Center for Immigration Studies

Backgrounder

April 2009

The Appearance of Security

REAL ID Final Regulations vs. PASS ID Act of 2009

By Janice Kephart

Partial adherence [to AAMVA's 2004 DL/ID Security Framework] may cause more harm than good, providing the appearance of security where in fact security does not exist.

— AAMVA DL/ID Security Framework (February 2004), p. 8

Introduction

The move toward more secure issuance of state identification documents may be in jeopardy. The most recent iteration of the National Governors Association secure ID bill circulating the Senate for signatures for possible introduction, the "Providing for Additional Security in States' Identification Act of 2009" or PASS ID Act, gives the appearance of security for drivers licenses and non-driver IDs (DL/ID) when, in fact, security does not exist. The PASS ID Act would provide for insecure issuance practices by the states that, for the most part, were in place prior to 9/11. In many ways, the PASS ID Act is a step backward for most states, or at least an endorsement of the status quo, because nearly all states are implementing elements of the REAL ID Act[1] — the 2005 measure designed to raise state ID standards in response to the 9/11 attacks — even in states that have passed legislation that precludes REAL ID implementation. However the new bill's mandate to verify an ID applicant's legal presence in the United States by 2013 is voluntary, as any state can opt out of PASS ID Act requirements.

In addition, the proposed bill pulls back on nearly all key recommendations included in the American Association of Motor Vehicle Administrators' 2004 *AAMVA DL/ID Security Framework*,[2] while undoing or leaving unanswered issues already resolved through the arduous comment process that led to the 2008 REAL ID regulations in operation today. In addition, the PASS ID Act leaves the 9/11 Commission secure ID recommendations in the dust, setting minimum standards that the 9/11 hijackers could easily have bypassed. In essence, the PASS ID Act creates an atmosphere where an applicant's identity *du jour* can pass muster and be issued a legitimate drivers license/ID with a "unique symbol" indicating the issuing state has complied with federal DL/ID issuance standards. This ID would then have expanded use, enabling not only access to federal national security facilities, boarding commercial aircraft, or entering nuclear power plants, but also for use in establishing identity for employment with programs such as E-Verify.

The PASS ID Act would have a result for state drivers license issuance similar to that uncovered by the March 2009 GAO report[3] revealing the poor vetting processes for U.S. passports, weaknesses that enabled government investigators to acquire fast-track U.S. passports based on phony Social Security and residence data, illegitimately obtained drivers licenses, and stolen birth record information.

In contrast to the current REAL ID Act regulations now in effect, the PASS ID Act would:

- Create new rulemaking that would not be completed for at least a year from enactment, leaving unclear the status of current REAL ID rules;

Janice Kephart is Former Counsel to the 9/11 Commission and Director of National Security Policy Center for Immigration Studies.

- Duplicate grant-making, leaving unclear the status of current REAL ID grant-making; and

- Push full compliance out until 2021, 20 years after 9/11 and four years past REAL ID.

The PASS ID Act does not repeal REAL ID, but instead replaces its substance by deleting identity verification and document authentication and replacing them with what is, for the most part, the status quo in most states, or standards that are less rigorous than those now in place. Certification that a state has complied with federal standards would not require a security plan to protect data or to protect against corrupt employee access to private data or production facilities. Moreover, there is no requirement that any state comply with the proposed law; state laws would pre-empt the PASS ID Act. If a state does choose to comply, there is little it has to do to prove compliance. For states well on their way toward REAL ID compliance, a simple letter from someone in the state (the bill even leaves the issue open of *who*) claiming compliance and seeking compliance certification from the DHS Secretary may be sufficient to have all licenses and IDs issued receive a federal stamp ("unique symbol") of approval.

There is no requirement to electronically verify date of birth, Social Security number, or lawful residence status — merely that questions be resolved with "appropriate action." Known weaknesses such as those used by the 9/11 hijackers — such as multiple licenses or IDs in different states and use of a single document to show principal residence — are either pushed into demonstration projects for the next six years (the one driver/one license rule) or returned to pre-9/11 requirements (proof of residence). The proposed bill would likely lead to increased identity theft and license shopping.

