Statement of

Ben Wu
Deputy Under Secretary
Technology Administration

U.S. Department of Commerce

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

"Information Security in the Federal Government: One Year into the Federal Information Security Management Act"

March 16, 2004

Thank you for this opportunity to testify today about the contributions of the National Institute of Standards and Technology (NIST) to strengthen information security in the Federal government.   I would like to principally focus my remarks on our important efforts to implement the assignments to NIST in the Federal Information Security Management Act (FISMA) of 2002 and some of the challenges we confront.

The Context of NIST Information Security Work

FISMA reinforced our long-standing statutory responsibilities for conducting security research and developing Federal information standards and guidelines.   We thank the Congress for this "vote of confidence" in our past work, with an expectation of continuing successful achievements in the future.

Information security is one of the most critical issues facing industry and government. The technological and scientific base that makes this country so strong is continually improving its ability to compete globally through tremendous advances in the capabilities of IT systems. As a nation, we are challenged to keep up with the growing complexity of our new technologies and the increasing sophistication of those seeking to maliciously interfere. Those "bad guys" continue to find new ways to breach our systems. While we focus on current implementations, new technology developments in IT systems and in other disciplines that increasingly rely on IT systems are coming on-line at an accelerating pace.

NIST standards and guidelines form the basis of the Federal government's ability to improve cyber security. Our information security work at NIST is conducted in our Information Technology Laboratory (ITL), which develops tests, metrics, and guidance for building trust and confidence in the IT systems that are now pervasive in the nation's economy, its organizational, governmental, scientific and technological infrastructure. NIST builds the trust of users of IT systems by concentrating on techniques and tools to manage, use, and improve IT systems, from single-user desktops, to highly complex multi-server, multi-node, wired and wireless systems that manage trillions of dollars in daily financial transfers, control power generation and distribution, and generate scientific and technological innovation.

NIST's success relies on its status as an objective, neutral, third party, allowing it to leverage its unique competencies to develop consensus solutions among private sector vendors, standards development organizations, and consortia. Unique competencies in smart cards, biometric devices and biometric analysis are applied to address the needs for better identity, authentication, and credentialing and to thwart identity theft. Tools, tests and metrics in software quality allow developers to "harden" code against "buggy" software and to protect against creation of unintended vulnerabilities; models, protocols and specifications for advanced networking technologies add resilience against catastrophic failure and provide agility to create networks where infrastructure is destroyed or does not exist. Our unique capabilities in theoretical mathematics, computational science and statistics enable other scientific disciplines to utilize IT systems to explore and innovate at the edge of technological frontiers.

NIST continues to take strides toward securing the nation's systems and information through development of tools, tests, metrics, and guidance but much remains to be done. FISMA and the Cyber Security Research and Development Act (CSRDA) of 2002 provide a roadmap for NIST to follow in performing this critical role. Today, I will discuss NIST's role in information security in the Federal government, one year into the Federal Information Security Management Act. Specifically, I will address:

- NIST responsibilities under FISMA;
- Summary of Standards Required by FISMA;
- Impact of Budget Restraints on NIST's Responsibilities under FISMA;
- Resources necessary for NIST to fulfill responsibility under FISMA;
- Other Supporting FISMA-related Activities at NIST; and
- Beyond our Current Plans and the FY 2005 Initiative.

NIST Responsibilities under the Federal Information Security Management Act of 2002

General responsibilities assigned to NIST under FISMA include:

- Developing IT standards for Federal systems, specifically to include security standards and guidelines;
- 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.

FISMA also contained a number of specific assignments to NIST, including development of:

- Standards to be used by Federal agencies to categorize information and information systems based on the objectives of providing appropriate levels of information security according to a range of risk levels;
- Guidelines recommending the types of information and information systems to be included in each category;
- Minimum information security requirements, such as management, operational, and technical security controls, for information and information systems in each such category;
- An Incident Handling Guideline and a Guideline to Identifying a System as a National Security System;
- Security performance indicators; and
- An annual public report.

Summary of Standards Required by FISMA

I would like to summarize the progress that we've made since FISMA became law on December 17, 2002. Significant progress has been made on these specific assignments and many have been completed.

