NATIONAL CYBERSECURITY CENTER OF EXCELLENCE MISSION:

Enable the adoption, identification, and use of cybersecurity solutions to meet business needs.

HOW TO PARTICIPATE/LEARN MORE

The NCCoE is seeking partners from industry, government, academia, and the nonprofit sectors. For further information and announcements, visit nccoe.nist.gov, email nccoe@nist.gov, or call (301) 975-4500.

National Cybersecurity Center of Excellence (NCCoE)
9600 Gudelsky Drive
Rockville, Md. 20850

NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

ADVANCING CYBERSECURITY, ENHANCING ECONOMIC GROWTH

Cover (color image):
Studies by NIST, industry, academic, and other collaborators at the NCCoE are expected to address a wide range of cybersecurity needs including ways to reduce vulnerabilities in virtualized and cloud computing environments.

June 2012

NCCoE NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

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

The National Cybersecurity Center of Excellence (NCCoE) is a public-private collaboration that will bring together experts from industry, government, and academia to design, implement, test, and demonstrate integrated cybersecurity solutions and promote their widespread adoption. Participants will develop practical, interoperable cybersecurity approaches that address the real-world needs of complex information technology (IT) systems.

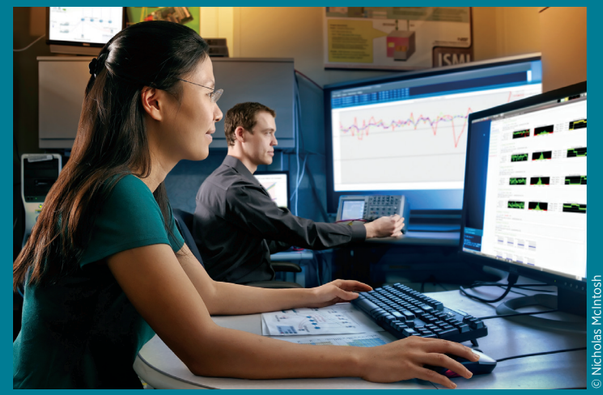
Through research, development, and deployment acceleration efforts, the center will:

- enhance trust in U.S. IT communications, data, and storage systems;
- lower risk for companies and individuals using IT systems; and
- encourage development of innovative, job-creating cybersecurity products and services.

The center is hosted by the U.S. Commerce Department's National Institute of Standards and Technology (NIST) in collaboration with the State of Maryland and Montgomery County, Md.

IT is central to financial, communications, health care, and physical infrastructures and even entertainment systems. It is also under constant attack by cybercriminals looking to steal business data, personal information, and devices, or disrupt private and government business with malicious code, denial of service and Web-based attacks.

The NCCoE provides a state-of-the-art computing facility where researchers from NIST can work collaboratively with both the users and vendors of products and services on holistic cybersecurity approaches. Center projects will demonstrate cybersecurity principles and practices that are feasible for businesses and measure them against standards.



© Nicholas McIntosh

NIST computer scientists work on an IT research project related to ensuring reliability of the planned nationwide smart electric power grid. Strong cybersecurity systems are vital to protecting everything from the power grid to corporate intellectual property to consumers' financial information.

By providing a test bed where new ideas and technologies can be tried out before being deployed, the center provides the opportunity to thoroughly document and share each solution, supporting specific industry sector business challenges. This will encourage the rapid adoption of comprehensive cybersecurity templates and approaches that support automated and trustworthy e-government and e-commerce.

KEY CENTER GOALS:

- Disseminate applied principles and mechanics underlying security standards, metrics, and best practices for secure and privacy-preserving information technologies
- Develop implementation templates for composing, monitoring, and measuring the security posture of computer and enterprise systems
- Achieve broad adoption of practical, affordable, and useful cybersecurity capabilities across the full range of commercial and government sectors

