NIST NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

DRAFT

NCCoE Project Portfolio

Advancing Cybersecurity Collaboration and Innovation

January 21, 2026

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.

How to Get Involved

As a trusted convener of cybersecurity experts—and backed by more than 180 formal agreements with industry—the NCCoE offers many ways to get involved and shape our work.

Our collaboration includes both formal and informal mechanisms, designed to enable organizations to share challenges and solutions with the NCCoE.

Formal Collaboration Agreements:

Provide hands-on, technical collaboration on NCCoE projects

- NCCoE Partners: U.S.-based organizations can become NCCoE partners by signing a memorandum of understanding (MOU) to join the National Cybersecurity Excellence Partnership (NCEP) program. Partners provide technical input to help the NCCoE address emerging cybersecurity challenges and trends, collaborate to identify new projects, and gain insights from the NCCoE's work.
- Project Collaborators: Organizations can collaborate with the NCCoE by signing a Cooperative Research and Development Agreement (CRADA) to provide hardware, software, and/or expertise to support a project. Collaborators work together to demonstrate technology and develop supporting implementation guides and resources to help organizations understand how to design and deploy their own solutions.
- Government Agency Collaboration: Federal agencies can support work at the NCCoE by establishing inter-agency agreements, enabling a range of activities, such as research, technology development, and the publication of NIST resources. Additionally, government agencies can sign CRADAs or MOUs to collaborate on NCCoE projects. For example, the NCCoE has worked with a government agency to develop a cybersecurity framework community profile for a specific industry sector.

Informal Collaboration:

Shape our priorities and provide feedback on NCCoE projects

- Events: The NCCoE hosts a variety of in-person and virtual events to solicit input on our work and raise awareness of cybersecurity best practices. Individuals can join the NCCoE's events to hear directly from cybersecurity experts and learn more about the NCCoE's work.
- Communities of Interest: Individuals can join Communities of Interest (COIs) to learn about NCCoE projects and provide feedback and ideas to inform NCCoE projects and publications.
- Public Comments: As part of our commitment to openness and transparency, our resources are published for public comment. We encourage everyone to share their feedback, perspectives, and expertise during open comment periods.

Get Involved + Stay Informed

Want to get involved in our work and 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

Our Research Priorities

Cybersecurity is more than protection—it is enabling trust, unlocking innovation, and supporting the digital systems driving our economy. As threats, technologies, and standards evolve rapidly, organizations must too.

At the NCCoE, we believe cybersecurity progress requires prioritization, collaboration, innovation, and optimism. These values shape how we select projects, convene partners, and advance practical approaches to design and deploy secure technologies.

Our Projects

Our projects are selected based on their alignment with NIST and government and industry priorities.

- National Priorities: The challenge addresses a nationwide cybersecurity challenge.
- NIST Mission and Available Resources: The work builds on NIST standards and technology expertise in areas such as cryptography, identity, risk management, privacy, trustworthy systems, and more.
- NCCoE Mission Alignment: The work addresses a real-world challenge using commercial technology.
- Industry Signals: The topic is consistently identified by industry participants as a priority.

Projects are organized across four guiding pillars, designed to address a wide variety of cybersecurity challenges, as shown below.

1. Data Protection: Securing sensitive information by applying cryptography, identity, and privacy-preserving technologies.
2. Trusted Enterprise: Securing core IT infrastructure, encouraging secure software development, and driving zero trust adoption.
3. Artificial Intelligence (AI): Advancing AI by focusing on securing AI and the use of AI for cybersecurity.
4. Resilient Embedded Systems: Securing the Industrial Control Systems (ICS), Operational Technology (OT), and Internet of Things (IoT) that power our infrastructure and everyday lives.

Types of NCCoE projects

Technology Demonstrations:
We collaborate with industry through CRADA agreements to build end-to-end technical architectures and publish implementation guidelines using commercial technology and existing standards.

Exploration Projects:
We explore specific cybersecurity challenges through informal collaboration and publish resources to help organizations understand and mitigate cybersecurity risks.

