Testimony of

Philip J. Bond

January 31, 2007

Chairman Feinstein, distinguished members of the Subcommittee, on behalf of ITAA's 325 corporate members, I'd like to thank you for inviting me to share our perspective on the potential use of personal identification technology at our nation's borders. In particular, I would like to discuss technologies available to implement an exit program at U.S. land border ports as part of the U.S. Visitor and Immigration Status Technology(US-VISIT) program as administered by the US Customs and Border Protection (CBP)
Agency at the Department of Homeland Security. I'd also like to take this opportunity to thank you and this committee for taking a closer look at this important border security program.

The Information Technology Association of America (ITAA), which I am proud to have joined about six months ago as President and CEO, provides global public policy, business networking, and national leadership to promote the continued rapid growth of the IT industry. The Association plays the leading role in issues of IT industry concern including information security, taxes and finance policy, digital intellectual property protection, telecommunications competition, workforce and education, immigration, online privacy and consumer protection, government IT procurement, human resources and e-commerce policy. ITAA members range from the smallest IT start-ups to industry leaders in the Internet, software, IT services, digital content, systems integration, telecommunications, and enterprise solution fields.

The ability to record and track the entry - and exit - of foreign visitors who pass through our ports of entry (POE) is an arduous task, but not an insurmountable one. Technology is available to aid in this important mission, but let me be clear: As is usually the case, there is no simple technological fix that holds all the answers.

Generally speaking, the US VISIT program requires that the government begin tracking all visitors who are entering the United States as non-immigrants, regardless of their country of origin. They may have a visa for some specific purpose (student, temporary employment, etc.) or they may be from one of the "visa waiver" countries in which case a visa is not required. Just as it is important to keep track of when and where such visitors enter the United States, it is equally important to keep track of when and where they leave the United States. Today the specific focus of my remarks is on the exit program portion of US VISIT; the procedures under consideration for keeping track of visitors as they leave the US at our land border ports of entry.

The goals of the US VISIT program are to enhance the security of our citizens and visitors, facilitate legitimate travel and trade, ensure the integrity of our immigration system and protect the privacy of our visitors. These goals present unique challenges at our congested land borders where visitors often wait hours for permission to cross. The

good news is that information technology offers policy makers many options, especially surrounding identity authentication and verification, to help make the vision of US VISIT a reality.

That said, technology is only one piece of the puzzle. It is also critically important to focus on the processes, policies and people that make a technology effective. Most importantly, and before any exit solution can be implemented at America's borders, DHS and CBP must focus carefully on the specific, detailed objectives for the exit portion of the program. The government, and ultimately its industry partners, will have to understand which objectives are essential and which are important but less critical to achieving the overall mission. Only after conducting such an analysis, can the United States decide which of the information technology solutions available for the exit program of US VISIT offer the most benefit to American taxpayers and our foreign visitors.

Please allow me to provide a brief overview of one broad technology field that has great promise for use in identity management and border security applications. I am speaking of course of Radio Frequency Identification Technology (RFID). RFID is not a new technology; it was first used during WW II. Rather it is a proven technology that is being used in new and innovative ways beyond simple supply chain management.

RFID systems use radio waves to transmit information from tags to readers in order to identify people or things. You are probably familiar with the bar code systems so common in retail stores. Each bar code represents a unique series of numbers that identifies a particular product. A laser scanner can read a bar code and then a computer can translate it into the unique number that identifies a given product. The computer then uses the number to retrieve information from a database and display the associated product description at check out.

RFID is employed in a similar fashion, but instead of a stamped bar code and a laser scanner, RFID systems use a radio frequency tag (transmitter) and a reader (receiver). Each tag includes a microchip to store information and an antenna to transmit that information over radio waves. A reader can then pick up that radio signal. In order for the RFID tag to be read, it must be transmitting on the same radio frequency as the reader. Different types of RFID tags use different radio frequencies, thus allowing for the short range (proximity) or long range (vicinity) transmission of information.