AAMVA DL/ID Security Framework

In February 2004, the American Association of Motor Vehicle Associations (AAMVA) released to their membership a 36-page *AAMVA DL/ID Security Framework* agreed upon by all North American Motor Vehicle Associations (MVAs). The *Framework* resulted from a two-year review by a special task force that covered all aspects of drivers license/ID issuance in the wake of the 9/11 attacks. The executive summary describes the purpose of the *Framework:*[4]

The license is now readily accepted as an official document for both licensed drivers, and, in most jurisdictions, for non-drivers. The Motor Vehicle Administrations (MVAs) who issue these documents have unique, continuous, and long-lasting contact with most of their constituents from the individual's teenage years onward....

This document provides minimum standards of security, interoperability, and reciprocity agreed upon by all North American MVAs regarding drivers license/identification card (DL/ID) issuance. Each MVA shall:

- *Either meet or exceed the requirements of the* Security Framework *based on risk analysis and resource availability.*

- *Determine that all individuals granted a DL/ID "are who they say they are."*

- *Ensure that each individual issued a DL/ID "remains the same person" throughout subsequent dealings both with itself or any other MVA.*

Simply expressed, this means:
One driver/identity;
One license document; and
One driver control record

throughout an individual's lifetime. Only a systematic and thorough approach ensures that minimum security standards and practices are met in each jurisdiction. ***Partial adherence [to AAMVA's 2004 DL/ID Security Framework] may cause more harm than good, providing the appearance of security where in fact security does not exist.*** [emphasis added]

Proposed PASS ID Act Changes

Below is a review of how the proposed PASS ID Act would change current REAL ID regulations currently in effect. This analysis is based on a legal summary of the REAL ID regulations I released in February 2008, "REAL ID Final Rules: A Summary,"[5] compared to a line-by-line analysis of the proposed PASS ID Act. The boxes contain AAMVA's DL/ID Security Framework recommendations.

Compliance

- States that issue non-compliant DL/IDs need not delineate (with a marker) these DL/IDs from compliant cards for federal purposes, ensuring confusion for those determining acceptability of documents for federal purposes
- Deletes benchmarks and timetable for compliance
- States may file a justification for noncompliance and receive an extension
- State laws pre-empt the PASS ID Act, including privacy laws
- Pushes off compliance for use of electronic verification of lawful status (via the Department of Homeland Security's SAVE Program) until January 1, 2013
- Deletes states' submission of a Security Plan by February 11, 2011, to support certification of compliance

AAMVA Requirement #9: Wherever possible, all jurisdictions shall electronically verify the data elements required for drivers license/identification card issuance with the originator of those data elements. … Whenever possible, the information on the documents should be verified directly with the source document issuing agency (e.g., Social Security Numbers should verified with the Social Security Administration [see Appendix "10-6.3-03 Social Security Number Verification Best Practices"], immigration documents should be verified with the U.S. Bureau of Citizenship and Immigration Services). Other data elements, such as an address, should be verified with the U.S. Postal Service or through a third-party vendor.

Identity Verification and Document Authentication

- Overall language change
  - Deletes "The applicant must provide sufficient documentation for a state to both verify identity and authenticate documents presented for the purpose of establishing identity."
  - Deletes requirement that electronic verification of identity information with the issuing agency be conducted whenever possible
  - "Verification with issuing agency" and "document authentication" no longer necessary; instead, states are to "take appropriate steps" to "validate" information presented
  - Deletes list of acceptable verifiable documents

AAMVA Recommendation #5: All jurisdictions should not grant a photo drivers license/ identification card to an undocumented immigrant.

- Lawful presence checks
  - Pushes off by two years (until January 1, 2013) use of the lawful presence database SAVE by states, if a state chooses to comply
  - SAVE need not be used for those claiming U.S. citizenship
  - States have free access to SAVE, if used
  - If a non-match in SAVE, state not prohibited from issuing DL/ID

AAMVA Requirement #8: All U.S. jurisdictions shall use the Acceptable Verifiable Resource List for the United States and follow all associated procedures.

  - No listing of acceptable documents to prove U.S. citizenship or identity and a photo ID is not required if it includes a person's legal name (full legal name not required) and date of birth
  - Makes no reference to the Memorandum of Understanding entered into in 2008 between the State Department and Department of Homeland Security (DHS) to make U.S. passport information available to DMV for U.S. citizenship checks

AAMVA Requirement # 13: The best unique personal identifier currently available is a framework of cross-verified data elements, especially a person's name, date of birth, and Social Security Number (U.S.). These data elements must be collected as unique identifiers from the documents on the approved list of acceptable verifiable documents.