Community Profiles:
We facilitate informal collaboration to develop a shared understanding of cybersecurity risks within a given community aligned to NIST's cybersecurity and privacy frameworks.

NCCoE Projects by Pillar (as of January 2026)

Data Protection

ACTIVE:
- Digital Identity Lab
- Digital Identities through Mobile Driver's Licenses
- Migration to Post-Quantum Cryptography
- Privacy Enhancing Technologies

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

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

Active Projects

Digital Identity Lab

POCs: Ryan Galluzzo, Bill Fisher | Contact: identity-lab-nccoe@nist.gov

Digital identity underpins secure access to systems. In 2025, the NCCoE launched a dedicated research lab to advance secure identity and authentication, focusing initially on passkey management for federal enterprise environments. An upcoming white paper will provide insights to help federal chief information security officers (CISOs) adopt next-generation authentication solutions.

Digital Identities through Mobile Driver's License (mDL)

POCs: Ryan Galluzzo, Bill Fisher | Contact: mdl-nccoe@nist.gov

Compared to physical driver's licenses, mobile driver's licenses (mDLs) are easier to use with digital transactions to prevent fraud, identity theft, and unauthorized access. The NCCoE's technology demonstration is tackling the security, privacy, and interoperability issues with mDLs. The NCCoE, working with industry and government partners, has developed a secure, standards-based reference architecture for mDLs, demonstrated real-world financial use cases, and delivered technical resources to support adoption. Next, the NCCoE will expand its mDL application in citizen-to-government use cases, working with new collaborators, like the General Services Administration's (GSA) Login.gov and Apple, to advance secure, efficient digital identity verification.

Migration to Post-Quantum Cryptography (PQC)

POC: Bill Newhouse | Contact: applied-crypto-pqc@nist.gov

Quantum computers powerful enough to break some public-key cryptography threaten the security of our data, systems, and networks—necessitating a transition from quantum-vulnerable cryptographic algorithms to quantum-resistant standards. The NCCoE's Migration to PQC project is working with collaborators to demonstrate practices that ease the migration to PQC. In collaboration with industry and federal partners, the project is demonstrating the capabilities of some automated cryptographic discovery and inventory tools and creating early opportunities for cryptographic algorithm coding collaborators to explore interoperability. The project is also exploring potential demonstrations for hardware-based PQC implementations and challenges for Public Key Infrastructures (PKIs) migrating to PQC.

Privacy Enhancing Technologies (PETs) Testbed

POCs: Gary Howarth, Justin Wagner, Ron Pulivarti | Contact: PETs@nist.gov

Performing data analysis—including training AI models—using sensitive data sources without adequate privacy protections can lead to the inadvertent disclosure of personally identifiable information (PII). Privacy Enhancing Technologies (PETs), such as differential privacy and secure multi-party computation, can enable data analysis and model training while protecting PII. The NCCoE launched a testbed to evaluate PETs and is continuing to incorporate additional technologies, with a focus on the analysis of sensitive genomic data. In 2025, the project conducted a public red teaming exercise to assess privacy risks against real-world attacks using genomic data. The team is seeking input to define impactful use cases and data types for scalable privacy solutions.

Concluding

Automation Support for the Cryptographic Module Validation Program (CMVP)

POC: Chris Celi | Contact: applied-crypto-testing@nist.gov

The Cryptographic Module Validation Program (CMVP) is essential for organizations required to use validated cryptography—ensuring that hardware and software cryptographic implementations meet standard security requirements. Given the volume of new modules and the pace of updates and patches to existing products, the volume and complexity of modules to be validated exceeds available capacity. To help the CMVP program complete timely validations, the NCCoE is demonstrating enhancements to streamline and automate the validation process. In 2026, the NCCoE will conclude its demonstration of the enhancements and publish results from the modernization effort.