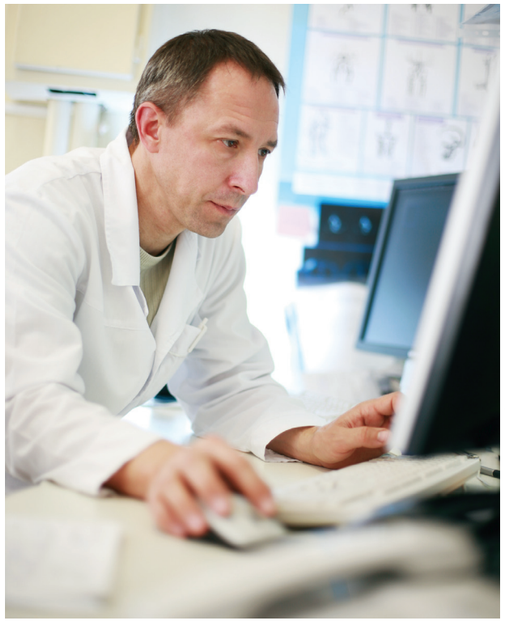
A NEW MODEL FOR PARTNERSHIPS

For many organizations that require complex IT systems—hospitals, government agencies, manufacturers, etc.—cybersecurity can be a black box. These organizations often do not have the in-house IT technical expertise to address the full range of their cybersecurity needs or to determine the best path to cost-effective solutions.

Cybersecurity vendors and broader community of IT vendors do their best to meet their clients' requirements. However, the segmented nature of the marketplace means many cybersecurity tools are applied in a piecemeal way, and as a result, vulnerabilities can occur that are not known to either the user organization or its vendors.

The center will undertake carefully developed use cases and associated technology implementations for the proposed solutions to resolve cybersecurity challenges. This approach will lead to integrated security templates, including appropriate technologies, tools, policies, and practices to create a trustworthy cybersecurity environment. Collaborators will define innovation gaps by documenting and sharing use case results.

Integrated cybersecurity techniques and technologies to be developed at the NCCoE may be used to help protect the privacy of patients' medical files as health care providers increasingly adopt use of electronic records.



© Konstantin Sutyagin/Shutterstock

HOW THE CENTER WILL WORK

In fiscal year 2012, NIST received $10 million in funding to establish a private-public partnership to operate the center. The center will host multi-institutional, collaborative efforts that individual member organizations do not have the expertise or resources to conduct alone. Results from center projects will be shared with the broad IT user and vendor communities.

The NCCoE mission will be pursued through public-private-sector teams and projects that promote frequent and direct interaction among experts in a collaborative environment. Team members will work together to identify objectives and create opportunities for collaborative leadership among technology and business communities.

> **"Cybercrime hurts individuals, businesses, and government agencies. We want to bring together the best minds and provide them with the best tools to create and test solutions."**
>
> *Under Secretary of Commerce for Standards and Technology and NIST Director Patrick Gallagher, February 2012*

The use cases will represent complex cybersecurity business challenges that require an integrated solution and have clear benefits for one or more particular industry sectors. For example, initial use cases could include:

- health IT solutions that use open interface standards to encourage interoperability, flexibility, and competition, while allowing wide broadband remote access and high levels of privacy and security;
- cloud computing solutions that provide strong methods for knowing the physical location of sensitive data and for monitoring and verifying permissions for data movement among cloud servers; and
- mobile computing solutions that provide trusted ways for organizations to communicate with their employees on their personally owned devices and yet protect that data if the device is lost or stolen or if the employee no longer works for the organization.

Use cases will be selected and refined through workshops and input from broad groups of stakeholders, as well as public feedback. Applicable standards and guidelines will be identified and interested IT vendors involved through open calls for participation.

The center will conduct a variety of interactive sessions intended to disseminate technical information and foster technical discussions. Examples of these sessions include Deep Dive Days, which explore a particular technical topic related to one or more center projects related to cryptography, continuous monitoring, identification, authentication, and authorization; technical discussions on academic research topics; and sessions that provide step-by-step, hands-on training on implementing center guidelines, standards, etc., in a test environment.

© Nicholas McIntosh

The NCCoE will identify complex cybersecurity challenges or "use cases" in areas such as mobile computing and then work with interested partners to design and demonstrate possible solutions.

WHY NIST?

Through its Information Technology Laboratory (ITL) and ITL's Computer Security Division, NIST plays a vital role in the development of standards, guidance, tests, and metrics related to security management and assurance, cryptography and systems security, identity management, and emerging security technology. NIST contributes to national and international standards setting and provides leadership in the development of technologies and standards for cloud computing, identity management, and as a government-wide leader and national coordinator for the National Initiative for Cybersecurity Education (NICE).

Extensive collaboration with government, industry, privacy advocates, nonprofit organizations, and many other stakeholder groups is an essential part of NIST's research and other activities.