

## THE CENTER GUIDES BUSINESSES TO STRONGER CYBERSECURITY PRACTICES.

The National Cybersecurity Center of Excellence (NCCoE) at the National Institute of Standards and Technology addresses businesses' most pressing cybersecurity problems with practical, standards-based solutions using commercially available technologies. The NCCoE collaborates with experts from industry, government and academia to build modular, open, end-to-end reference designs that are broadly applicable and repeatable.

## GET INVOLVED

Interested in contributing to the development of secure, standards-based technologies? We partner with members of industry, government and academia to demonstrate cybersecurity capabilities using commercially available technologies.

## LEARN MORE

Visit <http://nccoe.nist.gov>

## CONTACT US

Email: [nccoe@nist.gov](mailto:nccoe@nist.gov)

Telephone: 240-314-6800

## VISIT US

Arrange a visit to our state-of-the-art facility in the heart of Maryland's technology corridor.



National Cybersecurity Center of Excellence  
National Institute of Standards and Technology  
9600 Gudelsky Drive  
Rockville, MD 20850

# NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

Accelerating the deployment  
and use of secure,  
standards-based technologies





ACCELERATING THE DEPLOYMENT AND USE OF SECURE, STANDARDS-BASED TECHNOLOGIES

**OUR STRATEGY:** DRIVEN BY THE CYBERSECURITY NEEDS OF AMERICAN BUSINESSES

**VISION**

ADVANCE CYBERSECURITY

A secure cyber infrastructure that inspires technological innovation and fosters economic growth

**MISSION**

ACCELERATE ADOPTION OF SECURE TECHNOLOGIES

Collaborate with innovators to provide real-world, standards-based cybersecurity capabilities that address business needs

**GOALS**

PROVIDE PRACTICAL CYBERSECURITY

Help people secure their data and digital infrastructure by equipping them with practical ways to implement standards-based cybersecurity solutions that are modular, repeatable and scalable

INCREASE RATE OF ADOPTION

Enable companies to rapidly deploy commercially available cybersecurity technologies by reducing technological, educational and economic barriers to adoption

ACCELERATE INNOVATION

Empower innovators to creatively address businesses' most pressing cybersecurity challenges in a state-of-the-art, collaborative environment

**OUR COMMITMENT:** ADVANCE CYBERSECURITY THROUGH APPLIED STANDARDS AND TECHNOLOGIES

**ACCELERATED RESULTS**

Established in 2012 through a partnership among NIST, the State of Maryland and Montgomery County, the NCCoE meets businesses' most pressing cybersecurity needs with reference designs that can be deployed rapidly.

**NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY**

The NCCoE is part of the NIST Information Technology Laboratory and operates in close collaboration with the Computer Security Division. As a part of the NIST family, the center has access to a foundation of prodigious expertise, resources, relationships and experience. NIST is a recognized thought leader in:

- » cryptography
- » hardware roots of trust
- » identity management
- » key management
- » risk management
- » secure networking
- » secure virtualization
- » security automation
- » security for cloud and mobility
- » software assurance
- » usability and security
- » vulnerability management

**OUR APPROACH:** REDUCE BARRIERS TO ADOPTION OF SECURE TECHNOLOGIES

**BUSINESS MODEL**

The NCCoE uses commercially available technologies as modules in end-to-end solutions that can be rapidly applied to the real challenges that businesses face each day. The center has a four-step process:

1. work with members of industry sectors to define cybersecurity problems
2. assemble teams of experts from industry, government and academia
3. build practical reference designs—based on commercially available technologies—that are usable, repeatable and secure
4. facilitate rapid, widespread adoption and use of secure technologies through practice guides, which include all of the material and information needed to deploy a reference design

**BENEFITS**

Cybersecurity solutions that are:

- » based on standards and best practices
- » usable, repeatable and can be adopted rapidly
- » modular, end-to-end and commercially available
- » developed using open and transparent processes
- » matched to specific business needs and bridge technology gaps