Cybersecurity and Privacy of Genomic Data

POCs: Ron Pulivarti, Justin Wagner | Contact: genomic_cybersecurity_nccoe@nist.gov

Advancements in genomic sequencing technologies have accelerated the speed and volume of data collection and analysis—while creating vast amounts of data to be secured. The NCCoE is focused on understanding the threats to genomic data and opportunities to use secure technologies to address them. In 2026, the NCCoE will publish the final version of NIST Special Publication 1800-43, *Threat Modeling for Genomic Data*, with guidelines on cybersecurity and privacy threat modeling for genomic data. The NCCoE will also finalize the Genomic Data Cybersecurity and Privacy Community Profile (NIST IR 8467). The NCCoE's work on genomic data cybersecurity will continue through the PETs and Dioptra projects.

Ransomware CSF Profile

POC: Bill Fisher | Contact: ransomware@nist.gov

Ransomware attacks cause significant disruption to organizations, as well as significant losses. To help organizations identify and mitigate risks of ransomware attacks, the NCCoE is updating NIST IR 8374, *Ransomware Risk Management: A Cybersecurity Framework 2.0 Community Profile* to align with the NIST Cybersecurity Framework 2.0. The updated version provides practical guidelines for reducing ransomware incidents in line with the latest CSF outcomes and will publish a final version in 2026.

Active Projects

5G Security Testbed

POCs: Jeff Cichonski, Mike Bartock | Contact: 5G-security@nist.gov

As 5G networks bring unprecedented connectivity and speed, 5G introduces new security capabilities and new risks. The NCCoE has built a 5G testbed with a fully operational standalone network to demonstrate technologies and collaborate with industry to develop practical solutions to strengthen 5G security. This project is providing clear guidelines to help organizations deploy and manage safer 5G networks by leveraging the latest security features in current 5G standards. Looking ahead, we will upgrade our 5G testbed and explore new security measures for roaming, private 5G environments, and Open RAN (Open Radio Access Network).

Secure Software Development (DevSecOps)

POCs: Alper Kerman, Michael Ogata | Contact: devsecops-nist@nist.gov

The purpose of this project is to illustrate and document a practical approach to implementing NIST Secure Software Development Framework (SSDF) practices to elevate the overall security posture of organizations that develop and produce software in typical DevSecOps environments. Per Executive Order 14306, the NCCoE's DevSecOps project is demonstrating secure software development practices aligned with NIST's SSDF. This work will help organizations improve security at all stages of the software development lifecycle. In 2026, we will publish detailed guidelines, use cases, and reference architecture to further assist organizations.

Concluding

Data Classification Practices

POC: Bill Newhouse | Contact: data-nccoe@nist.gov

Data classification practices allow organizations to discover, identify, and label their unstructured data—which is a pre-requisite for organizations to use zero trust architectures, start post-quantum cryptography migrations, and use artificial intelligence. Unstructured data that has undergone data classification practices becomes ready to benefit from data-centric technologies that can apply an organization's cybersecurity and privacy policies. In early 2026, the team will release the draft NIST Special Publication 1800-39, *Implementing Data Classification Practices*, with demonstrations of data classification practices on unstructured data for public comment.

Forming Projects

Identity and Authorization of Software Agents

POCs: Bill Fisher, Ryan Galluzzo, Harold Booth | Contact: AI-Identity@nist.gov

As AI agents are empowered to take on more tasks, enterprises need reliable ways to verify their identity and authorizations. Based on stakeholder input, the NCCoE is interested in launching a technology demonstration project to demonstrate how identity standards and best practices can be applied to software agents, with a focus on agentic AI applications. The team intends to publish a concept paper and solicit input from the community to inform the scope for potential future projects.

Active Projects

Autonomous Vehicle Vision

POC: Apostol Vassilev | Contact: amat@nist.gov

With the increasing deployment of AI-enabled autonomous vehicles, cyber assurance is crucial to protect against potential threats that could manipulate or disrupt the vehicle's perception of its surroundings, compromising safety and trust in these systems. The NCCoE is working on cyber assurance for autonomous vehicles by developing a public dataset and a testbed with difficult-to-handle and adversarial road/traffic conditions with the goal of improving autonomous vehicles and accelerating their safe deployment. In 2026, the project is planning to release white papers on its efforts.