I want to focus today on those two basic types of RFID systems, both of which are widely used and commercially available. Proximity-read RFID systems contain a secure chip with advanced computing powers and are the technology at work in so-called "smart cards." Smart cards require a user to swipe them across a reader or come in close proximity to a reader. These cards are commonly used today as keys to buildings or computer systems. With their advanced computing powers, they are very good at authenticating a given user; that is, ensuring that the person using the card is indeed the person whom he or she claims to be. Smart cards can also contain not just a coded set of numbers like those contained in bar codes, but also digital files containing personal information, an ID number, an address or phone number, a digital photo image or even a digital fingerprint image. Smart cards are used for many federal government credentialing programs

including those under the authority of Homeland Security Presidential Directive 12 (HSPD-12), the Transportation Worker Identification Credential(TWIC) and the DoD Common Access Card (CAC).

Alternatively, ultra high frequency (UHF) or vicinity-read RFID systems have a longer read range - a maximum of twenty to thirty feet. They are frequently used for asset tracking and inventory control, but they can have many other applications, including identity management. In identity management applications, vicinity-read RFID technology normally transmits a unique identifier to a secure database where actual personal identifiable information is stored. The RFID card/tag itself contains no personal information, only the unique identifier. This is done to ensure that no personally identifiable information can be skimmed off the transmission from the card to the reader. The federal government is already using this type of technology in several trusted traveler programs at the border like NEXUS, FAST, and SENTRI.1 Additionally, the regulations proposed by the Department of State for the Western Hemisphere Travel Initiative call for vicinity-read RFID technology. This type of RFID system is very familiar to anyone who has experience with the EasyPass automated toll collection system in use along the East Coast (e.g., the Delaware Turnpike) and in the Washington area to collect highway tolls.

For this hearing, I was asked to discuss whether technology currently exists that can verify the identity of a foreign visitor leaving this country, as mandated by Congress.
The short answer is yes; both proximity and vicinity read RFID technologies can help accomplish this task. I have to quickly qualify my answer, however, to say, "It Depends." The fact is that each of these technologies has both benefits and shortcomings that designers of the automated entry and exit system will have to take into account.

As a baseline, consider a border without any RFID technology: To verify the identity of foreign visitors upon exit, DHS could simply build multiple exit lanes, stop every vehicle and person leaving the land border, and use available techniques to authenticate and verify documents presented by foreign visitors. Other security measures could be added by using the numerous types of biometric authentication technologies available (iris scans, fingerprints authentication, etc) and compare them with information gained when the individual first entered the US.

As a step up, DHS could issue all US VISIT applicants a Form I-94 credential upon entry. This credential could be a proximity read RFID smart card, similar to the epassport
or HSPD-12 compliant cards, which are highly secure and can encrypt any information that is transmitted. Visitors would then authenticate their identity upon exiting the border by going through a reader station. Additional CBP officials located at exit stations could visually verify that the person exiting matches the person whose identity is recorded on the card. Additional technology could be added to improve the system. For example the system could provide thumb print readers next to the smart card readers so that a visitor leaving the country could swipe his or her card and then place a thumbprint on the reader to provide a biometric match on the card. This would eliminate some of the visual inspection noted above. All of this could be implemented to achieve 100% compliance, but this too would require that traffic be stopped and individuals get out of their cars and buses to present their electronic credentials in close proximity to a reader and be visually cleared.

All of these solutions require significant investment in infrastructure and the stopping of traffic at the nation's land borders. The feasibility of creating new delays at the border is questionable when one considers the enormous volume of border crossings, numbering in the millions of individuals each day2. This may not be the best way to facilitate legitimate travel and trade. On the other hand, stopping traffic to inspect travelers' documents may still be the answer if 100% authentication and compliance is the only acceptable outcome. Still, by the time new exit facilities with multiple lanes are built, technologies that today are in development will most likely be ready for adoption, leaving only an antiquated system to protect our nation's land borders.

All of the options that I have mentioned so far would require significant investment in personnel and infrastructure. For example, land border points of entry (POE) would need to be expanded to accommodate larger exit lanes outfitted with reader technology. DHS would need to perform a cost/benefit analysis to see if this type of technology would meet the business requirements of the US-VISIT program.