- Social Security number checks
  - No requirement for a state to use the Social Security Online Verification (SSOLV) database

- Deletes requirement that applicant provide a Social Security number, only needing to "take appropriate steps to validate" the number if the applicant "has been issued a Social Security number"
- Existing procedures for resolving non-matches adequate
- States have free access to SSOLV, if used

- Date of Birth Checks
  - Deletes listing of acceptable documents to prove date of birth
  - Deletes requirement that states verify birth certificates through the Electronic Verification of Vital Events (EVVE) system, as it becomes available (13 states have digitized their birth records to date, and three are sharing information for DMV applicants). A 9/11 Commission recommendation made law in the 2004 Intelligence Reform and Terrorism Prevention Act, Section 7211, "Minimum Standards for Birth Certificates."[6] The law requires states to certify they are in compliance with HHS standards on birth certificate issuance and prohibits any federal agency from accepting a birth certificate for official purposes that does not comply with federal standards.
  - Deletes requirement that DL/ID not be issued until resolution with issuing office if there is a non-match or a document does not appear authentic

- Principal Residence Checks
  - Deletes proof of principal residence with two documents of state's choosing, requiring only "documentation showing the person's name and address of principal residence." This weakness was exploited by the 9/11 hijackers.

- One Driver/One License
  - Deletes requirement that state "make reasonable efforts" to ensure that applicant does not have more than one DL/ID under a different or same identity in state where applying, or has been issued a DL/ID in another state. This weakness was exploited by the 9/11 hijackers.
  - State only needs to "take appropriate steps" to determine that applicant has terminated a prior DL/ID in another state
  - Sets up a demonstration project in place until 2015 limited to determining whether "an applicant for a drivers license is not currently licensed in another state," precluding interstate exchange of information until at least 2015

- Applicant Processing
  - Facial image need not be captured until after submission of application, permitting "MVA shopping"
  - Deletes requirement that applicant supply full legal name

AAMVA Requirement #10: The name is a critical data element used by jurisdictions to collect, record, store, display, and match identification data. To ensure uniformity and accuracy, the complete name shall be collected upon initial application.

  - Deletes applicant declaration that information presented is true and correct under penalty of perjury

  - Retains eight-year validity for DL/IDs, but doesn't begin compliance period until 2013, pushing back full compliance until 2021. REAL ID would achieve compliance by 2017, saving four years — 20 years after 9/11 — until full compliance is achieved.

- Reissuance
  - Deletes provision to set forth procedures to verify identity for the purposes of reissuance so that the same individual who originally applied receives the reissued ID (designed to reduce ID theft)

Tamper-Resistant Cards

AAMVA Requirement #12: To provide a common security protocol for all jurisdictions, the AAMVA Card Specification provides minimum card security specifications in the following threat areas: counterfeit/simulation; alteration/forgery; cannibalization (using parts of cards together); photo/signature substitution…. The AAMVA Card Specification provides criteria to use … in a layered and structured application…. Levels of security are defined as:

- Level 1, first line — inspection visible to the human eye or apparent to touch
- Level 2, second line — inspection requiring the use of a tool or instrument (e.g. magnifying glass, UV light)
- Level 3, third line — inspection requiring higher level of inspection (e.g., microscope)

[Eleven benefits of having a common security protocol are then listed.]

- Hardened DL/ID Cards
  - Deletes level 1 (requires an "easily identifiable visual or tactile feature" for cursory examination without aids), level 2 (feature detected by "trained inspectors with simple equipment") and level 3 (feature only detectable by forensic inspectors) security features, instead calling for a "combination of security features designed to protect the physical integrity of document including… prevention of… fraud"
  - Deletes requirement that states not use technologies commonly available to the general public and to counterfeiters
  - Deletes requirement that states submit a report indicating a card's ability to deter and detect forgery and counterfeiting, or that DHS reserve the right to conduct independent forensic analysis of DL/IDs

AAMVA Requirement #12: All jurisdictions shall follow the "Personal Identification — AAMVA International Specification — DL/ID Card Design." … Commonality in card design is necessary to simplify comparison of data elements and enhance reciprocity. There are hundreds of card variations across North America, which creates confusion, hampers recognition, and authentication of genuine documents, and prevents detection of fraudulent DL/IDs by LE and other users.

