CYBERSECURITY AT NIST

BY THE NUMBERS

$262 billion

Value of e-commerce transactions in the United States in 2013
(Forrester)

$445 billion

Estimated cost to the global economy from cybercrime
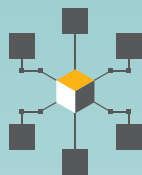*(McAfee)*

800 million

Estimated number of individual's records compromised in 2013
(Risk Based Security)

3,000+

Representatives from industry, government, and other partners worked with NIST to develop the Framework for Improving Critical Infrastructure Cybersecurity.

The Challenge

U.S. and global economies depend on information and communications technologies to facilitate commerce, government, and innovation. Today's computing environment includes constant growth in the amount of digital information and number of interconnected devices, as well as a rapidly evolving threat environment that exploits increased complexity and connectivity. These factors place the nation's security, economy, and public safety and health at risk and create the need for cybersecurity standards, technologies, and best practices that address interoperability, usability, and privacy. We must ensure that public and private organizations, large and small, understand their cybersecurity risks and have the standards and technologies necessary to best protect themselves.

What NIST Does

NIST plays a critical role in protecting our individual, corporate, and public-sector data, information, and systems from attacks by individual actors, criminal organizations, and nation-states. NIST's cybersecurity activities range from conducting fundamental research such as improved techniques for measuring elements of security to disseminating the results of that research in many forms.

- Develops and reviews standards and coordinates the development of large sets of standards to protect IT systems.

- Writes guidelines that help government and private organizations secure their IT.

- Develops tools, procedures, and test environments for evaluating cybersecurity technologies and the security of emerging information technologies.

- Establishes validation programs to confirm standards are properly implemented in IT products and services.

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

Recent Program Highlights

- Coordinated the development of a standards-based cybersecurity framework, providing a structure that organizations, regulators, and customers can use to assess and strengthen their cybersecurity programs.

- Launched the National Cybersecurity Center of Excellence (NCCoE), which provides businesses with real-world cybersecurity solutions based on commercially available technologies.

- Initiated the Privacy Engineering Initiative to develop guidance for information system users, owners, developers, and designers handling personal information.

- Published more than 40 different standards and guidelines to help protect non-national security IT systems from cyber threats.

Budget
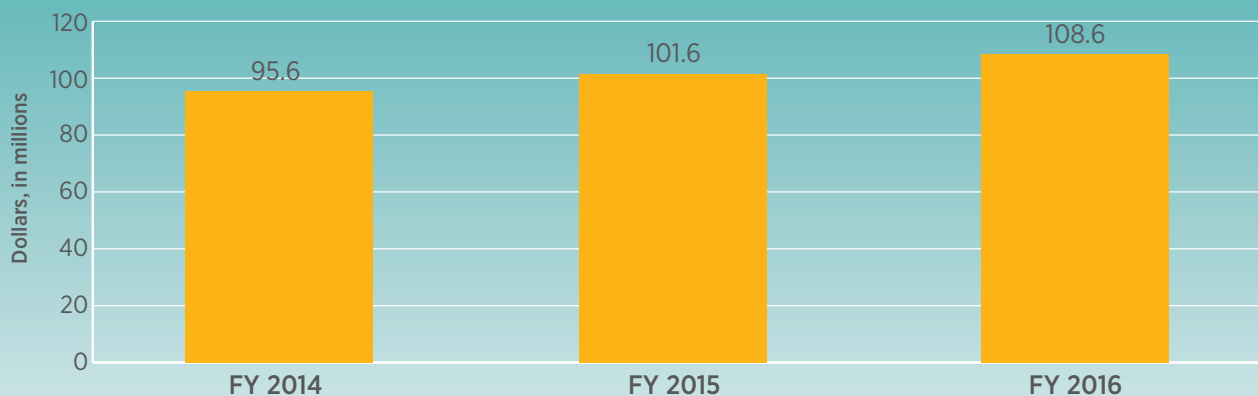
The FY 2016 total includes $4.4 million for the National Initiative for Cybersecurity Education, $15 million for the National Cybersecurity Center of Excellence, $16.5 for the National Strategy for Trusted Identities in Cyberspace, and $72.7 million for cybersecurity research and development.

New in FY 2016

NIST requested an increase of $7 million and 10 new full-time employees to strengthen the nation's cybersecurity posture by providing strong cryptographic solutions, and for the development of privacy-enhancing solutions and tools.

With the requested funds, NIST will focus on:

- Ensuring the continued delivery of robust and independent cryptography capabilities, including

  - Expanding NIST's cryptographic team;

  - Expanding collaborations with academia and industry;

  - Research and development programs to incorporate new cryptographic capabilities in areas such as cryptography for constrained environments, quantum-resistant cryptography, and cryptography in support of privacy; and

  - Developing and promulgating standards, guidelines, tests, and measurements to support a post-quantum computing market.

- Developing the tools and standards necessary to assess and manage privacy risks.