NATIONAL CYBERSECURITY CENTER OF EXCELLENCE (NCCOE)

ORGANIZATIONAL SPECIFICS

Standards Organizations:	3GPP, IETF, NIST
Technical Committees:	https://www.nccoe.nist.gov/get-involved/collaborate-us-technical-contributions
Other Partnering Organizations:	The National Cybersecurity Excellence Partnership (NCEP) program
Government Organizations:	https://www.nccoe.nist.gov/get-involved/collaborate-us-government-organizations
Industry Sector(s) / Technology:	Sectors covering: Consumer Data Protection; Energy; Financial Services; Healthcare; Manufacturing; Public Safety/First Responder; Water/Wastewater Technology: 5G Cybersecurity; Applied Cryptography; Artificial Intelligence; Critical Cybersecurity Hygiene; Cybersecurity for the Space Domain; Data Classification; Data Security; DevSecOps; Digital Identities – mDL; Genomics Cybersecurity; Internet of Things (IoT); IPv6; Mobile Device Security; Supply Chain Assurance; Trusted Cloud; Zero Trust Architecture
Program / Activity Website URL(s):	https://www.nccoe.nist.gov/

STANDARDS DRIVEN PUBLIC-PRIVATE PARTNERSHIP (PPP) OBJECTIVES

PPP Drivers:

The National Cybersecurity Center of Excellence (NCCoE), run by the National Institute of Standards and Technology (NIST), brings together government agencies, industry organizations, and academic institutions to collaborate on cybersecurity challenges and protect the nation's critical infrastructure. The drivers for this partnership are both internal and external. NIST is often internally driven to seek new connections to understand the needs of industry, academia, or federal or local government communities within a specific program area. Information Technology Lab (ITL) has the broad mission to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology through research and development in information technology, mathematics, and statistics. Therefore, NCCoE fills a gap in a technical area while also being influenced by external drivers (e.g., congressional mandates) to initiate projects and partnerships. For example, NIST formed the NCCoE as a result of calls from other agencies, the intelligence community, and then-Senator Barbara Mikulski (D-MD) to "work to strengthen U.S. economic growth by supporting automated and trustworthy e-government and e-commerce."

PPP Goals:

The National Cybersecurity Center of Excellence (NCCoE) is a collaborative hub where industry organizations, government agencies, and academic institutions work together to address businesses' most pressing cybersecurity challenges. Through this collaboration, the NCCoE develops modular, easily adaptable example cybersecurity solutions using standards, best practices, and commercially available technology. The standards produced are known as the 1800 series.

NCCoE goals include:

1. **Provide practical cybersecurity:** help organizations secure their data and digital infrastructure by equipping them with practical ways to implement standards-based, cost-effective, repeatable, and scalable cybersecurity solutions
2. **Increase rate of adoption:** enable companies to rapidly adopt commercially available cybersecurity technologies by reducing their total cost of ownership
3. **Accelerate effective innovation:** empower innovators to creatively address businesses' most pressing cybersecurity challenges in a state-of-the-art, collaborative environment

Public Sector Role & Participation:

The primary leaders for the NCCoE are as follows:

- NIST/NCCoE: leadership role, convener, responsible for the outcomes
- The MITRE Corporation: federally funded research and development center (FFRDC) partner for the NCCoE; operates the NCCoE
- FFRDC: supports technical and operational activities

In addition, other groups are engaged in certain specifics including:

- Other government agencies: participate and often co-sponsor projects
- Private sector: both a benefactor of the solution and a developer via projects, or a partner through the National Cybersecurity Excellence Partnership
- Academia: students, faculty, researchers, and administrators from K-12 and higher education communities through the Academic Engagement Community of Interest

In addition to contributing to individual projects, the NCCoE forms long-term relationships with industry organizations through the National Cybersecurity Excellence Partnership (NCEP) program. As part of the NCEP program, industry organizations pledge to contribute physical infrastructure such as hardware and software components, intellectual knowledge including best practices and lessons learned, or guest researchers to work side by side with federal staff in NCCoE's test environments. NCEP organizations are accepted based on the feasibility of their proposed collaboration with NCCoE, their relevance to NCCoE's strategy, and the potential to advance cybersecurity through their partnership. Qualified companies are invited to join a memorandum of understanding (MOU) with NIST and NCCoE.

Implementation Methods:

FFRDCs are public-private partnerships that are established to meet special long-term research or development needs that cannot be met as effectively by existing in-house or contractor resources. FFRDCs are a major endeavor for NIST to initiate, requiring significant implementation time and effort. However, FFRDCs can be well worth the initial implementation effort—more than paying for their investment in terms of quality outputs and deep partnership growth over time. NIST's only FFRDC (NCCoE) continues to achieve success year after year. Working with its FFRDC partner the MITRE Corporation, NIST engages with the larger cybersecurity community through the NCCoE, including specific sectors like transportation, energy, and healthcare, on a scale it would not be able to otherwise.