- Surface Requirements for DL/ID Cards, and MRZs (Machine-Readable Zones on Documents)
  - Full legal name not required, nor required to match identity documents
  - Digital photo need not meet ICAO (International Civil Aviation Organization) standards
  - Signature need not comply with AAMVA standards
  - Deletes data elements: date of transaction, expiration date, state/territory of issuance
  - Deletes ICAO standards in display of information on card

AAMVA Requirement #12: The AAMVA Card Specification describes a common design and physical layout for DL/IDs where each data element is prescribed a zone on both the front and back of the card. Data elements appear on the card in both human and machine-readable formats.

  - MRZs:
    - Need not adhere to any standard
    - Deletes standard data elements for inclusion on face of card such as inventory control number or state card design revision date
    - Precludes federal regulation to "require a single design or numbering system to which DLs/IDs issued by all states must conform"

System and Personal Data Security

AAMVA Recommendation #1: Each MVA should create a Risk Assessment Plan for those document issuing systems and then implement appropriate document fraud prevention and detection systems, as given in the white paper, to minimize both employee and customer fraud.

- Standards for Data Storage
  - Deletes requirement that states certify they have a decurity plan covering (1) physical security of production facilities and storage areas for card stock and production; (2) compliance with Drivers Privacy Protection Act; (3) securing physical features of DL/IDs; (4) securing biometric use; (5) standards for document retention and destruction; (6) standards to prevent "unauthorized access, use, or dissemination of applicant information and images of source documents."

AAMVA Recommendation #8: All jurisdictions should provide for data sharing between law enforcement and motor vehicle administrations including, but not limited to, exchanges of digital photos and driver records.

  - Deletes requirement that digital images be stored in a manner interoperable with other states' photo capture and law enforcement use
  - Deletes requirement that document and signature images be stored under standards interoperable for law enforcement use

- Employee Background Checks
  - Deletes employee background checks

AAMVA Requirement #1: Each MVA shall use the "AAMVA Fraudulent Document Recognition (FDR) Model Training Program" (FDR Training Program) in employee training programs for document fraud. The program addresses paper, laminated, and plastic government identification documents.

  - Deletes employee fraudulent document training
  - Deletes encouragement to use E-Verify in hiring of employees
  - Deletes control of employee access to information or DL/ID production

Add-ons

- Criminal Code
  - Criminalizes trafficking in *stolen*, not just *false*, authentication features
  - Aviation watchlists are to add convictions for use of a false DL at an airport

- Grant Program
  - Adds another state grant program in addition to REAL ID based solely on numbers of DLs or IDs produced by the state during the year grant applied for and assures all states receive a minimum grant (note*:* most recent grant issuance in December 2008 under REAL ID did just that, see table in my blog, "Secretary Chertoff's Stocking Stuffer: States Get Infusion of Secure ID Monies")[7]
  - Does not require states to account for monies allocated, nor provide oversight to DHS for use of monies

9/11 Commission Recommendations

At the foundation of the 9/11 Commission "terrorist travel" recommendations on secure IDs was the basic understanding that terrorists will continue to embed themselves in the United States as long as identification and identity document-issuance processes are easily manipulated. The Commission stated:

> *All but one of the 9/11 hijackers acquired some form of U.S. identification document, some by fraud. Acquisition of these forms of identifications would have assisted them in boarding commercial flights, renting cars, and other necessary activities.*
>
> ***Recommendation:*** *Secure identification should begin in the United States. The federal government should set standards for … sources of identification, such as drivers licenses.*
>
> ***Recommendation:*** *The President should direct the Department of Homeland Security to lead the effort to design a comprehensive screening system, addressing common problems and setting common standards with system-wide goals in mind.*[8]

As the 9/11 Commission noted, there was only one 9/11 hijacker who did not obtain some form of U.S. identification, whether a state-issued drivers license, personal ID, or both. Three of the five hijackers who attacked the Pentagon used fraudulently obtained licenses to board. The terrorist pilot of that plane had four IDs, all from different states, with at least one obtained by fraud. And if REAL ID had been in effect in 2001, the 9/11 operational ringleader and pilot of the first World Trade Center plane, Mohamed Atta, would only have been four days from an expired license when he was pulled over for a speeding violation on July 5,

2001. It may, too, have been that the Pennsylvania pilot, Ziad Jarrah, when pulled over for speeding two days prior to 9/11, would have been discovered holding multiple licenses from Florida and a Virginia ID. Red flags may have been raised. Instead, he simply drove away with a $270 ticket.

