

Statement of

Edward Roback
Chief, Computer Security Division

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

Before the

House of Representatives
Committee on Government Reform
Subcommittee on Technology, Information Policy, Intergovernmental
Relations and the Census

“Locking Your Cyber Front Door – The Challenges Facing Home Users and
Small Businesses”

June 16, 2004

Chairman Putnam, members of the Subcommittee, thank you for this opportunity to testify today on our perspective regarding the challenges facing home users and small businesses in better securing their systems and information. I would like to address the questions you asked in your invitation to testify and tell you about the numerous cybersecurity activities underway at NIST. Many of these can assist small businesses in implementing better security controls.

NIST has had a long-standing role in working effectively with industry and federal agencies in ensuring the protection of sensitive information and information systems. Our research helps protect the confidentiality, integrity, and availability of information and system services. Helping to ensure secure flow of business-related information is essential to the functioning of our economy and indeed to our democracy. Our broader work in the area of information security is, generally speaking, applicable to a wide variety of users – from small business to the large agencies of the Federal government. Let me start by quickly reviewing our responsibilities in the area of information security.

NIST's Current Statutory Responsibilities

The Cyber Security Research and Development Act of 2002 assigned to NIST the following key responsibilities:

- Establish a program of assistance to institutions of higher education that enter into partnerships with for-profit entities to improve the security of computer systems;
- Institute a program to award post-doctoral research fellowships to individuals seeking research positions at institutions engaged in cybersecurity research;
- Develop checklists establishing settings and option selections that minimize security risks associated with federal government computer hardware or software systems;
- Support and consult with the Information System Security and Privacy Advisory Board, which has the mission to identify emerging issues related to computer security, privacy, and cryptography; and
- Conduct intramural cybersecurity security research.

The Federal Information Security Management Act (FISMA) of 2002 assigned NIST the following responsibilities:

- Developing IT standards and guidelines for the security of Federal systems;
- Conducting research to identify information security vulnerabilities and developing techniques to provide cost-effective security;

- Assessing private-sector policies, practices, and commercially available technologies;
- Assisting the private sector, upon request; and
- Evaluating security policies and practices developed for national security systems to assess potential application for non-national security systems.

With these broad legislative mandates in mind, let me now share our views on the issues posed by the Subcommittee.

Home users and small businesses face an enormous challenge in protecting their computers, which are connected to the Internet. These systems are operated in environments where there is normally not full knowledge or understanding of 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 people to become experts in this area. In addition, home users and small businesses, like all organizations, want to embrace and have available the latest advances in technology to make their tasks easier. For example, many may have no idea that their computers, if unprotected, can be used as zombies to launch distributed denial of service attacks. Many may not understand that sensitive information, residing on their machines, may be accessed and otherwise misused potentially resulting in great harm. 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. They also face the challenges of trying to determine what security configuration settings should be in place for their systems (given their risk environments) – and then how to actually “turn on” those settings.

We are all experiencing receipt of an overwhelming amount of SPAM e-mail and unfortunately, although filters are available to assist in identifying and blocking SPAM, the spammers continue to find ways to circumvent these solutions. In large organizations, we are certainly better positioned both from a staffing and budget perspective to put very strong formal processes in place to monitor and manage our environments in order to make them more secure. SPAM is more than an inconvenience. SPAM may also deliver viruses or worms or have fraudulent intent. Phishing schemes, the Internet version of social engineering to fool individuals into divulging personal financial data such as credit numbers or social security numbers, have become pervasive. Uninformed home users and small businesses may become victims.

The vulnerability of any one small business may not seem significant to many other than the owner and employees. However, over 95 percent of all U.S. businesses are small or medium-sized. 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. Therefore a vulnerability common to a large

percentage of these organizations could pose a threat to the Nation's economy and overall security.

In the special arena of information security, vulnerable small businesses also run the risk of being compromised for use in crimes against governmental or large industrial systems upon which we all rely. Most small businesses cannot afford an extensive security program, or often even hire a single full time expert. Nonetheless, they confront serious security challenges and must address security requirements based on identified needs. The difficulty for these organizations is to identify cost-effective security mechanisms and obtain training that is practical and feasible for their environment. Such organizations also need to become more educated consumers in terms of security, so that their limited security resources are well applied to meet the most obvious and serious threats.

