Testimony of
William T. Alsbrooks
Great Bear Solutions Group

Before the U.S. House of Representatives Committee on Oversight and Government Reform, Subcommittee on Government Management, Organization and Procurement

Wednesday, June 25, 2008 2:00 p.m.
Rayburn House Office Building Room 2247

Chairman Towns, Ranking Member Bilbray, and other distinguished members of the subcommittee – I thank you for the invitation to appear before you today to provide my assessment of the card security features of the new US Department of State B1/B2 Visa Border Crossing Cards.

A quick background: I retired from General Dynamics Information Technology in the fall of 2007 and today I run my own consulting firm, Great Bear Solutions Group. In the interest of full disclosure, I have served as a paid consultant to both OVD Kinegram and Lasercard. For almost 20 years, I was the Vice President in charge of the Credential Technology Group. Since 1995, my group deployed over 40M secure ID cards of all types containing the most sophisticated security features known.

The Border Crossing Card (BCC)

Keep in mind that the Department of Homeland Security has stated that RFID infrastructure will be deployed to only 39 Ports of Entry. Even at those sites, there will be times where; readers will fail, card antennas will fail, databases will go down, and power will not be available. BCC cards will also be used for identification not just at the border crossings but also in the interior of the United States where there will be no readers.

Given that, it is important to understand the following:

1. ID cards with national security implications such as the BCC and Passport Cards must provide for reliable face-value visual authentication in the absence of machine readers and specialty card reading tools.

2. Card features that require special readers to check for covert or forensic features such as magnifiers, ultra violet or infra red lights or special lens, are of little to no value to a tier one inspector. If a secure ID card cannot be visually authenticated with an unaided eye it is poorly conceived and easily compromised.

3. A reliable secure "flash pass" that can be visually authenticated with the unaided eye is available today. Unfortunately, the card that I have been asked to assess and that the Department of State intends to deploy is not that card. Deployment of that card will effectively "lower the bar" on ID card security for this generation of cards, which I believe poses a grave threat to our national security.

The most durable, secure and tamper-resistant card available for the American public is the card that has been developed for the new Permanent Resident "Green" Card. This advanced technology card incorporates all of the security features specified for the Border Crossing and Passport Cards – including the RFID chip – however, it is significantly more reliable on face-value inspection because of the inclusion of the latest "state of the art" laser-engraved optical security stripe.

This card is *self-referential* – meaning that the laser engraved photo and name on the front and back of the card can be *referenced* to verify each other. It contains high resolution images which function at a forensic level and also offer unsurpassed visual authentication when using only an unaided eye.

The specifications for the Passport Card and new Border Crossing Cards are the same– just different artwork and optical variable device (OVD).

Let me explain why I believe that the features in the proposed new cards aren't "good enough" to rely on for a "secure flash passes":

The new card specifications do include overt, covert and forensic features. However, they rely on security features most commonly associated with currency, such as: security printing, (guilloche, micro line, moiré, and rainbow printing), traceable particulates, scrambled indicia, and optically variable inks. Most of these features require the use of specialized tools or access to lab equipment to validate the card's authenticity. As a result, these features are frequently simulated in counterfeit currency world-wide.

It is the nature of the secure document business and in the best interest of the American public that the best of breed proprietary single source technology be utilized in secure ID cards so that components of our most valuable national documents are not easily obtained by criminals. Most of the technology that has been specified for the new card is sole-source proprietary technology. The OVD Kinegram was chosen by the State Department and separately sole-sourced. The artwork is done on a proprietary software product. The color-changing inks are single sourced. If scrambled indicia is used – it is a proprietary technology. Any type of traceable particulate or security thread will be proprietary and require proprietary readers. Although we are not talking about paper in this case – it is commonly known that all US currency is printed on CRANE paper. The optical security stripe is a proprietary single source feature. I believe it offers a solid and unique security benefit.

For visual authentication of the new cards - the Department of State has "bet the whole farm" on the security of the laser engraved personalization and the OVD Kinegram.

Laser Engraved Personalization

Laser engraving is not new technology, it is not unique nor is it difficult to duplicate. It is also not impossible to alter. I have been using laser engravers since we first produced the Canada Permanent Resident Card in 2002. I believe that it is the best choice for this application and it should be used on these cards. However, it is not a feature that is going to stop an accomplished counterfeiter. Laser engravers are readily available, affordable for low volume counterfeiters, and can be purchased on EBay.

Optical Variable Device

OVD Kinegram produces an extraordinary optical variable device. It is a unique combination featuring both metalized and transparent materials – it has horizontal and vertical movement – color diffractive light shifting and multiple images. My group has used Kinegrams since 2002 and I recommend that the Kinegram remain on these cards. It is the best of its breed in the world.

"All that glitters is not gold" and sophisticated holograms both authentic and counterfeit are now widely manufactured and readily available world-wide. Technology to produce holographic devices is not closely held. Unfortunately, it is a feature that can be simulated and will not stop an accomplished counterfeiter.

It is important to note that the Kinegram feature is not individual specific – they are visually all alike - once the OVD has been compromised, a simulation can be mass produced.

Also of great concern to me is the fact that the Kinegram can be removed from a real card intact and reapplied to a counterfeit. Even though the current plan is to embed the OVD under the top layer of the card, it can be readily separated using heat and a knife, or any of a number of solvents which can be purchased at a local drug or hardware store. Again, any accomplished counterfeiter will have no problem doing this as soon as he gets his hands on an authentic card.

Optical Security Stripe

Today's "state of the art" laser engraving is actually being done utilizing optical stripe security. This technology does constitute a huge obstacle to counterfeiters.

The new Border Crossing Cards should continue to include an optical stripe - only then can the Department legitimately claim to be issuing the most "durable, secure and tamper-resistant cards available to the American public".

There are two distinct components to the overt features on the new optical cards. First, common images like portraits or statues that can be seen clearly with the naked eye – yet retain their detail and integrity under 400 power magnification.

Second, each optical stripe is now 24mm in width and is uniquely personalized with a larger much clearer digital photograph and with the biographical data of the card holder. The image is permanently burned into the optical media with a laser into the core of the card. It can be destroyed but it cannot be altered.

These features have been designed in close consultation with forensic and intelligence officers from the DHS/ICE Forensic Document Laboratory and represent an enormous challenge to any level of counterfeiter – including those state sponsored.

In accordance with the Illegal Immigration Reform and Immigrant Responsibility Act of 1996 (IIRIRA), the current BCC contains a fingerprint biometric stored in the optical stripe which can be validated in a matter of seconds. The specification for the new BCC cards, however, does not include a fingerprint biometric and will instead rely on visual comparison to the digital photograph. Visual comparison of a photo retrieved from a data base by an inspector does not constitute the functional equivalent of a fingerprint biometric verification.

Without question, the optical security stripe is the most demonstrably secure overt feature available for secure ID cards. The optical stripe can easily be added to the new cards currently specified for the Border Crossing Card and Passport Cards. If it were - inspectors would then be able to rely on the visual authentication of the document. The digital photo and biographical features on the face of the card would be rendered relevant and unaltered by simply referring to the optical media on the reverse side. My colleagues and I refer to this card as a "self-referential – reliable flash-pass".

Thank you for your time. I will be pleased to answer any questions.