Statement of
Benjamin H. Wu
Deputy Under Secretary for Technology

Technology Administration
U.S. Department of Commerce

Before the

Committee on Government Reform

Subcommittee on Government Efficiency, Financial Management and Intergovernmental Relations

Subcommittee on Technology and Procurement Policy

House of Representatives
United States Congress

"Views on H.R. 3844, the Federal Information Security Management Act of 2002"

May 2, 2002

Good morning Chairman Horn and Members of the Subcommittee. On behalf of the Department of Commerce's Technology Administration and its National Institute of Standards and Technology (NIST), thank you for the invitation to speak to you today. I am Ben Wu, Deputy Under Secretary for Technology at the Department of Commerce. I am pleased to be here with you today to share with you the Department's views on H.R. 3844, the Federal Information Security Management Act of 2002. I note that the Administration is still developing a position on H.R. 3844.

Let me first commend you, Mr. Chairman, and the entire Subcommittee for continuing your focus on the critical issue of cybersecurity in Federal departments and agencies. Today's hearing will again remind Federal agencies that cybersecurity must be addressed in a comprehensive manner on a continuing basis. Like other elements of homeland defense, we are unlikely to ever be "finished" with cybersecurity. It demands the continuing attention of the Congress, the Executive Branch, industry, academia, and the public.

The NIST security program supports the nation's homeland defense effort as well as E-Government by enabling improvements in service to our citizens through secure electronic programs. As I will discuss in greater detail shortly, in the area of cybersecurity, NIST has specific statutory responsibilities for Federal agencies under the Computer Security Act of 1987 and follow-on legislation, including the Government Information Security Reform Act (GISRA). NIST is responsible for developing standards and guidelines to assist Federal agencies in the protection of sensitive unclassified systems. This is in addition to our broad mission of strengthening the U.S. economy – including improving the competitiveness of America's information technology (IT) industry. In support of this mission, we conduct standards and technology work to help industry produce more secure, yet cost-effective, products, which we believe will be more competitive in the marketplace. Having more secure products available in the marketplace will, of course, also benefit Federal agencies, because they principally use commercial products to construct and secure their systems.

NIST's Computer Security Division in our Information Technology Laboratory (ITL) is the focal point of our cybersecurity program. We focus on a few key areas: cryptographic standards and applications; security research; security management; and security testing. Our testing program includes both the National Information Assurance Partnership (a joint NIST and the National Security Agency program) and the Cryptographic Module Validation Program (a joint NIST and Government of Canada program).

In his testimony to you on March 6, 2002, Dr. Arden Bement, the Director of NIST, provided a broad-ranging review of NIST's activities undertaken to fulfill our important cybersecurity responsibilities. For the sake of brevity today, I would simply encourage

you to see his testimony for details. (Available on line at http://www.nist.gov/testimony/2002/abgisra.html)

NIST's Current Statutory Responsibilities

The Computer Security Act of 1987 was established to improve security and privacy of sensitive[1] information in Federal computer systems. In the realm of protecting sensitive unclassified information and systems, the Act assigned NIST responsibility to:

- Develop uniform security standards and guidelines for the protection of Federal computer systems within the Federal government;
- Develop technical, management, physical and administrative standards and guidelines for cost-effective protection of sensitive information and Federal computer systems;
- Develop guidelines for use by operators of Federal computer systems in training their employees in security awareness and good security practices;
- Develop validation procedures to evaluate the effectiveness of the security standards and guidelines developed;
- Assist the private sector, upon request, in using and applying NIST standards and guidelines;
- Provide technical assistance to operators of Federal computer systems in implementing these standards and guidelines; and
- Coordinate closely with other agencies such as the Departments of Energy and Defense, the Office of Management and Budget, and others as appropriate, to assure to the maximum extent feasible that standards and guidelines developed are consistent and compatible across the entire Federal sector (classified and sensitive unclassified).