Hardware and software purchased by small businesses and home users today is frequently installed without making any changes from the original configurations delivered by the vendor. Unfortunately, in most cases, these configurations have not been optimized for security. This puts home users and small businesses at risk and they need to better educate themselves about security features and what the implications and risks are associated with poorly configured systems. Given the state of software insecurity today, vendors are frequently issuing security patches for their products. Users need to be aware of the importance of these patches, where to get up-to-date information about these patches, and procedures for installing them. I would point out that the efforts of the DHS US-CERT are particularly germane here. Lessening the burden on home users and small businesses must include greater efforts on the part of Government working with the IT vendor community in order to deliver more secure products to IT consumers.

In that regard, Mr. Chairman, I'd like to share with you some of the work NIST is doing to support security improvements in this area.

NIST has formed a partnership with the Small Business Administration (SBA), and the Federal Bureau of Investigation's InfraGard program to sponsor workshops and on-line support for small businesses. This Co-sponsorship, which began in FY2002, has just been renewed this year. Because our experience shows that it is often very difficult for a small business to spare a person even for a half-day workshop, we have built a Small Business Resource Center on the NIST web site where our training materials can be freely accessed and used by small businesses for distribution and in-house security sessions.

We have also provided briefings to organizations at various events engaged with small businesses to publicize these available resources such as the Association of Small Business Development Centers, The National Entrepreneurial Conference and Expo, SBA's Senior Corps of Retired Executives, and the American Association of Community Colleges where many small business owners may hire students. We also placed security tips in the SBA Solutions Newsletter, which reaches more than 14,000 business owners.

Another area in which NIST has provided assistance is through its Manufacturing Extension Partnership's eScan Security Assessment Tool. The eScan Security

Assessment provides the small business with a diagnostic tool designed to assess the electronic security infrastructure of a small business and provide an action plan for improving it through a set of recommendations to correct many security problems.

U.S. small manufacturers are dependent upon the secure and reliable processing, storage and transmittal of information to conduct their internal and external business. Information and knowledge about customers, orders, manufacturing and intellectual property are the primary assets of any private business. Unfortunately, many businesses are not aware of the latest strategies for ensuring the security of their physical workplace and their information systems. These issues are especially important in the many defense manufacturing supply chains, as the security of the information and the ability to maintain business continuity affect the security of the entire country.

The *eScan* Security Assessment measures how well a business performs in these critical security areas:

- Strategies & Tactics for Virus Protection
- Physical Environment Security
- Contingencies for Mechanical Failures
- Security Policies & Procedures
- Internet and eCommerce Security
- File Permission Security
- Back-up Policies and Procedures
- Contingency Planning
- Miscellaneous Security Issues
- Operating System Security
- Wireless Security
- International eCommerce Concerns

The NIST MEP Centers are available to conduct the assessment and/or assist the company in solving their security issues. The *eScan* Security Assessment is available online at <http://escan.nist.gov/sat/index.nist>.

But in addition to these specific efforts, we believe that home users and small businesses can benefit greatly from a broad range of initiatives that we have undertaken. NIST continues to take strides toward securing the nation's infrastructure and support all users of information technology (IT) through its development of tools, standards, metrics and guidance.

Security Guidelines and Standards

We continue to develop standards and guidelines in support of our Federal responsibilities. Many of these are also used, on a voluntary basis, by organizations in the private sector. Hundreds of thousands of copies of our guidelines have been downloaded from our Computer Security Resource Center.

We recognize that the guidance, as written, has not been tailored for use by home users and small businesses, however, we are considering the development of a series of guidance which could be tailored for better usability by this group of users. The presentation would take the form of quick reference guides reinforcing good security principles and practices for specific IT components (Web, email, etc.).

A sample of some of our recent guidance releases is listed below:

- Wireless Network Security: 802.11, Bluetooth, and Handheld Devices;
- Security Guide for Interconnecting Information Technology 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.

See <http://csrc.nist.gov/publications/nistpubs/index.html> .

Network Security

Mr. Chairman, I'm very pleased to note that at NIST, we are aggressively working on development of robust, resilient, agile networks as defense against the kind of distributed denial of services (DDoS) attacks cited in your invitation letter.