There is another option: Vicinity-read or Ultra-High Frequency (UHF) RFID technology could also be used at the border placed in an I-94 credential. Multiple credentials could be read as vehicles slowly go through reader stations. As with any type of exit program, some visual inspections would need to occur. Like the other options I have discussed there will need to be an investment in infrastructure. Unlike the other options, it would keep the traffic moving and would align with existing trusted traveler programs at the border. However, the current generation of UHF solutions, like existing smart card products, do not independently tie a person to an ID card through biometrics without human intervention to examine a photo and match it to the person's face. The limitation of vicinity read RFID technology when applied for this purpose is that it only proves that an I-94 form left the country, which of course is not the same thing as proving that an individual left the country.

I am aware that there was a pilot program using UHF for the US VISIT exit program and that the results were not good. ITAA was not part of that program, so I am not fully conversant with the testing and results. However, I do know that the UHF technology works. The government is using such systems for several trusted traveler programs at the border, and they have proven to facilitate travel while authenticating traveler identity.

Furthermore, there is technology on the horizon that will combine biometric authentication with long range radio frequency transmission. For example, technology now under development will require a person to activate their credential by placing a thumb on the device. The credential will then verify the user's identity by authenticating his or her thumb print and unlocking the credential's unique identifier for transmission to a reader.

Given the special challenges of avoiding compounding congestion and delays at our nation's land-border crossings while controlling the entry and exit of visitors, it may very well be that vicinity-read RFID technology holds the most promise. By implementing this type of technology through a phased approach, DHS could achieve a high-level of compliance without delaying the flow of traffic. DHS could begin by using the technology available to collect useful exit data on foreign visitors, encourage them to

comply through education programs and support the endeavor with the right policies and training. Then, as new classes of RFID solutions come on line that support higher levels of authentication and compliance, those technologies can be integrated into the existing infrastructure with relative ease. In this way, the government can realize some benefits on behalf of the American taxpayer in the near term while increasing the dividends of security and commerce in the future.

Before concluding, I would like to very briefly discuss legitimate concerns about protecting individuals' privacy at the border. Either version of RFID technology can be a part of a secure solution. UHF technology is sometimes branded as inherently insecure but that claim does not hold up to scrutiny. For example, in DHS's NEXUS and SENTRI programs, the registered traveler ID cards do not transmit any private information about the cardholder. They only transmit a random serial number that is meaningless until it is matched in a secure database to a particular individual. Therefore, it is useless to any unauthorized individual. In the 10 years that these programs have been in operation, I am not aware of a single case of identity theft. The US-VISIT pilot program followed the same model, and it is my understanding the Western Hemisphere Travel Initiative will do the same. So I think the American people should be reassured that their personal information is not going to be put at significant risk in these programs.

In closing, it is crucial that we begin to implement the US VISIT exit program and that we do so with clear, realistic and prioritized objectives in mind. With the help of the private sector, the government can fully realize the vision of the US VISIT program over time. It is really a question of how and when rather than if we will accomplish this mission. Thank you again for the opportunity to testify before the subcommittee today, Chairman Feinstein. I would be happy to answer any questions that you or members of the subcommittee may have.

1 NEXUS - Canadian Border Dedicated Commuter Lane. The project of the Canada-United States Shared
Border Accord, designed to facilitate pre-enrolled, low risk, vehicular traffic across the Canadian and United States border. SENTRI - Secure Electronic Network for Traveler's Rapid Inspection. The system that provides an
electronic, dedicated commuter lane that expedites the flow of low-risk, frequent border crossers across the
southern border. Sensory system is based on RFID technology.
FAST - Free and Secure Trade. The program that provides dedicated commercial lanes for expedited processing to qualifying commercial participants. Sensory system for FAST is based on RFID technology
http://www.dhs.gov/xlibrary/assets/foia/US-VISIT_RFIDattachB.pdf

2 U.S. Customs and Border Protection Fact Sheet.
http://www.cbp.gov/linkhandler/cgov/newsroom/fact_sheets/typical_day.ctt/typical_day.pdf
6-6