usacm ACM US Public Policy Council

June 3, 2011

Kim Hildred
Staff Director
Subcommittee on Social Security
Committee on Ways and Means
U.S. House of Representatives
B-317 Rayburn Building
Washington, D.C. 20515

Dear Ms. Hildred:

Thank you again for the opportunity to have Dr. Antón testify before the Social Security Subcommittee on April 14, 2011. In response to the questions in the Subcommittee's letter of May 17, 2011, we include the following responses. The questions are in **bold text**. Should you have any additional questions, please contact me at 202-659-9711.

1) In your testimony you advise against relying on single factor authentication, such as biometric, to identify a person because it makes the factor a target for theft and manipulation. The Department of Homeland Security is beginning a pilot project with the State of Mississippi that will allow an employer to match an employee's driver's license against the state's database. Is this a promising idea if used with another authenticator, and if not, why?

If "another authenticator" means another verified form of ID, then the Mississippi pilot seems to be a promising idea, because it would increase the effort required to commit identity fraud, and it would also increase the chances of such fraud being caught. However, there are still a number of potential problems with the proposal.

The driver's license is only as strong as the system a state uses to verify identity when granting drivers licenses. If a "good enough" false ID is used successfully to obtain a driver's license and that license is then used as the "another authenticator" then the system will be no more effective at verifying identity than it would be if only the single false ID was presented. A false driver's license coupled with knowledge of a matching Social Security number is often sufficient to obtain any number of otherwise legitimate secondary authentication documents. This has happened in other states, so it could be a problem in Mississippi, but we are unfamiliar with the specifics of their particular system.

Besides the possibility of issuing false licenses based on "breeder" documents that are suspect or obviously forged, the driver's license system in Mississippi (and in other states) may be subject to insider misuse. Employees who have access to the system might insert fraudulent records or grant licenses that are entered into the system by mistake or because of bribes. Several years ago there was one instance where the staff of a driver's license bureau in Virginia was making falsified licenses and entering them into the state computer system, no questions asked, in return for payment of (rather paltry) bribe.

Another potential problem with this system is that not everyone who is a resident in Mississippi and who will need to have their employment verified will have a driver's license in Mississippi, or a valid 2nd authenticator. Individuals who are unable to drive for reasons of health, disability, economic necessity or simply choice may not have a drivers license or state-issued alternative. The pilot project should not exclude them.

On a related note, there is the possibility that someone may not be able to present his or her documents for verification because of exigent circumstances: consider the many people in southern states, including Mississippi, who have lost all their records recently in tornados and floods. This would not only make it difficult for them to verify their employment, but it might make it difficult or impossible for them be (re)issued a drivers license if the system is not designed with these possibilities in mind. In some states a person must show some ID to obtain a duplicate of an issued driver's license - a clear problem for people in disaster zones.

Of course, employers who falsify E-verify results in some way or fail to closely examine the presented documents will also continue to be a potential weakness.

Although a program connecting a driver's license match with a 2nd authenticator is a promising idea, and may well be more accurate than current practice, weaknesses in the implementation of the system will likely continue. There are clear opportunities for fraud in use of E-Verify even with such a program, but too strict a set of restrictions on proper authenticating documents may well deny employment access to some people with legitimate authority to work. How frequent those instances will be in practice is impossible for us to quantify in advance.

2) Please outline the security of state driver's license systems and the degree to which the risk of document fraud for REAL ID compliant licenses has been reduced.

There are many different systems for driver's licenses, and we have not studied the specifics of their security features and mechanisms. However, many of the REAL-ID features are intended to reduce document fraud by making the physical licenses more difficult to modify or forge, providing mechanisms that may be used to more strongly authenticate the identity of the holder, and to require uniform documentation for obtaining licenses.

To the best of our knowledge, REAL-ID compliant licenses are more difficult to forge or alter than their predecessors. However, this is simply a matter of cost and technology, and eventually forgeries will appear (if they have not already).

The machine-readable features intended to more strongly authenticate the identity of the holder are only as good as the entity conducting the authentication. If someone does not have a 2-D barcode reader, or does not carefully match picture against person, then the extra features in the license are of no extra value than most older licenses.

The process of applying for licenses continues to be a weakness because of significant amounts of identity theft, forgery and other identity-related crime. Individuals are likely still able to present false documents with valid Social Security numbers and other data to obtain a license that is not a match to their real identity. In a REAL-ID compliant state the documents will be imaged and stored, but that will not prevent the license from being issued. Given the pressure for these licenses, the market for valid forged documents to use in applying for a license will undoubtedly develop. If license personnel are careless or criminally complicit that will only compound the problem.

As noted above, there may be people who will have difficulty obtaining a REAL-ID compliant license because of the loss of documents. A mechanism must be in place for these people to obtain IDs. However, that same system will be ripe for abuse by some individuals wishing to do so. We have seen stories of criminals who joined displaced people from Hurricane Katrina claiming to have lost all their possessions so as to establish new identity documents with no criminal record.

In 2007, the Data Privacy and Integrity Advisory Committee to the Secretary and the Chief Privacy Officer of the Department of Homeland Security issued 12 recommendations for enhanced privacy and security of REAL-ID cards (DPIAC Report 2007-01) to be included in the final rule for REAL-ID. None of them were adopted. USACM has provided comments and briefs over the last 6 years on REAL-ID on the privacy and security challenges of the program. These challenges go beyond issues related to fraud.

3) To obtain a passport or other authentication, one needs a certified birth certificate. However, is the system for obtaining copies of a valid birth certificate protected from fraud within most states?

This is not a topic we have studied. However, from the personal experience of committee members both obtaining a birth certificate and successfully forging one are not difficult tasks in several states, and we suspect that forging or altering a birth certificate from most states are also not difficult. Many birth certificates were, historically, forms that were simply filled in by hand or typewriter. Certified copies were either retyped, or later, photocopied, then stamped or embosed (or both). These kinds of documents are not difficult to forge or alter.

For example, a certified birth certificate one of our members used to obtain his passport had an official stamp and a hand-embossed seal, which was the standard up until recently in many states. The stamp could be recreated on a computer printer in a matter of a few hours, and then run off onto a manual stamp for use with an inkpad. The embossed seal is of the same size and shape as those used by notaries or for marking library books. A little work with carving tools, wax, and pewter would result in a new embosser good for making several hundred counterfeit certificates using aged paper.

Obtaining birth certificates is not difficult in many places. Clerks are often busy and may not be required to ask why a copy is requested. In others, presenting a fake driver's license or other ID in the name of certificate (or a relative) is sufficient justification; when ordering by mail a photocopy of those false IDs may be all that is necessary. As an example, documentation at <http://www.state.nj.us/health/vital/jerseycity.shtml> indicates a case where existing birth certificates are no longer accepted (likely because of fraud), and a link is provided describing how to order a certified birth certificate by mail.

If you have any additional questions, please do not hesitate to contact me.

Regards,

Cameron P Wilson

Cameron Wilson
Director of Public Policy
Association for Computing Machinery