NIST's efforts in Internet security research are focused on both near term objectives of expediting significant improvements to the security and integrity of today's Internet technologies, and longer term objectives such as exploring the use of quantum information theory to develop ultra-secure networking technologies of the future.

Our near term research is directed at working with industry and other Government agencies to improve the interoperability, scalability and performance of new Internet security systems and to expedite the development of Internet infrastructure protection technologies. NIST staff is actively working with the Internet Engineering Task Force (IETF) to design, develop, standardize and test new protocols that will make authentication, confidentiality and integrity services inherent capabilities of all networks based upon Internet technologies. NIST has taken leadership roles within the IETF in the specification of public key infrastructure, network layer security and key management technologies. Working shoulder to shoulder with industry, NIST is contributing technical specifications, modeling and analysis results, research prototypes and test and measurement tools to the IETF community to expedite the standardization of ubiquitous Internet security services and to foster the rapid development of commercial products.

Another area of focus for our near term efforts is the research and development of technologies to protect the core infrastructure of Internet. NIST is working with the IETF and other government agencies to devise means to protect the control protocols and infrastructure services that underlie the operation of today's Internet. NIST's research and standardization efforts in this area include: extensions to the Domain Name System (DNS) to add cryptographic authentication to this most basic Internet service, and the design and analysis of protection and restoration mechanisms to improve failure resilience of core switching and routing infrastructures. Our future work in this area will focus on improving security and resilience of core Internet routing protocols.

Looking further into the future, we see the potential for new computational paradigms 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 are not dependent upon today's cryptographic techniques.

Wireless Mobile Device Security

With the trend toward a highly mobile workforce, the acquisition of handheld devices such as Personal Digital Assistants (PDAs) is growing at an ever-increasing rate. These devices are relatively inexpensive productivity tools and are quickly becoming a necessity in today's business environment. Most handheld devices can be configured to send and receive electronic mail and browse the Internet. However, as handheld devices increasingly retain sensitive information or provide the means to obtain such information wirelessly, they must be protected.

Our efforts to date have focused on improving several aspects of security: user authentication, policy enforcement, and wireless communications. For user authentication we have developed a framework for multi-mode authentication that allows more than one authentication mechanism to contribute to the verification of a user's identity. For example, a biometric, such as voice input, may be required in combination with a security token, such as a smart card, before a user is permitted to access the contents of a device. In addition, we have invented a visual means of authentication that not only is easier than passwords for users to authenticate, but also significantly more powerful, and we have contributed updates to an open source code initiative that allow smart cards to be used on certain handheld devices.

For policy enforcement, we have developed a system that requires users to present a policy certificate to a device, as a means of moving from a restricted processing environment to one in which the privileges accorded a user via the policy certificate are enabled. Policy rules govern such things as application usage, file access, and communications interfaces, including wireless communications. This mechanism allows organization policy controls to be asserted on handheld devices, which typically are at the fringes of an organization's influence, and was designed to tie in with emerging Public Key Infrastructures.

For wireless communications, we have developed a highly-regarded publication on Wireless Network Security, aimed at reducing the risks associated with 802.11 wireless local area networks and Bluetooth wireless networks that are commonly used with handheld devices.

Security Awareness and Outreach

Timely, relevant, and easily accessible information to raise awareness about the risks, vulnerabilities and requirements for protection of information systems is urgently needed. This is particularly true for new and rapidly emerging technologies, which are being delivered with such alacrity by our industry.

We actively support information sharing through our conferences, workshops, web pages, publications, and bulletins. Finally, we also have a guideline available to assist agencies with their training activities and are an active supporter of the Federal Information Systems Security Educators' Association.

We sponsor the web-based Computer Security Resource Center (CSRC) to provide a wide-range of security materials and information to the community and link to the Federal Computer Incident Response Center at DHS and other emergency response centers. CSRC now has over 20 million "hits" annually. On CSRC, one of the most popular resources is the NIST-developed web-based tool known as ICAT that allows users to identify (and then fix) known vulnerabilities for their specific software. ICAT provides links to vendor sites at which the users can obtain patches to fix these vulnerabilities. This is important because many computer break-ins exploit well-known vulnerabilities. Over 6600 vulnerabilities are now catalogued in this NIST on-line database that receives over 200,000 hits per month. See <http://icat.nist.gov/icat.cfm> . While vulnerability patching is important, the sheer numbers of vulnerabilities and patches will become untenable in the long run. Users, including small businesses, should not be hesitant about expressing their needs for more secure, reliable, and robust software to vendors.

