Biometrics and the Border Management Challenge

Testimony of

Dennis Carlton
Director of Washington Operations
International Biometric Group, LLC

To the

House Select Committee on Homeland Security
Subcommittee on Infrastructure and Border Security

"Integrity and Security at the Borders:
The US VISIT Program"

January 28, 2004

My name is Dennis Carlton and I am the Director of Washington Operations for International Biometric Group of New York City. On behalf of our company, I'd like to thank the committee for the opportunity to talk to you about the technology called biometrics and some of the likely the issues associated with introducing biometrics into the border management system.

Let me begin with a brief description of International Biometric Group so that you better understand who we are and our unique position in the world of biometrics. International Biometric Group, or IBG, provides independent consulting services to government and private industry customers interested in implementing biometric technologies. Our organization focuses on three primary functions: (1) evaluating and reporting on biometric products and vendors, as well as the markets in which they compete, (2) advising clients on how to implement biometric systems, and (3) integrating a wide range of biometric hardware and software to meet the security needs of our customers. We take a practical, hands-on approach toward biometrics. We have conducted extensive comparative performance testing of more than fifty different biometric solutions so that we know how they're likely to perform in the real world. IBG holds to a strict vendor-neutral policy, which enables us to maintain close relationships with biometrics vendors while ensuring that our clients receive accurate and independent advice on which biometric systems can best meet their needs.

I'd like to take a moment to review some of the basics of biometrics. A technical definition of biometrics is the automated measurement of behavioral or physiological characteristics of a human being to determine or authenticate their identity. In other words, it's the use of computers to confirm who a person is by matching a behavior or a permanent physical characteristic with similar records in a database. Biometrics alone can't determine an individual's identity but they can effectively distinguish one person from another. There is a wide range of products in the market that can acquire and match a person's biometric data to perform a quick and accurate identification. With respect to border management, the U.S. has focused its attention on

fingerprint matching and facial recognition biometrics, although other biometrics such as iris recognition, hand geometry, and speaker authentication technologies are also being assessed.

One year ago, IBG delivered a report to the White House Office of Science and Technology Policy entitled "Use of Biometric Technologies in the United States Visa Issuance and Border Entry/Exit Systems". I was the principal investigator and author of this report, a summary of which has been included in the material provided to committee members. In conducting research for this study we visited several U.S. consulates around the world as well as American sea, air and land ports of entry. The OSTP sought a no-holds-barred look at the practical challenges of implementing biometrics in the field both at consulates and ports of entry – I like to think we accomplished that goal. From the OSTP research and our subsequent participation in several ongoing initiatives involving biometrics and international travel security, IBG has gained significant insight into the integration, performance, and workflow challenges associated with implementing biometrics within US VISIT and our border management system.

IBG's report to the OSTP highlighted several issues related to integrating biometrics within US VISIT worthy of reemphasis before this committee:

- Biometrics should be implemented in a manner that augments rather than replaces existing border management IT systems. The fact that an individual matches the biometric associated with a travel document does not ensure that the individual qualifies for admission to the United States. Biometrics alone cannot replace the professional judgment of experienced border management personnel.
- Since the current generation of biometric technologies is not 100% accurate, a seamless exception handling process must be incorporated throughout the design of the system.
- The system also must be designed with an eye toward continuing technology refreshment. The lifecycle of biometric products turns over at least as fast as other IT components – US VISIT should be designed with seamless transitions to newer, more accurate solutions in mind.
- The government must invest in continuing research and development into improving biometric products. The centennial of the Wright Brothers first powered flight serves as a reminder that significant innovations may come from unlikely sources. In the past few years there has been an explosion of new biometric technologies being introduced into the marketplace, many of which warrant the nurture of the federal government. In addition to financial support, the federal government may need to approve regulatory and legislative changes to authorize the development of databases that can be used to test the effectiveness of new biometric solutions.

The success of any biometric solution depends in great measure on its stakeholders establishing realistic performance expectations for the system; given its unprecedented scale and visibility, this will be especially true of the US VISIT system. Among the key performance considerations are:

- Stakeholders need to have practical expectations as to the performance of biometric technologies. The current generation of biometric systems is not 100% accurate but biometrics don't need to be perfect in order to enhance border security. The mere presence of a device that can positively link an individual with the documentation they carry will serve as a deterrent to many impostors. Border inspection personnel use their

professional judgment to resolve exception situations every day; biometrics problems can be resolved in much the same manner as any other identification document discrepancy.