Cyber AI Profile

POC: Kat Megas, Barbara Cuthill | Contact: CyberAIProfile@nist.gov

Artificial Intelligence (AI) has become a driving force behind today's technological development, transforming industries and redefining how society operates. Advancements in AI technology introduce both cybersecurity opportunities and challenges to organizations. The NCCoE is developing a Cyber AI Profile to help organizations address emerging cybersecurity risks from AI by applying existing frameworks like the NIST Cybersecurity Framework. This work will guide the community in securing AI systems, enabling AI-driven cyber defense, and countering AI-enabled cyber-attacks. In January, the NCCoE hosted a public workshop to gather input on the preliminary draft profile.

Dioptra

POC: Harold Booth | Contact: dioptra@nist.gov

With the growing reliance on machine learning systems, rigorous security evaluations are crucial for understanding and mitigating potential vulnerabilities. Dioptra is a software test platform for facilitating various types of evaluation, including security evaluations of attacks and defenses for machine learning systems. The NCCoE is developing new features for Dioptra to improve usability and aid in the design of experiments. The NCCoE is also working to integrate various open-source libraries into Dioptra and expand the scope of its evaluation capabilities. In 2026, Dioptra will demonstrate features and use cases for characterizing genomic data.

NCCoE Chatbot

POCs: Alper Kerman, Harold Booth | Contact: nlp-nccoe@nist.gov

The NCCoE is conducting an internal pilot to understand and explore the benefits and risks of generative AI systems, as well as potential strategies to mitigate potential threats. In June 2025, the project team published NIST IR 8579, *Development and Implementation of the NCCoE Chatbot: A Comprehensive Report*, outlining point in time lessons learned from this pilot. Future planned publications provide additional lessons learned on mitigating threats to Large Language Model (LLM) and Retrieval Augmented Generation (RAG) systems, as well as on prompt engineering.

Forming Projects

OT Cybersecurity: Asset Management

POCs: Michael Powell, CheeYee Tang | Contact: ot_nccoe@nist.gov

Effective asset management—maintaining accurate tracking of devices, systems, and their configurations—is a critical foundation for cybersecurity. Asset management within OT networks can be particularly challenging due to multiple factors: legacy system limitations, geographically distributed assets, diverse communication protocols and architectures, and operational constraints. This complexity makes it more difficult for organizations to assess risk and adopt modern security controls, like zero trust. Based on stakeholder input, the NCCoE is interested in launching a technology demonstration to provide practical guidelines for achieving and maintaining OT cybersecurity, starting with asset management. This work will help organizations establish the foundation to support risk assessments and implement modern security controls, guided by the challenges specific to OT. In 2026, the NCCoE plans to publish a project description for public feedback and invite collaborators to support the project.

Active Projects

Manufacturing Supply Chain Traceability

POC: Michael Pease | Contact: blockchain_nccoe@nist.gov

The growing complexity and interdependency of supply chains underscore the need for traceability of components, materials, and products to mitigate cybersecurity risks, maintain supply chain integrity, and facilitate effective supply chain risk management. Building upon frameworks and standards such as NIST CSF 2.0 and IEC 62443, the NCCoE is investigating the challenges of supply chain traceability and linking traceability records through the development of a Meta-Framework. This work aims to help suppliers and manufacturers envision effective and interoperable traceability solutions to support stronger supply chain risk management. In 2026, the NCCoE will expand the Meta-Framework principles and concepts by publishing a reference implementation to support the investigation and experimentation of traceability use cases.

Positioning, Navigation, and Timing (PNT) CSF Profile

POCs: Nakia Grayson, Ya-Shian Li-Baboud, Suzanne Lightman | Contact: pnt-nccoe@nist.gov

Positioning, Navigation, and Timing (PNT) services—such as the Global Positioning System (GPS)—are foundational capabilities for our nation's infrastructure. NIST developed the original PNT Community Profile to support organizations that rely on PNT services, providing a flexible structure for identifying and mitigating risks to systems, networks, and assets using PNT signals and data. In March 2025, NIST announced plans to update the PNT Community Profile to reflect the new CSF 2.0, as well as stakeholder feedback.

