Post-Quantum Cryptography**
- Privacy Enhancing Technologies Testbed

CONCLUDING:

- **Automation Support for the CMVP Program**
- Genomic Data
- Ransomware CSF Profile

Trusted Enterprise

ACTIVE:

- **5G Security Testbed**
- **Secure Software Development (DevSecOps)**

CONCLUDING:

- **Data Classification Practices**

Cybersecurity & Artificial Intelligence

FORMING:

- **Identity and Authorization of Software Agents**

ACTIVE:

- Autonomous Vehicle Vision
- Cyber AI Profile
- Dioptra
- NCCoE Chatbot

Resilient Embedded Systems

FORMING:

- **OT Cybersecurity: Asset Management**

ACTIVE:

- Manufacturing Supply Chain Traceability
- Positioning, Navigation, and Timing CSF Profile
- Semiconductor CSF Profile
- Transit CSF Profile

CONCLUDING:

- **Manufacturing Response and Recovery**
- **Water and Wastewater**

Legend
Bold: Formal Collaboration (CRADA)
Regular: Informal Collaboration (non-CRADA)

Data Protection

Data Protection

Cryptography, Identity, and Privacy

ACTIVE:

- Digital Identities through Mobile Driver's Licenses (mDL)
- Migration to Post-Quantum Cryptography (PQC)
- Privacy Enhancing Technologies Testbed

CONCLUDING:

- Automation Support for the CMVP Program
- Genomic Data
- Ransomware CSF Profile

Recent Highlights

- **mDL:** Announced New Government Use Cases & Presented on 12/16 Webinar
- **Ransomware:** Presented on 1/28 Ransomware Risk Management Webinar

What's Next

- **mDL:** Practice Guide for Financial Use Cases
- **PQC:** Automated Cryptographic Discovery and Inventory demonstrations
- **Genomics:** Genomic Data Threat Modeling Practice Guide
- **CMVP:** Practice Guide

Project Spotlight:

Migration to Post-Quantum Cryptography

NIST | NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

Goal: Demonstrate practices that ease the migration to PQC.

- Demonstrate capabilities of some automated cryptographic discovery and inventory (ACDI) tools.
- Create early opportunities for cryptographic algorithm collaborators to explore interoperability.

Collaborators: 55+ collaborators representing industry, software providers, hardware providers, and federal agencies.

Status:

- Published mapping of PQC migration capabilities to security objectives and controls from the NIST CSF 2.0 and SP 800-53 (September).
- Preparing to publish two papers outlining demonstrations of ACDI tools for endpoint and network layer algorithms.

Next Steps:

- Exploring potential demonstrations for hardware-based PQC implementations and challenges for Public Key Infrastructures (PKIs).

Project Spotlight:

Migration to Post-Quantum Cryptography

NIST | NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

CRADA Collaborators (as of February 2026)

- Amazon Web Services, Inc. (AWS)
- ATIS
- AvInyaSQ
- Cisco Systems, Inc.
- Cloudflare
- Comcast
- Crypto4A Technologies, Inc.
- CryptoNext Security
- Cybersecurity and Infrastructure Security Agency (CISA)
- CyberSeQ
- cyberzero
- Data-Warehouse GbmH
- Dell Technologies
- DigiCert
- Entrust
- General Dynamics Information Technology (GDIT)
- Google
- HP, Inc.
- HSBC
- IBM
- IDEMIA Secure Transactions
- Information Security Corporation
- InfoSec Global
- ISARA Corporation
- JPMorgan Chase Bank, N.A.
- Keyfactor
- Kudelski IoT
- Leidos
- M&T Bank
- Microsoft
- National Security Agency (NSA)
- NTT Data
- NXP Semiconductors
- Palo Alto Networks
- Post-Quantum
- PQSecure
- PQShield
- Qinvicta
- QuantumXchange
- QuSecure
- SafeLogic, Inc.
- Samsung SDS Co., Ltd.
- SandboxAQ
- Santander
- SEALSQ
- Siemens
- SSH Communications Security Corp
- Society for Worldwide Interbank Financial Telecommunication (SWIFT)
- Tectonic
- Tenable
- Thales DIS CPL USA, Inc.
- Thales Trusted Cyber Technologies
- Tychon
- U.S. Army DEVCOM C5ISR Center
- Utimaco
- Verizon
- Wells Fargo
- wolfSSL