- The system design must incorporate a comprehensive security and privacy architecture. Good security and privacy practices are not antithetical and can both be accommodated in US VISIT. Biometrics themselves are privacy neutral – it's the way they are employed, and the protections put in place to limit misuse, that make biometrics either privacy-invasive or privacy-protective. What is essential is that individuals are fully informed on how their data is collected, used, shared, and secured. For more information about biometrics and privacy I commend to you an IBG-sponsored website dedicated exclusively to the subject, www.BioPrivacy.org.
- Reaching a consensus with our international partners on privacy policy will be difficult because of significant differences in our privacy expectations. In general, while Americans often don't hesitate to provide personal data in exchange for commercial benefits but frequently oppose sharing such data with government, their counterparts in Europe and Asia view cooperation with their government as a duty of citizens in a civil society but don't feel similarly compelled to provide personal data to commercial concerns. For the time being, some parties have staked out extreme positions. Compromise will mostly likely be achieved when views converge toward a standard that defines a minimal exchange of a traveler's personal or biometric data to effect efficient commerce between governments.

The advent of US VISIT and biometric technologies will certainly alter the primary and secondary inspections processes at U.S. ports of entry but these changes need not result in delay and inefficiency. Some of the measures that can be taken to reduce the impacts caused by these changes include:

- U.S. border management solutions must be designed to accommodate multiple forms of biometric technologies. Although the International Civil Aviation Organization has specified that facial recognition is the universal biometric to secure machine-readable travel documentation, the U.S. will continue to leverage its investment in fingerprint databases to identify travelers who might pose a security threat. A universal biometric solution is not necessary in order to achieve a secure border management solution so long as countries agree to provide one another with the software necessary to decode and match the specific biometric data associated with a travel document – this approach would allow Visa Waiver Program participating countries to confirm the identity of one another's citizens. A travel document that is secured by multiple forms of biometric technologies would significantly complicate the job of a forger or impostor. Eventually the U.S. will need to employ biometrics to secure the travel documents it issues its own citizens or risk having a U.S. passport become the document of choice for fraudsters or terrorists seeking to avoid being exposed by biometric identification.
- The challenge of implementing biometric identification at land ports of entry is daunting but not insurmountable. IBG believes that portable fingerprint reading devices can be employed to capture images of the index fingers of all passengers in a vehicle in order to authenticate them with the travel documentation they carry and to check against watch lists of undesirable individuals. The capture of fingerprints must take place 'upstream' from the primary inspection station so that a biometric search can be conducted before the vehicle reaches the primary inspection position. In this way, the biometric search does

not impact the overall primary inspection time and the primary inspector is not distracted from conducting a thorough assessment of the vehicle, its occupants, and its contents.

- At exit points or other U.S. government service centers such as post offices, the government should provide a self-service kiosk that will allow exiting U.S. citizens a means for self-enrollment of their travel-related documentation and biometrics. In exchange for taking the time to scan their identity documentation (e.g., driver's license, passport, etc.) and providing a biometric sample, the U.S. citizen could use a 'Blue Lane' that would offer expedited processing when returning. The success of solutions like the SENTRI system on the U.S.-Mexico border and the U.S.-Canadian cooperative program called NEXUS shows that both U.S. and foreign citizens are willing to provide personal and biometric data to the government in exchange for the very tangible benefit of expedited border crossing. If they become widely used, these solutions could help make a dent in the rise in identity theft crimes by making it much more difficult for an identity thief to travel internationally on a stolen U.S. identity document.
- We should expect that most problems associated with biometrically secured travel documents would be of an innocent or inadvertent nature rather than a fraud attempt. It won't be a sufficient solution to just turn away at an airline counter or border post a traveler who has a problem matching a biometric sample with a travel document. The U.S. should provide travelers with a real-time problem resolution solution – a phone number or email address where they can immediately reach someone in an ombudsman-like role who can begin the process of resolving their travel documentation problems.

In summary, biometrics will play an increasingly important role in enhancing the integrity of U.S. border management systems. With clear guidelines and careful compliance with the rules of how, when, and where biometrics will be collected and employed, these tools can improve border security while at the same time protect the privacy and dignity of the legitimate traveler.

I look forward to responding to the committee's questions.