The 9/11 hijackers could do the same today. It is still possible to obtain multiple licenses and IDs because a one driver/one license rule is not in effect. Multiple DL/IDs issued in the same state to the same individual — under one name or multiple names, are still not routinely checked, and states do not cross-check such data. It's not only possible to game the system; it's likely. Police officers' hands are tied when they can't cross-check the ID they've been handed against any other information.

The 9/11 hijackers are not the only terrorists we know of who have taken advantage of blind spots and weaknesses in ID issuance standards. One terrorist caught in 2001 on the northern border, Nabil al Marabh, had five drivers licenses and a hazardous materials permit. Mir Aimal Kansi, who killed two people outside CIA headquarters in 1993, got a Virginia drivers license despite being in the United States illegally. These problems have been reduced significantly because many states have chosen to check lawful presence through the federal SAVE database in the past two years, leaving only four states struggling with a surge in illegal alien activity in their states. (Maryland is one, though its legislature is considering a legal presence requirement for DL/ID issuance for all new applicants.) REAL ID has encouraged SAVE use, as this is a required benchmark for compliance, and the result has been a marked increase in security and reduction of fraud.

Conclusion

As long as proof of lawful presence in the United States is not required of drivers license or non-driver ID applicants, anyone can take advantage of those vulnerabilities. In addition to terrorists, criminals of all kinds — identity thieves, counterfeiters, deadbeat dads, even underage teens seeking IDs to drink and drive — also use multiple IDs to hide their true identity from the law. In 2005, identity theft cost a staggering $64 billion, with $18.1 billion of that cost involving theft of a drivers license or ID. Individual consumers spend an average of 330 hours trying to undo identity theft and suffer $15,000 on average in losses. With REAL ID, drivers license identity theft will be much more difficult because more secure IDs will verify ID information before a DL/ID is issued and because the cards themselves will become more tamper-resistant and make it easier for law enforcement to determine fakes.

The proposed PASS ID Act would likely promote identity fraud by weakening many of the security standards set by the REAL ID Act. In essence, it would return license and ID issuance to pre-9/11 standards.

End Notes

[1] http://thomas.loc.gov/cgi-bin/query/z?c109:H.R.418.

[2] http://www.aamva.org/aamva/DocumentDisplay.aspx?id={25BBD457-FC4F-4852-A392-B91046252194}.

[3] Department of State: *Undercover Tests Reveal Significant Vulnerabilities in State's Passport Issuance Process,* GAO-09-447, March 13, 2009, http://www.gao.gov/products/GAO-09-447.

[4] AAMVA DL/ID Security Framework , p. 8.

[5] http://www.911securitysolutions.com/docs/REALIDFinalRules.pdf.

[6] http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=108_cong_public_laws&docid=f:publ458.108.pdf.

[7] http://www.cis.org/kephart/chertoffsstockingstuffer.

[8] 9/11 Commission Report, pp. 390, 387, http://govinfo.library.unt.edu/911/report/index.htm.

Center for Immigration Studies
1522 K Street, NW, Suite 820
Washington, DC 20005-1202
(202) 466-8185
center@cis.org
www.cis.org

Backgrounder

The Appearance of Security

REAL ID Final Regulations vs. PASS ID Act of 2009

Janice Kephart

The move toward more secure issuance of state identification documents may be in jeopardy. The most recent iteration of the National Governors Association secure ID bill circulating the Senate for signatures for possible introduction, the "Providing for Additional Security in States' Identification Act of 2009" or PASS ID, gives the appearance of security for drivers licenses and non-driver IDs (DL/ID) when, in fact, security does not exist. The PASS ID Act would provide for insecure issuance practices by the states that, for the most part, were in place prior to 9/11. In many ways, the PASS ID Act is a step backward for most states.

4-09

Center for Immigration Studies
1522 K Street, NW, Suite 820
Washington, DC 20005-1202
(202) 466-8185 • (202) 466-8076
center@cis.org • www.cis.org