Semiconductor Manufacturing CSF Profile

POCs: Alex Nelson, Nakia Grayson | Contact: semiconductor-manufacturing-profile@nist.gov

The semiconductor manufacturing process is highly complex and dependent upon interconnected networks, making it vulnerable to cybersecurity threats. The NCCoE is working with industry stakeholders to develop a CSF Community Profile to provide guidelines for secure semiconductor manufacturing. The project team is currently reviewing feedback on the draft Profile and engaging with the community.

Transit CSF Profile

POC: CheeYee Tang | Contact: transit-nccoe@nist.gov

Transit agencies manage a complex network of interconnected digital systems supporting critical functions, such as signaling, scheduling and dispatch, emergency communications, and more, increasing their vulnerability to cyber-attacks. The NCCoE is working with industry and federal agencies to develop a CSF Community Profile that helps transit operators manage cybersecurity risk alongside safety and operating requirements—addressing key cybersecurity challenges and providing practical guidelines for improving resilience. In January 2026, the NCCoE will publish the initial public draft of the Community Profile and will publish a final version later in the year.

Concluding

Manufacturing Response and Recovery

POC: Michael Powell | Contact: manufacturing_nccoe@nist.gov

Although strong security measures can mitigate cyber risks, cyber-attacks can still happen. For OT/ICS systems, responding quickly and recovering from a cyber-attack is critical; a well-planned response and recovery strategy enables organizations to mitigate the effects of an attack and rapidly restore control systems to a safe and operational state. The NCCoE is completing its work with industry to demonstrate an approach for responding to and recovering from an attack on ICS systems within the manufacturing sector by leveraging the following cybersecurity capabilities: event reporting, log review, event analysis, and incident handling and response. In early 2026, the project will publish an initial public draft of guidelines to help manufacturers respond and recover from cyberattacks.

Water and Wastewater

POC: CheeYee Tang | Contact: water_nccoe@nist.gov

Water and wastewater (WWS) utilities are increasingly being targeted by cyber criminals and nation-state actors with intent to disrupt U.S. critical infrastructure, particularly through remote access. The NCCoE is finalizing its work with collaborators to demonstrate technologies and architectures to achieve secure remote access for water and wastewater utilities. The project plans to publish final guidelines in 2026.

Past Projects

Since the NCCoE was established in 2012, our projects have demonstrated our commitment to developing practical, standards-based approaches to enhance cybersecurity across industries.

A brief selection of example projects is provided below:

- Access Rights Management for the Financial Services Sector
- Addressing Visibility Challenges with TLS 1.3 within the Enterprise
- Attribute Based Access Control
- Data Confidentiality
- Data Integrity: Ransomware and Other Destructive Events
- Derived Personal Identity Verification (PIV) Credentials
- Domain Name System-Based Electronic Mail Security
- Energy Sector Asset Management: For Electric Utilities, Oil & Gas Industry
- Identity and Access Management for Electric Utilities
- Implementing a Zero Trust Architecture
- Improving Enterprise Patching for General IT Systems
- IT Asset Management
- Mobile Application Single Sign-On: Improving Authentication for Public Safety First Responders
- Mobile Device Security: Cloud and Hybrid Builds
- Multifactor Authentication for E-Commerce
- Privileged Account Management for the Financial Services Sector
- Protecting Information and System Integrity in Industrial Control System Environments
- Protecting the Integrity of Internet Routing: Border Gateway Protocol (BGP) Route Origin Validation
- Securing Distributed Energy Resources
- Securing Electronic Health Records on Mobile Devices
- Securing Picture Archiving and Communication System (PACS)
- Securing Property Management Systems
- Securing Small-Business and Home Internet of Things (IoT) Devices
- Securing Telehealth Remote Patient Monitoring Ecosystem
- Securing Web Transactions: TLS Server Certificate Management
- Securing Wireless Infusion Pumps in Healthcare Delivery Organizations
- Trusted Cloud: Security Practice Guide for VMware Hybrid Cloud Infrastructure as a Service (IaaS)
- Trusted IoT Device Network Layer Onboarding
- Validating the Integrity of Computing Devices

