Testimony of

Cita M. Furlani
Acting Director
Information Technology Laboratory

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

before the

Subcommittee on Regulatory Reform and Oversight
Committee on Small Business
U.S. House of Representatives

"The State of Small Business Security in a Cyber Economy"

March 16, 2006

Introduction

Chairman Akin, members of the Subcommittee, I am Cita Furlani, Acting Director of the Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST), part of the Commerce Department's Technology Administration. Thank you for this opportunity to testify today on our perspective regarding the "State of Small Business Security in a Cyber Economy." We recognize that small businesses play an important role in the U.S. economy. Since use of the Internet is critical in the delivery of goods and services for all businesses, the importance of addressing risks associated with doing business in a cyber environment cannot be overstated. Today I will focus my testimony on NIST's cyber security programs and activities that can assist small businesses.

NIST has long worked effectively with industry and federal agencies to help protect the confidentiality, integrity, and availability of information systems. Ensuring that business-related information is secure is essential to the functioning of our economy -- and indeed to our democracy. Our broader work in the areas of information security, trusted networks, and software quality is applicable to a wide variety of users – from small and medium enterprises to large private and public organizations including agencies of the federal government.

I will share the initiatives NIST has taken to increase the level of awareness and security best practices among small businesses. Small businesses, like all organizations, want to embrace and have available the latest advances in technology to make their tasks easier, improve productivity, and remain competitive. But they face an enormous challenge in protecting their information in a cyber environment.

Since nearly 99 percent of all U.S. businesses are small or medium-sized[1], a vulnerability common to a large percentage of these organizations could pose a significant threat to the Nation's economy and overall security. Many of these businesses house very sensitive personal information including healthcare or financial information. Many small businesses also provide services to our federal, state, local and tribal governments and have access to government information or systems. In the interconnected environment in which we all operate, it is vital that this important sector of our economy be aware of the risks and take appropriate steps to ensure their systems are secure.

When implementing new technologies, small businesses need to fully understand all of the potential security risks created by connecting to the Internet. Indeed, the risks to our systems are so complex and pervasive, that we cannot reasonably expect small businesses to be experts in all areas of security including properly implementing security controls for complex system configurations and assessing security features associated with new and emerging technology.

[1] 2003 County Business Patterns. http://www.census.gov.

NIST's Current Statutory Responsibilities under FISMA

Under the Federal Information Security Management Act (FISMA), NIST was assigned the following responsibilities:

- Develop IT standards and guidelines to secure federal systems;
- Conduct research to identify information security vulnerabilities and develop techniques to provide cost-effective security;
- Assess private-sector policies, practices, and commercially available technologies;
- Assist the private sector upon request; and
- Evaluate security policies and practices developed for national security systems to assess potential application for non-national security systems.

While targeted primarily toward federal agencies, the FISMA security standards and guidelines also are used widely by other organizations, including small businesses to help ensure that the information systems supporting enterprise operations are well protected, thereby enhancing competitiveness and productivity.

A sample of some NIST guidance which is available to small businesses is listed below:

- Guide for Securing Microsoft Windows XP Systems;
- Wireless Network Security;
- Security Considerations for Voice Over IP Systems;
- Security for Telecommuting and Broadband Communications;
- Guidelines on Electronic Mail Security;
- Guidelines on Securing Public Web Servers;
- Systems Administration Guidance for Windows 2000 Professional;
- Guidelines on Firewalls and Firewall Policy;
- Procedures for Handling Security Patches;
- Contingency Planning Guide for Information Technology Systems; and
- Risk Management Guide for Information Technology Systems.

All of these documents, as well as our ITL Bulletins, are available on our web-based Computer Security Resource Center (CSRC) (http://csrc.nist.gov) which provides a wide range of security materials and information to constituents. CSRC now has over 20 million "hits" annually. The CSRC site also contains many policies, procedures, and practices from both federal agencies and the private sector that are also advertised to the public through our publications and outreach efforts.

We have developed guidance for organizations, large and small, to maximize the security of their information systems so that they may securely conduct business transactions over the Internet. Hardware and software purchased by small businesses today are frequently installed without making any changes from the original configurations delivered by the

vendor. We are helping small businesses to understand security features and the importance of correct configuration. Even if they have taken steps to minimize the opportunity for inappropriate access by investing in firewall technology and virus protection software, they may not have correctly installed, managed, or updated those capabilities. Given the state of software insecurity today, vendors frequently issue security patches for their products. We are advising users of the importance of these patches and where to get up-to-date information and procedures for installing patches through our outreach efforts such as our website, workshops and conferences.

Interagency Collaborations

In 2002, NIST partnered with the Small Business Administration (SBA) and the Federal Bureau of Investigation's InfraGard program to sponsor computer security workshops and provide online support for small businesses. The workshops, which are held across the country, feature security experts who explain information security threats and vulnerabilities and describe protective tools and techniques which can be used to address potential security problems. To expand our outreach efforts, we have also developed a Small Business Outreach Site where you can find security resources and request a workshop to be held in your local area. (See http://csrc.nist.gov/securebiz/).

