Testimony of

Mr. Benjamin Wu

October 9, 2002

Good morning. I am Ben Wu, Deputy Under Secretary for Technology of the Department of Commerce. Thank you for inviting me to discuss the work of the National Institute of Standards and Technology under the U.S.A. Patriot Act and the Enhanced Border Security and Visa Reform Act. The Technology Administration (TA) is the only Federal agency working to maximize technology's contribution to America's economic growth. The National Institute of Standards and Technology (NIST), a part of the Technology Administration, works with industry to develop measurements, standards and a variety of technologies. Our efforts are designed to enhance American productivity, facilitate trade and improve the quality of life.

NIST has four related programs: The laboratories, including the Information Technology Laboratory that works with the biometrics industry. The Baldrige National Quality Program, which promotes excellence in business, health care and education. The Advanced Technology Program, which funds high-risk private sector research on promising technologies that have the potential for making a broad impact on economic growth. And the Manufacturing Extension Partnership, in which NIST works with 2,000 manufacturing specialists and staff at affiliated centers around the country. NIST has a staff of some 3,000 scientists, engineers and other personnel, and about 1,600 visiting researchers.

Last year's terrorist attacks on the Pentagon and the World Trade Center taught us a great deal about our strengths and weaknesses as a nation. We witnessed great courage on the part of men and women in the military, fire fighters, police officers and ordinary citizens. And many of us experienced an unfamiliar sense of vulnerability. Yet, in some ways, the attacks have backfired on the perpetrators. They sparked a sense of solidarity among Americans, and strengthened our determination to enhance the security of our citizens.

President Bush, the entire administration, and the Commerce Department are committed to strengthening homeland security while maintaining American leadership in science and technology and accelerating the pace of scientific discovery and technological innovation.

Systems using biometrics--automated methods of recognizing a person based on physiological or behavioral characteristics--are increasingly being used to verify identities and restrict access to buildings, computer networks, and other secure sites. In our view, biometric technologies are a part of a needed foundation for secure identification. Biometric technologies can support homeland security, prevent ID fraud and play a role in supporting confidential financial transactions. In the biometrics arena, NIST has worked with industry and other government agencies for years.

Improved Biometrics Critical to Border Security

The successful use of the classic biometric, fingerprints, owes much to NIST research and development. For more than 30 years, NIST computer scientists have helped the FBI improve the automation process for matching "rolled" fingerprints taken by law enforcement agencies or "latent" prints found at crime scenes against the FBI's master file of fingerprints. NIST test data have been used to develop automated systems that can correctly match fingerprints by the minutiae, or tiny details, that investigators previously had to read by hand. In cooperation with the American National Standards Institute (ANSI), NIST also developed a uniform way for fingerprint, facial, scar, mark, and tattoo data to be exchanged between different jurisdictions and between dissimilar systems made by different manufacturers.

In conjunction with the FBI, NIST has developed several databases, including one consisting of 258 latent fingerprints and their matching "rolled" file prints. This database can be used by researchers and commercial developers to create and test new fingerprint identification algorithms, test commercial and research systems that conform to the NIST/ANSI standard, and assist in training latent fingerprint examiners. The increasing use of specialized "live" fingerprint scanners will help ensure that a high-quality fingerprint can be captured quickly and added to the FBI's current files. Use of these scanners also should speed up the matching of fingerprints against the FBI database of more than 40 million prints.

Computer scientists at NIST also have extensive experience working with systems that match facial images. While facial recognition systems employ different algorithms than fingerprint systems, many of the underlying methods for testing the accuracy of these systems are the same. This work has been extended to include the specific biometric systems and scenarios required for visa systems under the Patriot Act, as amended by the Enhanced Border Security and Visa Reform Act. NIST has statutory responsibilities to develop and certify a technology standard that can be used to verify the identity of persons applying for a U.S. visa or using a visa to enter the country. The Department of Justice and Department of State also expect NIST to certify the accuracy of specific government and commercial systems being considered for use in this visa system.

These acts call for developing and certifying a technology standard for verifying the identity of individuals, and determining the accuracy of biometrics. NIST is spearheading the Face Recognition Vendor Test 2002, which is evaluating automated facial recognition systems that eventually could be used in the identification and verification process for people who apply for visas to visit the United States. The significance of the Face Recognition Vendor Test 2002 is evident by its large number of sponsors and supporters; this includes sixteen government departments and agencies. The current evaluation builds on the success NIST personnel have had in evaluating face recognition systems over the last decade. The evaluation methodology developed for FRVT 2002 will become a standard for evaluating other biometric technology. We will learn precisely how accurate and reliable these new systems are.