FIPS Publication 199, *Standards for Security Categorization of Federal Information and Information Systems* (completed January 2004)

FISMA directed NIST to develop an information categorization standard for the Federal sector to support inter-agency, intra-agency and third party information sharing and ensure that consistent sensitivity (or impact) designations were applied. This is a crucial first step in the overall risk management process in that these categorizations influence an organization's determination regarding what security controls should be applied to protect the confidentiality, integrity and availability of the information. A problem, which had been noted by OMB, was the inconsistent application of security controls as information was shared across agency and third party boundaries. FIPS 199 provides a standard framework for government-wide use in information designation.

NIST Special Publication (SP) 800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories* (public draft now available; on track for completion in Summer 2004)

The companion guidance for FIPS 199, this Special Publication recommends a process by which agencies may categorize their systems and a methodology for effectively applying the principles included in FIPS 199. It presents common categories of information used by agencies and suggests default sensitivity or impact levels for these common information types (financial, personnel, health, etc.). It also provides a discussion and rationale for the generally recommended categorization for each information type, while recognizing that variances from the proposed default may sometimes be appropriate. Because of the numerous system interconnections and extensive use of data aggregation today, this guide helps highlight for agencies how the initial categorization can be influenced by special factors (factors such as mission and direct impact on mission). Again, it presents a common base of rationale which can be used government-wide to derive the impact of the loss of confidentiality, integrity and availability. This will assist in minimizing disparate treatment of information as it crosses organizational boundaries and a more cost-effective and consistent application of security resources.

NIST SP 800-53, *Recommended Security Controls for Federal Information Systems* (public draft available; on track for completion of FIPS 200 by December 2005)

This guidance document (which will form the basis for a future Federal standard, FIPS 200) defines security control baselines or minimum standards based on the impact category (Low, Moderate and High) of the information system as determined by the agency, using FIPS 199 and NIST SP 800-60. It also provides guidance for tailoring the baseline controls based on risk and cost-benefit assessments.

NIST SP 800-55, ***Security Metrics Guide for Information Technology Systems*** **(completed July 2003)**

This guideline, developed under FISMA and at the specific request of OMB, provides over twenty specific metrics that can be used by agencies to develop performance indicators for their programs. This guideline is now being used by agencies in developing their reporting under FISMA.

NIST SP 800-59, ***Guide for Identifying an Information System as a National Security System*** **(completed August 2003)**

This guidance was developed in conjunction with the Department of Defense and provides agencies criteria for identifying an information system as a national security system.

NIST SP 800-61, ***Computer Security Incident Handling Guide*** **(completed January 2004)**

NIST Special Publication 800-61, Computer Security Incident Handling Guide, assists organizations in mitigating the potential business impact of information security incidents by providing practical guidance on responding to a variety of incidents effectively and efficiently. Specifically, this document discusses the following items: 1) establishing a computer security incident response capability, including policy, procedure, and guideline creation; 2) selecting appropriate staff and building and maintaining their skills; 3) emphasizing the importance of incident detection and analysis throughout the organization; 4) maintaining situational awareness during large-scale incidents; and 5) handling incidents from initial preparation through the post-incident lessons learned phase, including specific advice on five common categories of incidents.

Other NIST Guidelines Currently in Development in Support of FISMA include:

- **NIST Special Publication 800-53A,** ***Techniques and Procedures for Verifying the Effectiveness of Security Controls in Information Systems*** (under development, draft expected in Summer, 2004, delayed due to budget cuts)
- **NIST SP 800-37,** ***Guide for Security Certification and Accreditation of Federal Information Systems*** (public draft now available; final draft expected Summer 2004)
- **NIST SP 800-63,** ***Recommendation for Electronic Authentication*** (public draft Jan 2003)
- **NIST SP 800-64,** ***Security Considerations in the Information System Development Life Cycle*** (Oct 2003)

- **NIST SP 800-50, *Building an Information Technology Security Awareness and Training Program*** (October 2003)
- **NIST SP 800-65, *Integrating Security into the Capital Planning and Investment Control Process*** (public draft expected by July 2004)
- ***Guideline on Voice over Internet Protocol Security*** (public draft Fall 2004)
- ***Guideline on Implementing IPSec*** (public draft Fall 2004)
- ***Guideline on use of IEEE 802.11i*** (secure wireless), (public draft Fall 2004)
- ***Guideline on Personal Digital Assistant Forensics*** (public draft Fall 2004)

