TESTIMONY
U.S. HOUSE OF REPRESENTATIVES
SELECT COMMITTEE ON HOMELAND SECURITY

Lawrence M. Wein
Paul E. Holden Professor of Management Science
Graduate School of Business, Stanford University

September 30, 2004
Hearing: Disrupting Terrorist Travel: Safeguarding America's Borders Through Information Sharing

Good afternoon, Chairman Cox, Ranking Member Turner, and the Members of the House Select Committee on Homeland Security. I am honored to appear before you today.

I am the Paul E. Holden Professor of Management Science at the Graduate School of Business, Stanford University. I teach operations management to MBA students, and perform research in the areas of operations management, medicine and biology. At their essence, many homeland security problems are service operations problems: Just as McDonalds needs to deliver hamburgers in a rapid and defect-free manner, the US Government needs to quickly deliver vaccines and antibiotics after an attack and to safely prevent nuclear weapons and terrorists crossing our borders.

Since September 11, 2001, I have used mathematics to analyze a variety of homeland security problems in bioterrorism (effective responses to terrorist attacks using smallpox, anthrax or botulinum toxin) and in border security (evaluating ways to detect nuclear weapons coming through ports). These analyses have led to policy recommendations, several of which the U.S. Government has adopted.

Today, I am here to discuss the results of a study I conducted at Stanford University with Ph.D. student Manas Baveja that examined the ability of the US-VISIT program to accurately match the fingerprints of visitors at ports of entry against a watchlist that contains the stored fingerprint images of suspected terrorists. The implications of our findings are disturbing, so much so that last week I briefed members of the Homeland Security Council, staff members from the Office of the Vice President, analysts from the Government Accounting Office (GAO) and officials from the Department of Homeland Security.

On the surface, biometric identification of the US-VISIT Program appears to be highly effective. A May 2004 NIST study, entitled "Matching Performance for the US-VISIT IDENT System Using Flat Fingerprints," predicted that the likelihood that US-VISIT would flag a terrorist whose fingerprints are stored on the biometric watchlist is 96%, while simultaneously limiting the false positive probability, i.e., the likelihood that a visitor not on the watchlist would nonetheless generate a watchlist hit, to 3 in 1,000.

So what's the problem? It turns out that the devil is in the details: The biometric software also computes the quality of each fingerprint image, and it is very difficult to accurately match poor-quality images. Our study stems from the belief that terrorist organizations can exploit this observation by choosing US-bound terrorists that have either poor image quality (e.g., worn out fingers) or deliberately reduced image quality (e.g., surgery, chemicals, sandpaper). The relevant data is publicly available on the NIST web site, and we know Al Qaeda has the sophistication to understand this and has a large pool of potential terrorists to draw from.

Using publicly available biometric data from NIST, we developed and analyzed a novel mathematical model that allows red-teaming: First, the government develops a biometric strategy to maximize terrorist detection for a given inspector staffing level, and then the visiting terrorist attempts to defeat the biometric system by choosing the image quality to minimize his chances of getting caught.

The results are sobering: the currently implemented strategy has only a 53% chance of detecting a terrorist during US entry, compared to the overall value of 96% mentioned earlier. The detection probability is reduced to essentially a coin-flip because the terrorist is allowed to exploit the vulnerability in the biometric system.

The good news is that our study pointed to possible solutions that our nation can implement. Rather than using the current one-size-fits-all rule for generating watchlist hits, we derived different rules for different levels of image quality and improved the likelihood of detecting a terrorist from 53% to 73% without increasing the false positive rate.

Unfortunately, our study predicts that increasing staffing levels of US Custom and Border Protection inspectors would offer only modest benefits, and could increase the 73% detection by only an additional 5%. Given that US-VISIT runs millions of watchlist checks each year, this is an unacceptable security risk.

Fortunately, our nation has a second solution it can rely upon. Instead of using a software system that scans two index fingers, we found that that allowing additional fingers to be tested from people with worse image qualities achieves a 95% detection probability, without increasing the primary plus secondary inspection workload associated with legal visitors.

Finally, the government's investment in biometrics at ports of entry for detecting terrorists should be assessed in light of the detection probability required to deter terrorists from crossing at an official port of entry. The deterrence value of a fingerprint system depends on the terrorists' perceived likelihood of successfully entering the US between the ports of entry, e.g., along the US-Mexico border. While this detection rate has been estimated to be approximately 25% in a recent Time Magazine article, it appears that Al Qaeda prefers to enter the US at ports of entry.

To summarize, there is a serious but reparable vulnerability in the biometric identification system of the US-VISIT Program, which is our last line of defense for keeping terrorists off U.S. soil. A minor software modification that allows the watchlist rule to vary with image quality can increase detection from 53% to 73%. I have provided details to officials who oversee the US-VISIT operations, and this should be implemented as soon as possible. The use of more than 2 fingers for low-quality images can achieve a detection probability of 95%. Although switching from a 2-fingerprint to a 10-fingerprint system may be costly and disruptive, there is no excuse for a 10-billion dollar program to settle for performance below this level. Indeed, our results are not inconsistent with the warning in the November, 2002 NIST report that a 2-finger search was not sufficient for identification from a large watchlist. If slower 2-finger matching algorithms cannot approach 95% detection for poor-quality images, then the US-VISIT Program should be reconfigured with 10-fingerprint scanners as soon as possible.

Our recommendations hinge on the assumption that terrorist organizations as sophisticated as Al Qaeda will eventually attempt to defeat the US-VISIT system by employing terrorists with poor-quality fingerprints. In light of the meticulous planning that went into the 9/11 attacks, I believe this assumption is not only prudent, but realistic.

Thank you, and I look forward to responding to your questions.