Fourteen companies participated in FRVT 2002. We deliberately designed a tough test that involved matching extremely challenging real world images. It required participants to process a set of about 121,000 images, and match all possible pairs of images from the 121,000 image set. In other words, this required some 15 billion matches. As you can imagine, this generated a mountain of data, and we are crunching all the numbers to see how well the systems worked.

NIST is also currently performing fingerprint matching accuracy studies. These include the following: using ten rolled fingerprints to match against the FBI database; using ten (or fewer) flat fingerprints to match against the FBI database; and using a single flat fingerprint for verification. It is important to determine the accuracy of all of these scenarios. To perform these tests in operational scenarios, NIST has received large scale databases from the INS, including 3 million fingerprint images. For each of 620,000 unique subjects, there are two or more samples from each index finger taken at different times. Another INS database contains 100,000 sets of ten rolled fingerprints and associated flat fingerprints.

This program will produce standard measurements of accuracy for biometric systems, standard

XML-based scoring software, and accuracy measurements for specific biometrics required for the system scenarios mandated under the Border Security Act. We hope this work will have wide impact beyond the mandated systems; standard test methods are likely to be accepted as international standards, and discussions are under way concerning the use of these same standards for airport security.

Another requirement of the Border Security Act is to establish document authentication standards for tamper resistant entry and exit documents to the U.S. NIST is recommending the use of Public Key Infrastructure technologies to provide for electronic tamper resistance.

Later this year, NIST expects to submit its report on this work to the State and Justice Departments for transmittal to the U.S. Congress. The report will make a recommendation on which biometric, or combination of biometrics, would best secure the nation's borders.

NIST Plays Key Role in Biometric Standards

Open consensus standards, and associated testing, are critical to providing higher levels of security through biometric identification systems. Throughout the years, NIST has worked in partnership with U.S. industry and other federal agencies to establish formal groups for accelerating national and international biometric standardization. Two recent additions to the list are the Technical Committee M1 on Biometrics, started in November 2001 by the executive board of the International Committee for Information Technology Standards (INCITS), and a new subcommittee on biometrics (the Joint Technical Committee 1 SC 37-Biometrics) created in June 2002 by the International Organization on Standardization (ISO). A NIST biometric expert is serving as chair of the former and acting chair of the latter.

The Biometric Consortium serves as the federal government's focal point for research, development, testing, evaluation and application of biometric-based personal identification and verification technology. The consortium now has more than 900 members, including 60 government agencies. NIST and the National Security Agency co-chair the consortium. NIST has collaborated with the consortium, the biometric industry, and other biometric organizations to create a Common Biometric Exchange File Format (CBEFF). The format already is part of government requirements for data interchange and is being adopted by the biometric industry. The specification is a candidate for fast track approval as an ANSI standard and as an international standard for exchange of many types of biometric data files, including data on fingerprints, faces, palm prints, retinas, and iris and voice patterns.

Just a few years ago NIST computer scientists did some innovative work that significantly extends the range of fingerprint matching capabilities available to law enforcement officers. Working with the FBI, we developed software that enhances low-quality fingerprints for electronic matching. Low-quality fingerprints are precisely the kind you are most likely to find at a crime scene. They are the opposite of the carefully done prints you get when a suspect is booked at a police station. Those are relatively easy to match electronically. Trying to make a match based on the latent fingerprints found at crime scenes is much more difficult. Typically, investigators have to work with smudged, partial prints that are naturally of poor quality.

Until recently, matching these crime scene fingerprints electronically with those in the FBI's database was almost impossible. The new software we developed in cooperation with the FBI makes it possible to search the entire FBI database, instead of only part of it. It also allows law enforcement agencies in different locations to exchange fingerprint information directly, instead of always working through a national database. The software speeds up and automates what had been a very laborious process.

Both the national and international communities need this work to be done, and time is a compelling factor for new homeland security applications. As you can see, there is much important work still to be done. When the private sector and universities team up with federal and state government, we succeed in leveraging the available resources. Thank you, Madame Chairwoman, I will be pleased to answer any questions you have.