Budgeting for NIST's Responsibilities under FISMA

Although we continue to give FISMA activities priority in our budgeting process, guidelines, standards, and related research in the following areas can not be accommodated within our FY 2004 funding level and have been scaled back or delayed:

- Guideline on archiving and disposal of information technology systems;
- Checklists and guidelines for effective implementation of COTS products (explicitly mandated by CSRDA);
- New security protocols for the core Internet, leaving a critical set of vulnerabilities that cannot be secured;
- Operating our Computer Security Expert Assist Team;
- Support to the National Information Assurance Partnership (reduced);
- Minimum-security recommended requirements for the most basic computer systems used by small businesses and home users;
- New investments in network security for wireless devices; and
- Implementation and use of IPv6.

At the current level of funding, we have delayed the following items previously included in our plans for FY 2005:

- Implementation guideline on use of minimum requirements for Federal systems (800-53)
- Comprehensive guideline on FISMA and other security requirements in the System Development Lifecycle
- Security program manager's guideline to information security program management
- Guideline on use of card-based technologies for cybersecurity
- Executive Guide to Cybersecurity
- Security requirements for operating systems, firewalls, biometrics, and process control systems
- Guideline for testing of operating systems, firewalls, and biometrics against the requirements
- Guideline for retrofit of cryptographic security modules for SCADA

- Guideline of conformance testing methods for security in process control systems
- Comprehensive Standards for Random and Pseudo-Random Number Generation to support strong cryptographic keys and strong algorithm initialization vectors
- Wireless Key Management for Secure Communications
- Incremental specifications for automated architectural security development
- Cybersecurity architectural guideline
- Standard set of Applications Programming Interface (APIs) for the specification, composition, enabling and disabling of policies that are amenable to uniform testing and could be applied to emerging technologies

Due to prioritization within the Computer Security Division, none of the specific tasks for developing guidelines under FISMA are affected; rather they are proceeding on schedule per the timeframes outlined in the Act.

Resources necessary for NIST to fulfill responsibility under FISMA

Now before the Congress is the President's FY 2005 budget request that includes a proposed increase of $6 million for NIST to address key national needs in cyber security. With the proposed increase of $6 million to NIST's current funding level of approximately $10.0 million, NIST will be able to more effectively work with industry and government agencies to accelerate solutions to critical cyber security issues. This specifically includes working with the Department of Homeland Security through its Science and Technology Directorate, as well as the Information Analysis and Infrastructure Protection Directorate's National Cyber Security Division to enhance collaborative efforts begun in 2003. This proposed expansion of NIST's current program will allow for additional deliverables in FY 2005 and a critical start to long-term work in key areas including:

Enhancing security, critical infrastructure application, and communication protocols. Numerous protocols are being developed for special purpose security, critical infrastructure and communications. The number of formal and *ad hoc* protocol standards precludes the ability for security specialists to participate in each effort; however, drawing upon the security, protocol, critical infrastructure, and vendor community, security guidance could be developed to provide protocol designers with advice and input into the design of secure protocols, hence enhancing security, critical infrastructure application, and communication protocols. Automated web-based testing for implementers of widely used protocols with security consequences could also be developed and provided to help assure correct implementation.

Expand the NIST Cryptographic Toolkit to include limited power, small-sized computing environments. Secure standard cryptographic mechanisms tailored for use in embedded devices are not being developed. Without such standards, security in these new technologies such as those associated with personal data assistants and blackberries already is inadequate as designers adapt existing standards to "fit" the low processing power and bandwidth available on an *ad hoc* insecure basis. As vulnerabilities are discovered, expensive patches must be applied and, since patching never achieves the desired coverage, system security exposures remain. The answer is to build products correctly from the start, but the available time window for action is closing. The NIST cryptographic toolkit will eventually be expanded to accommodate these limited power, small-sized computing environments. Guidance will also be developed and promulgated on where the new standards are applicable. The next generation of agile cryptographic security standards for process control, embedded systems, and mobile applications also will be developed. The key for effective use of these guidelines and standards throughout the community of developers is the timing of their release.

