NCCoE
NATIONAL CYBERSECURITY
CENTER OF EXCELLENCE

About the National Cybersecurity Center of Excellence

The National Cybersecurity Center of Excellence (NCCoE) turns standards and best practices into practical solutions to address some of the nation's most intractable cybersecurity challenges.

- As a key component of the National Institute of Standards and Technology's (NIST) cybersecurity program, the center collaborates with experts from industry, academia, and government to identify common problems. Then, using commercially available products, the NCCoE and its partners create and promote real-world cybersecurity solutions in the form of practical, technical guides.
- The NCCoE currently has 22 core partners, from Fortune 50 market leaders to smaller companies specializing in IT security, that have pledged to support the center with hardware, software and expertise. For an up-to-date list, see https://nccoe.nist.gov/partners.
- NIST, with the active support of the state of Maryland and Montgomery County, Md., established the center in 2012.
- In October 2014, NIST established the country's first Federally Funded Research and Development Center (FFRDC) dedicated to cybersecurity to support the NCCoE mission. The FFRDC functions as the only national laboratory dedicated solely to cybersecurity, providing research, development, technology and engineering expertise in support of NIST and the rest of the federal government. The FFRDC also provides access to expertise across the University of Maryland system and nine other university affiliates around the country.

The NCCoE

- **Is a valuable resource for companies and agencies—both those with security technologies and those needing new or improved security capabilities;**
- **Strengthens the security of the nation's businesses, improving the overall security of the economy; and**
- **Empowers innovators to creatively address businesses' most pressing cybersecurity challenges in a state-of-the-art, collaborative environment.**

https://nccoe.nist.gov/
nccoe@nist.gov

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

MONTGOMERY COUNTY MARYLAND 17 76

Maryland
DEPARTMENT OF COMMERCE

Approach

- The NCCoE collaborates with industry, including critical infrastructure sectors, to identify specific technical cybersecurity problems that affect entire industry sectors or reach across sectors.
- The NCCoE then identifies applicable standards and best practices and collaborates with the creators of commercial off-the-shelf products to use them in developing example solutions. Specialists at other government agencies and academia also participate in, and sometimes sponsor, these projects.
- The NCCoE publishes NIST Cybersecurity Practice Guides that show businesses how to put these example solutions into practice for themselves in ways that align with relevant standards and best practices.

Results

- With its first technology partner signing in April 2013, the center has spurred collaboration with and among large and small companies from multiple sectors—including health care, energy, financial services, retail, restaurants and hospitality.
- Federal agencies also have engaged the help of NCCoE, including the Department of Homeland Security, General Services Agency, U.S. Coast Guard and others.

SOME EXAMPLES OF NCCoE PROJECTS:

- Health care providers increasingly are using mobile devices to collect, access, process and transmit patient information. The NCCoE health care project, Securing Electronic Health Records on Mobile Devices, provides guidance for health care organizations seeking to improve the security of these ubiquitous devices.
- For electric utilities, the convergence of information technology with operational technology such as industrial control and Supervisory Control and Data Acquisition (SCADA) system, has created vulnerabilities that could affect the stability of the electric power grid. The NCCoE energy sector project, Identity and Access Management for Electric Utilities, provides guidance on converged access control capabilities to help secure this part of the critical infrastructure.
- Users of cloud services often don't know and can't control where their data resides. This is a problem for organizations and individuals that store and process sensitive information in the cloud. The NCCoE Trusted Geolocation in the Cloud project demonstrates the ability to restrict movement of users' data when using a cloud provider.
- The NCCoE Mobile Device Security project provides guidance to small- and medium-sized businesses on the implementation of capabilities to secure sensitive business data residing in the cloud and being accessed by employees on mobile devices.
- Financial services organizations have a wide array of information technology equipment, including data centers, work stations, mobile devices and mainframes. The first step in securing these assets is to identify who owns them, what operating systems and applications are running on them, and the status of any critical updates or patches. The NCCoE project for the financial services sector, IT Asset Management, provides guidance on implementing enterprise asset management capabilities.
- Many organizations struggle to ensure that users are able to access only the appropriate resources and systems. Another NCCoE project provides

them with the guidance they need to take advantage of Attribute Based Access Control capabilities—an advanced method to give access that also reduces the management overhead and the cost of managing identity and access management systems.

- NCCoE is working with the retail community to better protect information related to consumer transactions. This project to address improved security within and across the payment ecosystem will be discussed at a March 2016 workshop.
- The NCCoE project on DNS-Based Secured Email leverages recent developments in securing fundamental components of the Internet to increase the trustworthiness of email.

More about NCCoE's Facilities

- The NCCoE now has almost 5,600 square meters (60,000 square feet) of modern physical space and the information technology systems needed to host its staff and partners who work jointly on a variety of projects in its collaborative environment. This includes the space to house experts from the National Cybersecurity FFRDC, operated by The MITRE Corporation with active participation by the University of Maryland System.
- The new facility expands the center's workspace from four to 22 separate, flexible laboratories. That includes two larger areas capable of safely hosting large equipment—including a vehicle that will be used in an upcoming project on auto-related cybersecurity issues. This additional space now allows NCCoE to increase its collaborations and to undertake new projects.
- After being temporarily housed on the Shady Grove campus of the University of Maryland, NIST worked with the state of Maryland and Montgomery County, Md., to identify and procure a permanent facility for the center. Each contributed $4.5 million toward necessary renovations to the facility, in addition to $4 million from NIST. NIST has a 10-year license to use the facility for the NCCoE's mission.

Federal Agencies

- The Department of Homeland Security has entered into an interagency agreement with NIST to support initiatives identified in the administration's Cybersecurity Strategy Implementation Plan (CSIP). This collaboration will assist federal agencies in more effectively and efficiently implementing continuous monitoring on their systems.
- The NCCoE is also collaborating with the General Services Administration on research that is leading to new methods and mechanisms for supply chain security. With the active involvement of the University of Maryland, this work will have a significant impact on the cybersecurity of products and services that government and private-sector organizations purchase.

OTHER NCCoE COLLABORATIVE ACTIVITIES WITH FEDERAL AGENCIES INCLUDE:

- Assistance to the U.S. Coast Guard, working with the American Petroleum Institute, in applying the NIST Cybersecurity Framework to bulk liquid transport activities under its authority.
- Taking advantage of the expertise of National Security Agency staff who have participated in NCCoE projects.

Technology Providers