Learn More: PQC Migration Project Page

Trusted Enterprise

NIST NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

Trusted Enterprise

Foundational Infrastructure & Hardware Roots of Trust

ACTIVE:

- 5G Security Testbed
- Secure Software Development (DevSecOps)

CONCLUDING:

- Data Classification Practices

Recent Highlights

- **Data Classification:** Published draft practice guide
  - **Currently open for public comment!**

What's Next

- **5G:** Upgrading 5G testbed + final versions of 5G White Paper series
- **DevSecOps:** Publishing resources from the first implementation

Project Spotlight:

Secure Software Development (DevSecOps)

NIST | NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

Goal: Develop guidelines that demonstrate the implementation of best practices based on NIST's Secure Software Development Framework (SSDF)

Collaborators: 14 formal collaborators providing products, services, and/or expertise

Status:

- Preparing to publish an updated Executive Summary, Introduction, and a notional reference model and resources from the first example implementation, focused on demonstrating DevSecOps practices in a Microsoft Azure environment

Next Steps:

- Publish use case scenarios for the first example implementation
- Begin the second example implementation

Learn More:
DevSecOps Project Page

Artificial Intelligence

NIST | NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

Cybersecurity & Artificial Intelligence

Cybersecurity of AI Tools & AI for Cybersecurity

FORMING:

- **Identity and Authorization of Software Agents**

ACTIVE:

- Autonomous Vehicle Vision (AVV)
- Cyber AI Profile
- Dioptra
- NCCoE Chatbot

Recent Highlights

- **Software Agent Identity:** Released Concept Paper to solicit input on a potential project
  - ➢ **Currently open for public comment!**
- **Cyber AI Profile:** Published the preliminary draft profile and conducted workshop to discuss

What's Next

- **AVV:** Publishing white papers on efforts to-date
- **NCCoE Chatbot:** Publications on prompt engineering and mitigating threats to LLM/RAG systems
- **Dioptra:** Enhancements to Dioptra's evaluation capabilities

Project Spotlight:

Identity and Authorization of Software Agents

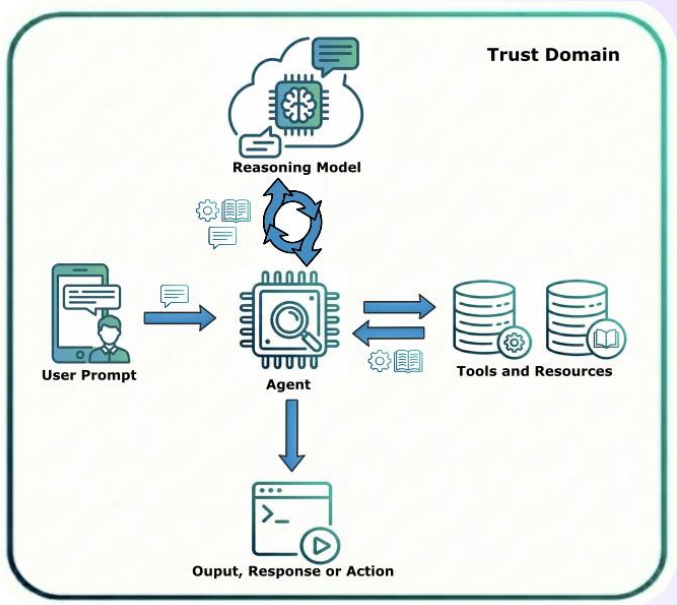
NIST | NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

Goal: Demonstrate how identity standards and best practices can be applied to software agents, focusing on Agentic AI applications.

- **Note:** This is a potential project that will be informed by public input.

Areas of Interest:

- Identification & Authentication
- Authorization
- Access Delegation/Non-Repudiation
- Logging and Transparency
- Tracking Data Flows



Status:

- Published Concept Paper on February 5.
- Comments open until April 2.
- Send comments to AI-Identity@nist.gov

Next Steps:

- Review public comments to determine project feasibility and scope.
- Publish a project description and invite collaborators to support the project.