These NIST responsibilities for the security of Federal sensitive systems were re-emphasized under the Government Information Security Reform Act (GISRA) in 2000. Under GISRA, NIST is tasked to:

[1] The Computer Security Act provides a broad definition of the term "sensitive" information: "any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled under section 552a of title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense or foreign policy." Note that this definition implies that sensitive information does not necessarily require confidentiality protection, as does national security (i.e., classified) information.

- Develop, issue, review and update standards and guidance for security of Federal information systems;

- Develop, issue, review and update guidelines for training in computer security awareness and accepted computer security practices;

- Provide agencies with guidance for security planning to assist in development of applications and system security plans;

- Provide guidance and assistance to agencies on cost-effective controls for interconnecting systems; and

- Evaluate information technologies to assess security vulnerabilities in Federal systems.

Proposed NIST Responsibilities under the Federal Information Security Management Act

Under FISMA, NIST would have the following key responsibilities:

- Develop IT standards and guidelines, including minimum requirements, for information systems;

- Develop security standards and guidelines, including minimum requirements, for the security of non-national security systems within the Federal government;

- Specifically develop guidelines for: 1) categorizing all Federal information and information systems according to a range of risk levels; 2) the types of information systems in each category; 3) minimum security requirements for information and information systems in each category; 4) detecting and handling Federal information security incidents; and 5) identification of national security systems within the Federal Government;

- Consult with other agencies to assure: 1) use of appropriate information security policies and procedures; 2) duplication of effort is avoided; and 3) that standards and guidelines are complementary with those employed to protect national security information and systems;

- Provide assistance to agencies on 1) complying with NIST-developed standards and guidelines; 2) detecting and handling security incidents; and 3) security policies, procedures, and practices;

- Submit proposed standards and guidelines, accompanied by recommendation of the extent to which they should be made compulsory and binding, to the Director of the Office of Management and Budget (OMB) for promulgation;

- Conduct security research;

- Develop security performance indicators;

- Evaluate private sector information security policies and practices for potential use in the government;

- Solicit recommendations of the Information Security Advisory Board on proposed standards and guidelines and also submit those to the Director of OMB; and

- Report annually to OMB on: 1) compliance with Clinger-Cohen requirements; 2) major deficiencies in Federal security; and 3) recommendations for improvement.

Additionally, germane to NIST's key security responsibilities, FISMA would:

- Establish an Office for Information Security Programs at NIST, the director of which would be responsible for administering NIST's information security responsibilities under FISMA;

- Authorize a $20 million level funding for NIST's security program;[2]

- Rename the "Computer System Security and Privacy Advisory Board" as the "Information Security Board," add the Director of OMB (and delete the Secretary of Commerce) as a customer for the Board's advice, and authorize funds for its operation; and

- Eliminate the existing process, under limited and specified circumstances, for agencies to waive the use of mandatory and binding security standards.[3]

Comments on FISMA

Overall, the drafters of the bill are to be commended for taking a sound and practical approach to information security, and one that will serve the nation well in the years ahead. The bill appropriately maintains the existing separation of responsibilities for Federal national security and sensitive systems. Current NIST activities are well aligned with the majority of the bill's provisions, and the additional activities, specific assignments, and envisioned growth of the NIST cybersecurity program will further

[2] Currently, approximately $10 million of direct Congressional appropriations funds the NIST security technical staff of about 45 to support our Computer Security Act responsibilities.

[3] Under the Computer Security Act and a November 14, 1988 delegation of authority from the Secretary of Commerce, agencies may waive the use of mandatory standards when compliance would adversely affect the accomplishment of an agency's mission or cause a major adverse financial impact that is not offset by governmentwide savings. Agencies must notify the Congress and publish a notice in the Federal Register of such decisions.

strengthen the security of Federal agency systems. Moreover, the bill will promote consistency in the protection accorded to similar systems and information across the entire government. Generally speaking, increasing the funding of the NIST program is consistent with the President's budget proposal, although the amounts proposed in the bill exceed those in the Administration's budget. I would respectfully offer the following specific comments on the bill for the Committee's consideration.