For more information on these and other projects, visit our website at https://nccoe.nist.gov

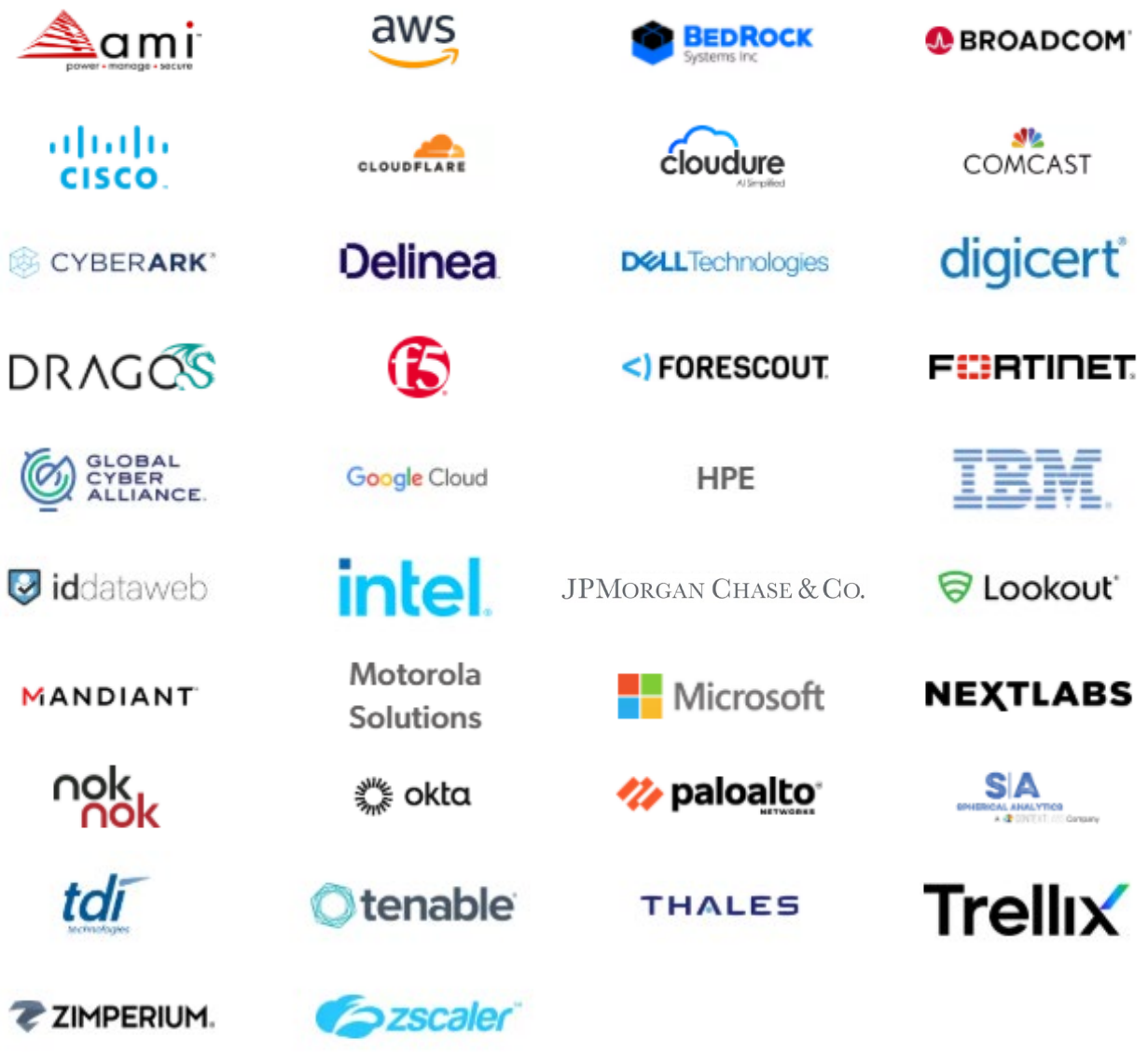
Have a Project Idea?