Fix broken wireless security standards by identifying, prioritizing, and accelerating approaches to securing wireless devices. Fixing insecure wireless security standards by identifying, prioritizing, and accelerating approaches to securing wireless communication protocols will speed the improvement of wireless security standards and ensure that insecure "interim fixes" do not become entrenched. NIST will participate in standards bodies activities to provide security expertise. Proof-of-concept prototype(s) for new wireless security technologies will be developed by leveraging, to the extent practicable, existing solutions (e.g., Public Key Infrastructure (PKI), Certificate Management, etc.). Guidance on wireless security design, implementation, and administration best practices will be written. Approaches to wireless security policy expression and enforcement, mobile device user authentication, secure ad hoc networking protocols, and intrusion detection in ad hoc networks will be developed. This is a one-time critical opportunity to make significant security enhancements, and speed is essential.

Metrics to understand, express, and improve our ability to build secure networks and systems from individually understood components. Systems of growing complexity tend to emphasize the challenge of building secure systems from secure components. There is a need to develop metrics to understand, express, and improve our ability to build secure networks and systems from individually understood components. Taxonomies could be developed for security metrics associated with assembling a networked computer system from components while ensuring it maintains desired security properties. Additionally, advanced methods could be developed to express security requirements for integrated systems, and metrics to enable rapid testing. Metrics to facilitate integration of components with known security exposures and risks are needed. Formal modeling of security properties in an architecture will be investigated. This is a major, long-term research effort, which could be launched in FY 2005 with appropriate funding.

Advanced means to cost-effectively control access of individuals and automated services to information and other automated services. Today’s cyber and physical threats along with legislation such as the USA PATRIOT Act, HIPAA and various national and foreign privacy laws have stressed the need to develop advanced means to cost-effectively control access of individuals and automated services to information and other automated services. This includes advanced access control meta models that will be capable of flexible, cost-effective implementation of strong cybersecurity access policies and standardized access policy definition frameworks (e.g., XML-based vocabularies). These frameworks could then be mapped to different enforcement mechanisms to develop a scalable, interoperable, enterprise-wide authorization-management framework.

Test procedures and guidelines for retrofitted cryptographic modules for system control and data acquisition (SCADA) systems. While last summer's black-out along the East Coast was attributed to an unfortunately and unlikely train of natural events, it was a bold reminder of the delicate state of some portions of our critical infrastructure and the need for significant upgrades to the IT supporting it. The security of SCADA and building control systems could be enhanced. With requested funding for FY 2005, test procedures and guidelines for retrofitted cryptographic modules for SCADA systems will be developed and standards for SCADA and other industrial control system security will be validated. Performance and conformance test methods for process controls, protection profiles for process control systems, and protocol standards for more secure communications for integrated building systems and services controls will be developed under this program.

Guide on approved media sanitization and disposal techniques. Approximately 5 billion gigabytes of information was created in 2002, equivalent to half a million libraries the size of the Library of Congress, or about 800 megabytes per person per year. There is a critical need for a guide on approved media sanitization and disposal techniques, which address today's new technologies such as mobile devices (Blackberry, PDAs), removable media (compact flash, secure digital), and hybrid devices (PDA/cellphones). As you may imagine, with the volume of digital information being produced and its rate of growth we receive numerous requests for appropriate disposal techniques. With requested funding increases, guidance in this area could be ready for public comment in FY 2005.

Other Supporting FISMA-related Activities at NIST

Cryptographic Modules for Federal Government Use. The Cryptographic Module Validation Program, operated in conjunction with the Government of Canada's Communication Security Establishment, has now validated over 750 modules. Our statistics from the testing laboratories show that 48 percent of the modules brought in for voluntary testing had security flaws that were corrected during testing. In other words, without our program, the Federal government would have had only a 50/50 chance of buying correctly implemented cryptography. Federal agencies are required to use validated modules in cryptographic applications. We expect that 200 or more modules will be submitted for validation within the next year. We continue to expect this program to grow, to include additional laboratory accreditations. Requested increases will enable us to enhance and expand this program.