Learn More:
Agentic AI Project Page

Resilient Embedded Systems

NIST | NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

Resilient Embedded Systems

Cybersecurity of OT/ICS & IoT

FORMING:

- OT Cybersecurity: Asset Management

ACTIVE:

- Manufacturing Supply Chain Traceability
- Positioning, Navigation, and Timing CSF Profile
- Semiconductor CSF Profile
- Transit CSF Profile

CONCLUDING:

- Manufacturing Response and Recovery
- Water and Wastewater

Recent Highlights

- **Transit Profile:** Released draft Profile
  - ➢ **Currently open for public comment!**
- **Supply Chain Traceability:** Released second draft of Meta-Framework

What's Next

- **OT Asset Management:** Publish project description for public feedback
- **Manufacturing Response and Recovery:** Publish draft practice guide for public feedback
- **Water and Wastewater:** Publish practice guide

Project Spotlight:

Transit CSF Profile

NIST NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

Learn More: Transit Profile Project Page

Goal: Develop a CSF Community Profile that helps transit operators manage cybersecurity risk alongside safety and operating requirements.

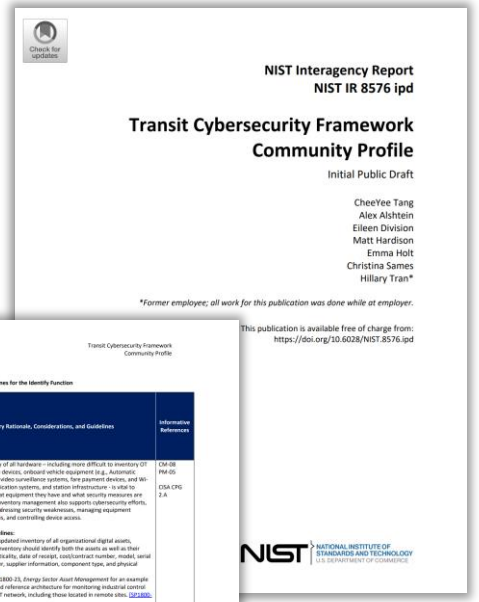
Collaborators: Includes Federal agencies, industry associations, and 15 transit agencies.

Status:

- Published draft Transit Profile on January 22.
- Comments open until February 23.

Next Steps:

- Review comments and publish final version.


NIST Interagency Report
NIST IR 8576 ipd

Transit Cybersecurity Framework Community Profile

Initial Public Draft

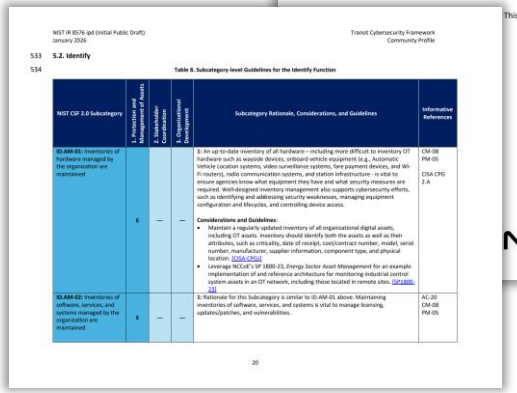
CheeYee Tang
Alex Alshtein
Eileen Division
Matt Hardison
Emma Holt
Christina Sames
Hillary Tran*

*Former employee; all work for this publication was done while at employer.

This publication is available free of charge from: https://doi.org/10.6028/NIST.8576.ipd


NEXTGOV FCW

NIST releases a new draft cybersecurity framework for systems that never stop moving



Open Q&A

NIST NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

Type your questions in the Q&A Section

How to Get Involved

NIST | NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

National Cybersecurity Excellence Partnership (NCEP)

Partners provide direction, resources and expertise to support the NCCoE's work

Cooperative Research and Development Agreement (CRADA)

Collaborators who provide hardware, software, and/or expertise for a project

Community of Interest (COI) Members

Individuals who want to learn about and provide input on the NCCoE's work

Interagency Agreements (IAAs)

Federal agencies who sponsor research projects at the NCCoE

Subscribe for Updates

Receive updates on NCCoE projects and publications

Join Events

Participate in the NCCoE's events and discussions

Provide Feedback

Review and provide feedback on our work

How to Stay Informed

Be the first to hear NCCoE updates!

Sign up to follow the NCCoE's work:

- Subscribe to NCCoE email updates
- Join a Community of Interest group
- Follow the NCCoE on LinkedIn
- Follow NIST Cyber on X

Scan the QR code to get started

NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

Questions? Feedback?

nccoe@nist.gov

nccoe.nist.gov