Contact us at nccoe@nist.gov.
Let's work together to accelerate cybersecurity innovation.

National Cybersecurity Excellence Partnership (NCEP) Partners

As part of our National Cybersecurity Excellence Partnership (NCEP) program, partners provide technical input to help the NCCoE address emerging cybersecurity challenges and trends, collaborate to identify new projects, and gain insights from the NCCoE's work.

The NCCoE's work is supported through active participation from our NCEP partners below.



Appendix: Project Collaborators

Formal collaborators on NCCoE projects sign a Cooperative Research and Development Agreement (CRADA) to provide hardware, software, and/or expertise to support a project. As of publishing, the NCCoE's projects are currently supported through the active participation from the project collaborators below.

Data Protection

Digital Identities through Mobile Driver's License (mDL)

- 1Password
- American Association of Motor Vehicle Administrators (AAMVA)
- Apple
- California Department of Motor Vehicles
- Capital One
- Department of Homeland Security (DHS), Science and Technology Directorate
- FAST Enterprises
- Georgia Department of Driver Services
- Google
- General Services Administration (GSA), Login.gov
- Idemia
- iLabs
- JP Morgan Chase
- Kentucky Transportation Cabinet
- Maryland Department of Transportation
- MATTR Limited
- Microsoft Corporation
- Navy Federal Credit Union
- New York State Department of Motor Vehicle
- Ohio Bureau of Motor Vehicles
- Okta
- OpenID Foundation
- PNC Bank
- Raymond James
- Scytales
- SpruceID
- Synchrony
- US Bank
- Wells Fargo
- Yubico

Migration to Post-Quantum Cryptography (PQC)

- Amazon Web Services, Inc. (AWS)
- ATIS
- AvInyaSQ
- Cisco
- Cloudflare
- Comcast
- Crypto4A Technologies, Inc.
- CryptoNext Security
- Cybersecurity and Infrastructure Security Agency (CISA)
- 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
- 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

Automation Support for the Cryptographic Module Validation Program (CMVP)

- Acumen Security
- AEGISOLVE
- Apple
- atsec
- AWS
- Cisco
- Cloudflare
- Katalyst
- Lightship Security
- Microsoft
- NXP Semiconductors
- SUSE

Trusted Enterprise

5G Security Testbed

- AMI
- AT&T
- CableLabs
- Cisco
- Dell Technologies
- Intel
- Keysight Technologies
- MiTAC
- Nokia
- Palo Alto Networks
- T-Mobile

Secure Software Development (DevSecOps)

- AMI
- Black Duck
- CyberArk
- Dell Technologies
- DigiCert
- Endor Labs
- GitLab
- Google
- IBM
- Microsoft
- NextLabs
- Palo Alto Networks
- Sagittal AI
- Scribe Security

Data Classification Practices

- ActiveNav
- Adobe
- GitLab
- Google
- IBM
- Janusnet
- JPMorgan Chase & Co.
- Quick Heal
- Thales Trusted Cyber Technologies
- Trellix
- Virtru

Resilient Embedded Systems

Manufacturing Response and Recovery

- Amazon Web Services
- Cisco
- Dragos
- Garland Technology
- Google
- GreenTec-USA
- Inductive Automation
- Qcor
- Rockwell Automation
- Siemens
- TDI Technologies
- Tenable

Water and Wastewater

- Asdwa – Association of State Drinking Water Administrators
- Bedrock Systems
- Cisco
- Cyber 2.0
- Denver Water
- Dragos
- I&C Secure
- Q-Net Security
- Radiflow
- Re-Wa
- StrongDM
- TDI Technologies
- US.ABB
- West Yost
- WSSC Water