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, non-profit organizations, and many other stakeholder groups is an essential part of NIST's research and other activities.

NATIONAL CYBERSECURITY CENTER OF EXCELLENCE MISSION:

Strengthening U.S. economic growth by accelerating adoption of integrated cybersecurity tools and techniques that promote automated and trustworthy e-government and e-commerce.

HOW TO PARTICIPATE/LEARN MORE

The center is now actively seeking partners from industry, government, academia, and the non-profit sectors. For further information and announcements, visit nccoe.nist.gov, email nccoe@nist.gov, or call 301 975-4500.

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.

February 2012

NATIONAL CYBERSECURITY CENTER OF EXCELLENCE

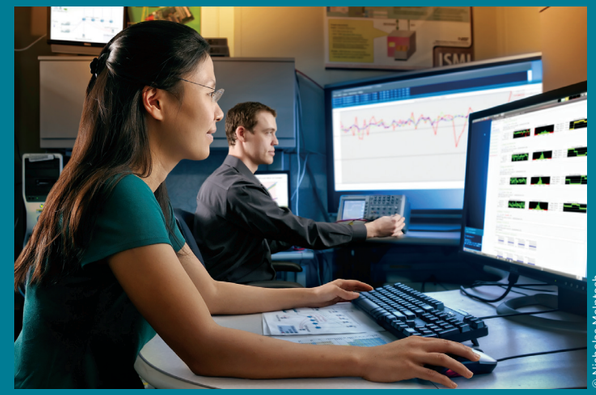
ADVANCING CYBERSECURITY, ENHANCING ECONOMIC GROWTH

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

The National Cybersecurity Center of Excellence (NCCoE) is a public-private collaboration for accelerating the widespread adoption of integrated cybersecurity tools and technologies. The center brings together experts from industry, government, and academia under one roof to develop practical, interoperable cybersecurity approaches that address the real world needs of complex information technology (IT) systems. By accelerating dissemination and use of these integrated tools and technologies for protecting IT assets, the center:

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

Expected to be located near Gaithersburg, Md., 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.



© 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.

BETTER PROTECTION EQUALS BETTER BUSINESS

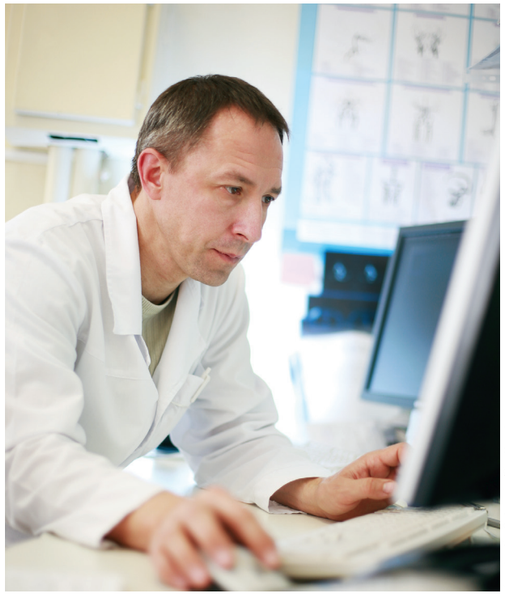
IT is pervasive. It's central to our financial, communications, health care, and physical infrastructures and even our entertainment systems. Unfortunately, it is also routinely attacked—too often successfully.

Cybersecurity—methods for protecting IT assets—is critical for protecting everything from an individual's private information to corporate data that is the backbone of business.

Online commerce, for example, is an essential and growing segment of the U.S. economy. A recent report by an industry research group projects total e-commerce sales to grow by 7 to 8 percent per year, reaching about $250 billion by 2014. Online sales allow both entrepreneurs and established businesses quick, low-cost access to potentially millions of customers, which can encourage innovation and create new jobs.

The Internet also offers business substantial efficiencies by allowing easy communications between business partners and with remote locations to collaborate on products, telecommuting options for employees, and other benefits.

This tremendous increase in online business transactions, however, gives cyber criminals greater access to business assets than ever before, opening up risks for intellectual property theft, identity theft, and other crimes. It is difficult to quantify the full cost of cyber crime, especially since many incidents are not reported. However, according to a study released by Symantec in 2011, global cybercrime costs a total of $388 billion in both direct financial losses and the value of lost time dealing with cyber crime effects. From September 2010 to September 2011, the study found that 431 million adults were victims of cyber crime and estimated that 69 percent of all adults experience cyber crime in their lifetimes.



© Konstantin Sutyagin/Shutterstock

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.

A study by the Ponemon Institute published in August 2011 found that cyber crime costs averaged about $5.9 million per year for U.S. companies with more than 700 IT users. The study was based on detailed information from 50 representative companies in various industry sectors. The 50 companies in the study experienced a total of 72 successful attacks per week, an increase of 44 percent over the previous year. The most costly cyber crimes were caused by malicious code, denial of service, stolen devices, and web-based attacks.

It is clear that businesses and individuals suffer substantial losses from cyber crime and have much to gain from broader adoption and deployment of strong cybersecurity tools and techniques and from sharing lessons learned across different industry sectors.

A NEW MODEL FOR PARTNERSHIPS

By providing a testbed where new ideas and technologies can be tried out before being deployed, the National Cybersecurity Center of Excellence encourages the rapid adoption of comprehensive cybersecurity templates and approaches that support automated and trustworthy e-government and e-commerce.

For many organizations that require complex IT systems—hospitals, government agencies, manufacturers, etc.—cybersecurity is a black box. Organizations buy systems and do their best to protect their assets, but they often do not have the inhouse IT technical expertise needed to address the full range of cybersecurity needs or to determine the best path to cost-effective solutions.

Cybersecurity vendors and broader 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 NCCoE will provide a state-of-the-art computing facility and researchers from the NIST to work collaboratively with both the users and vendors of products and services on holistic cybersecurity approaches. The center will undertake carefully developed use cases—comprehensive tests for proposed solutions to specific cybersecurity challenges—that will lead to integrated security templates including appropriate technologies, tools, policies, and practices to create a trustworthy cybersecurity environment.

The improved trust in cyberspace resulting from the center's efforts will support the development and adoption of innovative business methods that improve operational efficiency, reap significant financial benefits for public- and private-sector institutions, promote entrepreneurship, and create new employment and career opportunities.

KEY CENTER GOALS:

- Disseminate new principles and mechanics underlying security standards, metrics, and best practices for secure and privacy-preserving information technologies
- Develop and test methods 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

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.

Each project will start with a specific identified "use case," a complex cybersecurity challenge that requires an integrated solution and has 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; or
- 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.

By hosting workshops and gathering inputs from broad groups of stakeholders, the center will:

- select specific use cases and determine requirements for possible cybersecurity solutions;
- refine each use case based on public feedback, identify applicable standards and guidelines, and place an open call for participation by interested IT vendors;
- provide office space, basic hardware, and infrastructure components;
- work with users, vendors, and NIST experts to design, implement, test, and demonstrate possible solutions;

© 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.

- deploy and test the solution in a testbed environment; and
- document and share each solution with the detail needed so that others can reproduce it.

Additional center projects may center on cryptography; continuous monitoring; identification, authentication, and authorization in public-private sectors; or cybersecurity curriculum development.