Welcome to the NCCoE
RESOURCES FOR GROWING CYBERSECURITY COMPANIES IN MD
November 25, 2013
STRATEGIC PLAN

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 cybersecurity capabilities that address business needs

GOAL 1
Provide Practical Cybersecurity
Help people secure their data and digital infrastructure by equipping them with practical ways to implement cost-effective, repeatable and scalable cybersecurity solutions

GOAL 2
Increase Rate of Adoption
Enable companies to rapidly adopt commercially available cybersecurity technologies by reducing their total cost of ownership

GOAL 3
Accelerate Effective Innovation
Empower innovators to creatively address businesses’ most pressing cybersecurity challenges in a state-of-the-art, collaborative environment
PARTNERSHIPS

Established in 2012 through a partnership among NIST, the State of Maryland and Montgomery County, the NCCoE is dedicated to furthering innovation through the rapid identification, integration and adoption of practical cybersecurity solutions.

NIST ITL

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 strong foundation of expertise, resources, relationships and experience.

ITL THOUGHT LEADERSHIP

- Cryptography
- Identity management
- Key management
- Risk management
- Secure virtualization
- Software assurance
- Security automation
- Security for cloud and mobility
- Trusted roots of hardware
- Vulnerability management
- Secure networking
- Usability and security
Open & Transparent
Use open and transparent processes to complete work, and seek and incorporate public comments on NCCoE documentation, artifacts and results

Standards-Based
Apply relevant local, national and international standards on each security implementation and account for each sector's individual needs; demonstrate example implementations for new and emerging standards

Modular
Develop example implementations that rely on individual components which can be easily substituted with alternative commercially available components that offer equivalent input-output specifications

Usable
Design usable blueprints that end users can easily and cost-effectively adopt and integrate into their business without disrupting day-to-day operations

Repeatable
Enable end users to recreate NCCoE example implementations by increasing their awareness of commercially available components and equipping them with supporting information in methodological detail
OUTCOMES

Rapid adoption
of cybersecurity solutions that are usable, repeatable and secure

Practical cybersecurity solutions
that match specific business needs and bridge technology gaps

Cost-effective cybersecurity solutions
that are open, standards-based, modular, end-to-end and built on commercially available technologies

Accessible innovation test beds
with commercially available technologies and leading cyber technologists

Evidence-based collaboration
with leading experts from U.S. companies, universities, and NIST and other government agencies

Compliant cybersecurity solutions
that help businesses more easily follow relevant standards and regulations
USE CASES

Energy
- Identity and Access Management
- Situational Awareness

Financial Services
- Identity and Access Management
- IT Asset Management

Health IT
- Mobile Devices
Authenticated Email

Trusted Geolocation in the Cloud

Continuous Monitoring

Mobile Device Integrity
CENTER'S NEXT STEPS

Further use cases and building blocks in collaboration with cybersecurity community

YOUR NEXT STEPS

Contact us to explore opportunities to collaborate

Contact Us
nccoe@nist.gov
240.314.6800
http://nccoe.nist.gov