Consensus-based recommended security requirements and corresponding testing procedures. In recent years we have worked with industry to develop the "Common Criteria" which can be used to specify security requirements. These requirements are then used by private-sector laboratories, accredited by NIST, for the voluntary evaluation of commercial products needed for the protection of government systems and networks. This work is undertaken in cooperation with the Defense Department's National Security Agency in our National Information Assurance Partnership (NIAP). There is a critical and continuing need to develop consensus based recommended security requirements and corresponding testing procedures for commonly used security and security-related technologies such as operating systems, routers, and intrusion detection and prevention systems. The FY 2005 budget increase would provide for the development of the most critical security requirements. These requirements and procedures increase the security of IT products, bring consistency to the testing process, reduce the need for government oversight during evaluations, ultimately decrease the cost to industry for the validation of products and provides more evaluated security products to both Federal users and the public in general.

National Information Assurance Partnership. You may be aware that the National Strategy to Secure Cyberspace calls for a review of the NIAP. We have had staff discussions with NSA, the NIAP laboratories, and vendors to identify ways we might improve the process, through research, process changes, and to understand the resources needed for NIAP to fully succeed. Additionally, we are participating on the industry common criteria/NIAP task force, established at the December 2003 Department of Homeland Security National Cybersecurity Summit. The output of that task force, which NIST co-chairs, is expected to issue its report shortly and may interest this Committee. Requested increases are needed for the development of additional security requirements and corresponding testing procedures, and to more generally improve NIAP processes based on recommendations that come out of the NIAP review process.

Beyond our Current Plans and the FY 2005 Initiative

In recognition of the constrained budget realities, we have focused on the most critical items in our current program plan and the proposed FY 2005 budget. However, in addition to the funding we receive from Congress each year, we do conduct reimbursable work for other agencies. I thought it would be helpful to the Committee to share some of the information security services that NIST could offer to other agency sponsors.

National network of accredited organizations capable of providing cost effective, quality security assessment services based on the NIST standards and guidelines. By December 2005, NIST's *Recommended Security Controls for Federal Information Systems* will by law become *Minimum Security Controls for Federal Information Systems.* This will form the basis for a risk-based certification and accreditation of Federal information systems, giving agency report cards new meaning. Work must be completed to create a national network of accredited organizations capable of providing cost effective, quality security assessment services based on the NIST standards and guidelines. This will build more assurance in existing processes, build a higher degree of consistency into certification processes and provide for a more cost-effective approach to certification for which the resources expended for certification track with the sensitivity of the particular system.

Guideline on the effective integration of security into the Federal Enterprise Architecture. Another area of major importance is the development of detailed guidance on the effective integration of security into the Federal Enterprise Architecture (FEA). Although the FEA framework is in place, an instructive guide assisting agencies in correctly mapping current security standards and guidelines to layers of the existing architecture is needed to ensure that the Enterprise Architectures developed by agencies reflect and accommodate security components. The Federal CIO Council has begun work in this area and NIST will continue to partner with the Council on this effort.

Comprehensive security checklists and benchmarks. Both hardware and software are typically shipped already configured for ultimate functionality and interoperability and not for secure use. NIST could greatly assist the public *and* private sector by delivering a series of guidance and supporting templates for decision-making on system settings and configurations. Security checklists and benchmarks, i.e., recommended security settings for specific commercial products such as firewalls, operating systems, and database systems, could help organizations and individuals to help themselves while still taking full advantage of emerging technologies and still reduce threats such as identity theft, denial-of-service or other malicious attacks on information systems. DHS has graciously been supporting some important NIST work in this regard and we will be able to maintain a web-based portal and solicit checklists, and perhaps internally produce one or two checklists in FY 2005 and each year thereafter. To be comprehensive, checklists should exist for *all IT products with security functionality widely used in the Federal government*, as is required under CSRDA.

Guidelines for users and system administrators to reduce spam. The reduction of spam has become a high priority from offices to households across the country. NIST recently completed a SPAM workshop on the current technologies and approaches to minimizing the costs and related impacts of SPAM. Research in support of spam filtering and guidance for users and system administrators to reduce spam could greatly assist agencies in minimizing this ongoing problem. Perhaps more importantly, with the growth of voice over IP, spammer techniques will be employable against two of an organization's access points to the outside world. Therefore work should also be done to understand new security vulnerabilities introduced by spammer techniques used in conjunction with this emerging technology and the viability of countermeasures.