For the last four years NIST, in cooperation with SBA and the Association for Small Business Development Centers, has participated in the annual conference of Small Business Development Centers providing participants with information to increase awareness of NIST resources. In addition to our work with SBA and InfraGard, NIST is also working with the National Cyber Security Alliance (NCSA) to bring more online tools to small businesses on their small business website.
(See http://www.staysafeonline.org/basics/company/company.html)

Assistance for Small Manufacturers

NIST also is raising the awareness of the importance of cyber security in the small manufacturing community. The NIST Hollings Manufacturing Extension Partnership (MEP) was created to improve the competitiveness of America's smaller manufacturers. Realizing the gap in assistance for small firms in the cyber security area after September 11, 2001, NIST MEP developed the "eScan Security Assessment." This diagnostic tool was designed specifically for small businesses to determine how well their information technology systems are protected against failure or intrusion. It asks a series of questions and provides recommendations in the following areas: computer virus protection, file permissions, computer system physical environment, backup policies and procedures, potential computer system mechanical failures, IT contingency planning, information technology and security policies, international eCommerce concerns, Internet and eCommerce, and operating systems and security concerns.

The tool provides a report that scores each of these critical security areas. The assessment report categorizes the results and offers suggestions for improvement. NIST

MEP centers then assist the small manufacturers in addressing the issues uncovered in the assessment. While the NIST MEP program focuses on manufacturers, NIST has made the tool available for use online to all small businesses at http://escan.nist.gov.

National Vulnerability Database

NIST, with support from the Department of Homeland Security, recently developed the National Vulnerability Database (NVD) that integrates all publicly available U.S. Government computer vulnerability resources and provides references to industry resources. It contains information on almost 16,000 vulnerabilities and is available on our CSRC website at http://nvd.nist.gov/. Small businesses can go to this site to learn about vulnerabilities and how to remediate them.

Software Quality

Small and medium-sized businesses, indeed all organizations, rely on the software used on their information systems. We continue to work with industry to improve the security and reliability of software. For example, we develop standards and test suites for interoperable, robust, quality web applications and products. Our test suites are being used throughout the industry to improve the quality of implementations and specifications. We develop ways to measure the effectiveness of software assurance tools, and conduct research to assess current methods and tools in order to identify gaps and deficiencies which ultimately lead to software product failures and vulnerabilities. We conduct research and development in new areas to improve the quality of software, including software trustworthiness. We work with health-related organizations to advance the deployment of the electronic health records and to facilitate the development and implementation of a nationwide health information network.

IT Product Security Configuration Checklists

The Cyber Security Research and Development Act directed NIST to produce security checklists that cover specific technologies such as application servers, database systems, domain name servers, firewalls, operating systems, routers, and web servers. The checklists, when combined with high-quality guidance and training, substantially reduce the vulnerability of IT systems to attack. After working extensively with industry, IT vendors, and other government agencies, NIST has created a security checklist repository portal and detailed technical guidance on producing checklists. Working in concert with many government agencies such as the Office of Management and Budget, the National Security Agency, the Defense Information Systems Agency, the United States Air Force, the Department of Homeland Security and the private sector, the NIST repository now has some 87 checklists with an additional 15 expected to be finalized by May 2006. The checklists can be found at http://csrc.nist.gov/checklists/. DHS has provided crucial funding to support the development of this program.

Security Focused Research

NIST's near-term effort in Internet security research is directed at working with industry and other government agencies to improve the interoperability, scalability, and performance of new Internet security systems, to expedite the development of Internet infrastructure protection technologies, and to protect the core infrastructure of the Internet.

Looking further into the future, we see the potential for new computational models to threaten the mathematical underpinnings of today's cryptographic systems. In response, NIST is conducting research in the use of quantum information theory to devise ultra-secure network technologies that do not depend on today's cryptographic techniques.

NIST is a key player in the research and development of biometric standards and systems. We are working with industry and other government agencies to improve the accuracy of biometric systems that utilize fingerprints, face, iris and multi-modal technologies.

With a highly mobile workforce, use of handheld devices such as Personal Digital Assistants (PDAs) is quickly becoming a necessity for small and large organizations. NIST is working in collaboration with industry to improve authentication and encryption techniques associated with these products to ensure that the user's data and wireless communications are protected.

Meeting the challenge of securing our Nation's IT infrastructure demands a greater emphasis on the development of security-related metrics, models, datasets, and testbeds so that new products and best practices can be evaluated. The President's FY07 proposed budget will support NIST's collaborations with industry and academia to develop the necessary metrics and measurement techniques that will be combined to provide an assessment of overall system vulnerability. Utilizing approaches that have been successful in characterizing effects in the physical systems, NIST will develop the necessary measurement science and technologies to secure the Nation's IT Infrastructure.

Conclusion

In summary, Mr. Chairman, the IT security challenge facing small businesses is greater than it ever has been. Systems managed by small businesses are part of a large, interconnected community enabled by extensive networks and increased computing power. Certainly, there is great potential for malicious activity against non-secured or poorly secured systems or for accidental unauthorized disclosure of sensitive information or breach of privacy.

NIST will continue to develop ways to assist small businesses in their efforts to maximize capabilities and efficiencies offered by emerging technology while minimizing risk to their systems and information. We will continue our work in the areas of secure

configuration settings, product benchmarks, outreach, training, and research. The President's FY 2007 budget request would enhance those efforts.

We believe the programs and activities described today demonstrate our commitment to a more effective national cyber security environment by assisting small enterprises in protecting their assets and staying competitive in a cyber economy.

Thank you, Mr. Chairman for the opportunity to present NIST's views regarding security challenges facing small enterprises. I will be pleased to answer any questions that you and the other members of the Committee may have.