Each NCCoE project is led by a NIST Principal Investigator (PI). The PI provides oversight for the development of the project and manages a team of subject matter experts and the FFRDC operational support. NCCoE uses a phased approach:

1. NCCoE works with industry to generate a technical description and scope of work for addressing a pressing cybersecurity challenge. During this phase, NCCoE solicits public comment on the draft project description to ensure that the project will be as broadly applicable as possible. At the end of this phase, NCCoE publishes a final version of the scope of work that outlines the cybersecurity challenge and a draft architecture on its website.
2. NCCoE assembles a team of industry organizations, government agencies, and academic institutions to address the scope of work. NCCoE releases a Federal Register Notice (FRN) that announces the collaboration opportunity and defines the desired capabilities of the team members. Potential team members are invited to respond to the FRN with a Letter of Interest (LOI). NCCoE accepts LOIs on a first-come basis. Collaborators that join the build team sign a Cooperative Research and Development Agreement (CRADA) with NCCoE to provide commercially available products and expertise to the project.
3. NCCoE team builds a practical, usable, repeatable solution to address the cybersecurity challenge outlined in the statement of work. Industry collaborators provide support to install and configure their technologies. They also provide support throughout the build to address issues such as interoperability. As part of the development, the reference architecture is finalized. NCCoE documents the example solutions in the NIST Special Publication 1800 series, which maps capabilities to the NIST Cyber Security Framework and details the steps needed for another entity to recreate the example solution.

NCCoE also hosts several communities of interest (COIs) through which public- and private-sector organizations share business insights, technical expertise, challenges, and perspectives. NCCoE relies on the COIs to identify and define problems that NCCoE should address. Anyone is welcome to sign up for a COI.

Measurement of Success:

NCCoE has successfully produced many cybersecurity solutions over the past decade. NCCoE attributes its success in creating practical cybersecurity solutions to three key elements: collaboration, documentation, advocacy and education. NCCoE ensures each of these elements is present in every phase of its projects by:

- Engaging in regular, robust collaboration with experts and innovators from various sectors in addition to the broader technology community to help identify and address businesses' most pressing cybersecurity challenges;
- Documenting its work across media such as the NIST Special Publication 1800 series, industry-specific cybersecurity papers, technical notes, videos, and interactive guides, as well as mapping capabilities to the NIST Cybersecurity Framework and detailing the steps needed for another entity to recreate example solutions in part or in full; and
- Promoting what it does and how it does it, and teaching others ways to improve their cybersecurity posture.

Since its inception, the NCCoE has established over 500 collaborations through Cooperative Research and Development Agreements (CRADAs), NCEPs, academic affiliates, and interagency agreements. Each NCCoE project resulting in publication generally serves as a "how to" guide that demonstrates how to implement and apply standards-based cybersecurity technologies in the real world. The guides are designed to help organizations gain efficiencies in implementing cybersecurity technologies, while saving them research and proof of concept costs. Some specific examples include among others:

- The 3G Partnership Project (3GPP) specifications cover cellular telecommunications technologies (e.g., radio access, core network and service capabilities). NIST extended 3GPP's standards security protections to 5G networks supporting components for secure deployments.
- NIST's NCCoE Applied Cryptography program bridges the gap between development of fundamental cryptographic algorithms and their use in commercial off-the-shelf technology. NIST has been soliciting, evaluating, and standardizing quantum-resistant public-key cryptographic algorithms. To complement this effort, the NCCoE is engaging with industry collaborators and regulated industry sectors and the U.S. Federal Government to bring awareness to the issues involved in migrating to post-quantum algorithms and to prepare the crypto community for migration.
- NCCoE has produced a practice guide to demonstrate the practicality and effectiveness of using the Internet Engineering Task Force's (IETF) Manufacturer Usage Description (MUD) standard to strengthen security for IoT devices on home and small-business networks. This guide demonstrates how organizations can use MUD to reduce the vulnerability of IoT devices to network-based threats such as distributed denial of service attacks (DDoS) and mitigate the potential for harm resulting from exploitation of IoT devices.
- NIST's NCCoE analyzed risk factors in and around the infusion pump ecosystem by using a questionnaire-based risk assessment. With the results of that assessment, the NCCoE then developed an example implementation that demonstrates how healthcare delivery organizations can use standards-based, commercially available cybersecurity technologies to better protect the infusion pump ecosystem, including patient information and drug library dosing limits.

Key Takeaways:

Partnerships that were proactive and timely in nature have been successful. Lending NIST expertise to areas of critical national importance such as cybersecurity. For NCCoE, the timeliness of the partnership has meant that the FFRDC continues to have strong support for collaboration and involvement from/with other entities, even more than the partnership can support at any one time, allowing the partnership to grow and continue to be in demand. This allows NIST to consistently collaborate, develop deeper relationships with partners, and keep the partnership going indefinitely.

Advice for Others:

Measures of success depend on the PPP's purpose and goals. In addition to quantifying factors, qualifying measures including economic and social returns such as technology innovation, education, creation of new businesses, jobs, and social well-being should be considered. Strategic investments and financial sustainability, or the degree of sufficiency for federal funds should be another factor to consider. The long-term needs of the infrastructure should be considered as part of the PPP's funding model.

Last updated September 2024. This use case was developed as part of an ANSI project performed under the following financial assistance award 70NANB24H075 from U.S. Department of Commerce, National Institute of Standards and Technology.