Quality Code and Today's On-going Virus and Vulnerability Wars. You are probably familiar with the on-going daily virus wars that are currently raging, including viruses propagated by e-mail. In the early 1990s, NIST conducted anti-virus work, which was helpful to the establishment of today's robust anti-virus industry. The anti-virus industry is to be commended for keeping up with the continuing onslaught of viruses with timely updates to their virus definitions. In addition to viruses, with the continuing discoveries of vulnerabilities in commercial software and need to patch software, we are presently in a never-ending game of catch-up for users to stay up to date with the latest viruses and latest patches provided by vendors. And we are losing that catch-up game.

Of course, this is not a game but a serious security matter. Users do not keep their anti-virus programs up-to-date and do not apply software patches in a timely manner – if at all. When one steps back, it really highlights the need for the development of more secure code – code that will be resistant to viruses and other attacks that exploit vulnerabilities in software and hardware. We know how to build better code, but it is time consuming and tedious. The national annual costs of an inadequate infrastructure for software testing is estimated to range from $22.2 billion to $59.5 billion. We need to develop better secure code building technologies and standards, to include tests that vendors can run during development to produce high quality code and not impact their time-to-market requirements. NIST is ideally positioned to be able to do such work to help industry and thereby reduce the costs and security exposures for agencies and other critical users in the nation.

Closing

The standards and guidelines produced by NIST are key to the Federal government's ability to improve cyber security. NIST's impact reaches far beyond Federal systems. NIST guidelines are frequently used by state and local governments as well as by the private sector. In actively working with voluntary national and international standards development organizations, NIST guidelines and standards in areas such as cryptography and information security management are frequently adopted around the globe.

NIST takes its role in cybersecurity seriously and will work with the Committee to ensure that we are able to carry out our mandate to work with industry, academia, and standards development organizations to assure the secure flow of vital and sensitive information throughout our society. We applaud the Committee for its leadership and defining a critical role for NIST to play in supporting that effort. The FISMA activities – those already accomplished and currently underway – will lead to more consistent, risk-based, and cost-effective IT security at Federal agencies. The opportunities identified above would further strengthen Federal security.

These examples of our work and accomplishments demonstrate NIST's commitment to information security, across the government and the nation. They also demonstrate the base upon which NIST hopes to enhance our efforts, in line with the President's FY2005 budget request. It is an absolutely critical national need.

I am grateful to Chairman Putnam for holding this hearing, and for his support of NIST's critical role under FISMA. I will be pleased to answer your questions.

Technology Administration
BENJAMIN H. WU
DEPUTY UNDER SECRETARY OF COMMERCE FOR TECHNOLOGY

Ben Wu was sworn in as Deputy Under Secretary for Technology at the U.S. Department of Commerce on November 6, 2001. In this capacity, he supervises policy development, direction, and management at the Technology Administration (TA), a bureau of over 4,000 employees that includes the Office of Technology Policy (OTP), the National Institute of Standards and Technology (NIST), and the National Technical Information Service (NTIS).

TA serves as the principal resource to support Commerce Secretary Don Evans in developing policies to maximize science and technology's contribution to America's economic growth. Some of Ben's priorities have included supporting entrepreneurship and innovation, strengthening U.S. technology cooperation with other countries, enhancing research and development in our nation's federal laboratory systems, and creating greater collaboration between government, industry, and universities. Ben also participates in activities with the National Science and Technology Council (NSTC), a Cabinet-level council established by the President to coordinate science, space, and technology policy within the Federal research and development enterprise, and is the Executive Secretary for the NSTC Committee on Technology.

Prior to joining Commerce, Ben held senior staff positions in the U.S. Congress where he led on issues affecting United States technology and competitiveness policy. He worked in Congress from 1988, having served as Counsel to Congresswoman Constance A. Morella of Maryland and on the Science Committee, first serving on the Investigations and Oversight Subcommittee staff in 1993 and then on the Technology Subcommittee from 1995 until his current appointment.

Ben has extensive experience focusing on information technology, biomedical technology, and technology transfer policy. He was the primary congressional staff on legislation affecting federal intellectual property and federal technology transfer. Additionally, Ben has worked on Technology Administration issues since TA's inception in 1989, with particular emphasis on NIST. Ben was also the most senior member and the lead Committee staff of the House Y2K Task Force that directed congressional efforts to correct the Year 2000 computer problem.

Ben received a Bachelor of Arts from New York University in 1985 and a Juris Doctor from the University of Pittsburgh in 1988.