Security Assessment Guideline and Automated Security Self-Evaluation Tool (ASSET)

The Chief Information Officers Council and NIST developed a security assessment Framework to assist agencies with a very high level review of their security status. The Framework established the groundwork for standardizing on five levels of security and defined criteria agencies could use to determine if the levels were adequately implemented. By using the Framework levels, an organization can prioritize agency efforts as well as evaluate progress.

NIST Security Practices Web Sites

NIST operates the Federal Agency Security Practices (FASP) website to identify, evaluate, and disseminate best practices for CIP and security. The site contains many

agency policies, procedures and practices; the CIO pilot best practices; and, a Frequently-Asked-Questions section. Agencies are encouraged to share their IT security information and IT security practices and submit them for posting on the FASP site. Over 100 practices are now available via the site.

In accordance with tasking to NIST under FISMA, we are now expanding the service to share security practices from private-sector organizations.

Both of these sites may be of particular interest to small businesses.

IT Product Security Configuration Checklists

NIST is now in the process of developing IT product security checklists that provide settings and option selections that minimize the security risks associated with each computer hardware or software system that is, or is likely to become, widely used within the Federal Government. Vendors, agencies, and other reputable sources can use the template to construct and submit checklists that will populate a NIST public web-based repository. Within the next month we plan to publish a draft security guideline on checklist construction.

Closing

In summary, Mr. Chairman, the challenge facing home users and small businesses is greater than it has ever been. If they are to maximize all of the capabilities and efficiencies offered by emerging technology while minimizing risk to their systems and information, more must be done. Training efforts must be increased and more must be done in the areas of secure configuration settings, product benchmarks, outreach and research. Today, systems in homes and small businesses are part of a larger infrastructure. Those who have motivation to do harm normally will seek out the weakest link. Certainly, there is a high potential for malicious activity against these non-secured or poorly secured systems. As troubling as this is, of equal concern is the potential for accidental unauthorized disclosure of sensitive information or breach of privacy due to weak security controls on these systems.

We believe that some of the initiatives we've shared with you today, demonstrate our commitment to better national cybersecurity and recognize that more must be done by home users and small businesses to protect their information security.

Thank you, Mr. Chairman for the opportunity to present our views today regarding security challenges facing home users and small businesses. I will be pleased to answer any questions that you and the other members of the Committee may have.

Edward A. Roback
Chief, Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology

Mr. Roback serves as Chief of the Computer Security Division (CSD) at the National Institute of Standards and Technology (NIST) supporting the agency's responsibilities to protect sensitive Federal information and promote security in commercial information technology products. NIST-CSD also leads the implementation of NIST's responsibilities under the Federal Information Security Management Act of 2002 and the Cyber Security Research and Development Act of 2002. These efforts include work in the area of security standards, testing, e-authentication, studying security issues with emerging technologies, and developing security guidelines for Federal agencies. Mr. Roback heads NIST's participation on the NIST/NSA Technical Working Group and serves on the Committee on National Security Systems. He chaired NIST's algorithm selection committee for the Advanced Encryption Standard and served as Executive Secretary of the "Computer System Security and Privacy Advisory Board." He has also served on the U.S. Inter-agency Working Group on Cryptography and the U.S. delegation to the OECD Ad hoc Group of Experts on Cryptography Policy. He has chaired the Federal Agency Computer Security Programs Managers' Forum and co-authored *An Introduction to Computer Security: The NIST Handbook*. He also recently authored NIST's *Guidelines to Federal Organizations on Security Assurance and Acquisition/Use of Tested/Evaluated Products*.

Prior to joining NIST in 1989, he worked at the U.S. Department of State's Office of Information Systems Security. As a Presidential Management Intern at the Department, he concentrated on the development of systems security policy for the Department's classified and unclassified systems. He also participated in the computer security evaluation program, leading teams to evaluate computer security of classified and unclassified systems at U.S. Foreign Service missions worldwide. Mr. Roback received his M.A. at the University of Illinois at Urbana-Champaign in Political Science and holds a B.S. in Mathematical Economics and Computer Science from Rose-Hulman Institute of Technology.