The proposed transfer of authority to issue standards and guidelines from the Secretary of Commerce to the Director of OMB should be reconsidered. The Director of OMB issues broad information security policy and guidance to agencies complemented by the detailed security standards and guidelines developed by NIST. The proposed process presents the opportunity for delay as additional senior managerial approvals would be required. Instead, as we fight the war on terrorism, we should be thinking about how to streamline the development and issuance of security standards, while still maintaining the important process of public review and comment. Because NIST activities are more directly and immediately accountable to the Secretary of Commerce, it is appropriate that his authority be retained in this regard. The Secretary's strong and continuing engagement with industry also brings an important perspective to the standards development process.

In the bill there are also a number of references to the "standards development" role of OMB. Since OMB develops and issues broad security policy and guidance, this should be clarified vis-à-vis NIST's role to develop standards and guidelines within the Federal Government.

The third comment has to do with agencies' current limited ability to waive "mandatory and binding" standards. As you know, the Federal government is an exceedingly large and diverse environment -- with operations from Moscow to Honolulu to Washington -- with an even wider variety of sensitive and not-so-sensitive information and systems. The present approach, with its very public process of Congressional and public notice process (in the Federal Register) strongly discourages the waiving of mandatory standards. After all, there have only been a handful of security waivers since the passage of the Computer Security Act. In the field of security, like all others, we must spend Federal resources wisely in accordance with sound risk management. Eliminating this option may lead to wasteful or misapplied spending because, in some situations, there may be alternate security measures that effectively allow the agency to meet the same overall security *objective*, although not the letter of the standardized security method. For these reasons, we believe it makes sense to maintain the current approach.

Lastly, the bill would require that NIST provide OMB with an annual report regarding major deficiencies in information security at Federal agencies. Since NIST's responsibilities do not extent to providing day-to-day operational security for Federal agencies, any such report would be woefully incomplete. However, OMB will still obtain the necessary information under FISMA since its provisions, like those of GISRA, require agencies to provide OMB with a report of their independent security evaluations. OMB thus obtains a very direct and unfiltered view of the security posture of the agencies. I would note that this information would also be useful to NIST to help

identify potential needs of the agencies for additional security standards and guidelines (or modifications to those already existing). Therefore we request that this NIST reporting requirement be deleted as unnecessary and duplicative. Of course, we always stand ready to provide OMB with any additional information they may require.

We would welcome the opportunity to continue its discussions with the drafters to further refine the bill to address these and a few other very minor concerns that we have.

Conclusion

Let me close by emphasizing that our national commitment to improve cybersecurity must be increased -- in Federal agencies and elsewhere. As Representative Davis' bill again re-emphasizes, there is much more to be done to address cybersecurity in the Federal government. The NIST cybersecurity program has a proven track record of success and stands ready to play the enhanced role envisioned in FISMA.

Thank you, Mr. Chairman for the opportunity to present our views today on FISMA. I will be pleased to answer any questions that you and the other members of the Committee may have.

DEPUTY UNDER SECRETARY FOR TECHNOLOGY

TECHNOLOGY ADMINISTRATION

BENJAMIN H. WU

Benjamin H. 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 works along side Under Secretary Phillip J. Bond to support Commerce Secretary Don Evans in developing science and technology policies to maximize technology's contribution to America's economic growth.

The Office of the Under Secretary for Technology supervises policy development and direction among the Office of Technology Policy (OTP), the National Institute of Standards and Technology (NIST), the National Technical Information Service (NTIS), the Office of Space Commercialization (OSC), and other areas.

Prior to joining Commerce, Mr. Wu held senior staff positions in the U.S. Congress for thirteen years. Most recently, from 1995 until his current appointment, Ben led on technology issues with the Technology Subcommittee of the House Science Committee. He worked in Congress since 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.

Ben has extensive experience working on issues affecting United States technology and competitiveness policy. Specifically, he has focused on information technology, biomedical technology, and technology transfer policy. He has been the primary congressional staff member for 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 the National Institute of Standards and Technology. 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.