February 2017

Issue Brief # 2017 - 02

# Emerging Mobile Technologies and the REAL ID Act: Legal Challenges and Recommended Approaches

Scott P. Boylan
Senior Vice President & General Counsel
MorphoTrust USA, LLC

Lauren E. DiGiovine
Counsel
MorphoTrust USA, LLC

*Contributors*
Jamie Gagnon
Director, Government Affairs
MorphoTrust USA, LLC

Benjamin Silverstein
Manager, Government Affairs
MorphoTrust USA, LLC

Center for Cyber
& Homeland Security
THE GEORGE WASHINGTON UNIVERSITY

# Emerging Mobile Technologies and the Real ID Act:
## Legal Challenges and Recommended Approaches

**SCOTT P. BOYLAN**[1]
*Senior Vice President & General Counsel, MorphoTrust USA*

**LAUREN E. DIGIOVINE**
*Counsel, MorphoTrust USA*

*Contributors:*

**Jamie Gagnon**
*Director, Government Affairs, MorphoTrust USA*

**Benjamin Silverstein**
*Manager, Government Affairs, MorphoTrust USA*

## I. Introduction

Ensuring that an individual is whom they claim to be has been central to national security since the inception of the United States Department of Homeland Security ("DHS"). This issue presents itself when crossing borders, engaging in commerce, and, most prevalently of late, in immigration.

This paper evaluates the legal challenges faced by emerging mobile technologies today. Primarily, what roadblocks the REAL ID Act imposes on mobile technology advancements by providers of secure credentials: does the REAL ID Act, as written, impose a substantial impediment to the roll out of mobile driver's licenses ("DLs") or identification ("ID") cards in the United States? Are there any additional legal barriers to the development of mobile DL/IDs in US jurisdictions? How does the REAL ID act borrow from existing best practices in physical card security and how does that effectuate the REAL ID Act's legislative intent?

We further assess the history of the REAL ID Act, providing an overview of DHS, the passage of the Act, and the law's phased implementation. The relationship between REAL ID regulatory mandates and industry requirements as described in the American Association for Motor Vehicle Administrator (AAMVA)'s 2013 Card Design Standard is also addressed. This paper presents long-term considerations, both legal and policy-based. Finally, the authors present recommendations for various stakeholders, including but not limited to, governmental bodies and private entities.

## II. History of the REAL ID Act

The United States Department of Homeland Security ("DHS") was established in March 2003, after the terrorist attacks of September 11th 2001.[2] In the wake of the terrorist attacks, DHS was tasked with protecting the American people from future terror attacks and other threats. The National Commission on Terror Attacks Upon the United States ("the 9/11 Commission"), chartered with preparing a

[1] The authors would like to thank Mark DiFraia and Roland Fournier, who were consulted as subject matter experts in the drafting of this issue brief.

[2] Homeland Security Act of 2002, Public Law 107-296, 107th Congress. (2002) (This act established DHS, organized the 22 agencies into a single body, and tasked it with securing the nation's borders and combating terrorism).

complete account of the events surrounding the attacks and proposing policy recommendations, was influential in DHS' subsequent efforts.

The REAL ID Act[3] was passed by Congress in 2005 in response to the 9/11 Commission's recommendation that the federal government "set standards for the issuance of sources of identification."[4] In the 9/11 Report, the Commission stated:

> *Secure identification should begin in the United States. The federal Government should set standards for the issuance of birth certificates and sources of identification, such as driver's licenses. Fraud in identification documents is no longer just a problem of theft. At many entry points to vulnerable facilities, including gates for boarding aircraft, sources of identification are the last opportunity to ensure that people are who they say they are and to check whether they are terrorists.*[5]

Thus, a primary objective of the REAL ID Act was to enhance security through improved, standardized forms of state-issued identification. The Act, signed into law by President George W. Bush on May 11, 2005, is comprised of many parts. Most notably, the Act would develop national standards and formats for the design of state-issued identification cards including, but not limited to, driver's licenses. Previous legislative efforts to establish such standards had failed because of fear that doing so would create a national identification card.[6] However, attitudes shifted in the wake of the September 11th attacks, and support for standardization increased. The 911 hijackers had used fraudulent credentials to board the planes, highlighting a security gap.[7] Thus, reasons were rooted in factors including, but not limited to, a desire to reduce illegal immigration and improve border security.[8]

## III. Mobile DL/IDs: A Problem Statement

The Act was passed in 2005, when consumer-grade mobile technology was in its infancy. Since the passage of the REAL ID Act, there have been several advances in technology. Federated identification systems have become the norm with the advent of widespread network access and a marked increase in the number of networked devices. These advances have been embraced in cyberspace to allow for higher identity assurance, and these practices have migrated to the world of physical security and in-person identification.

Notably, in June 2015, MorphoTrust USA, LLC ("MorphoTrust") in partnership with the Iowa Department

[3] Referred to herein as the REAL ID Act or the Act, the REAL ID Act of 2005 is part of the much broader Emergency Supplemental Appropriations Act for Defense, the Global War on Terror, and Tsunami Relief, 2005, Pub. L. No. 109-13, 119 Stat. 231, 151st Congress (2005).

[4] National Commission on Terrorist Attacks upon the United States. (Philip Zelikow, Executive Director; Bonnie D. Jenkins, Counsel; Ernest R. May, Senior Advisor). *The 9/11 Commission Report, 390* (2004), *available at* http://www.9-11commission.gov/report/911Report.pdf.

[5] Id. At 390.

[6] See generally Manoj Govindaiah, *Driver Licensing Under the Real ID Act: Can Current Technology Balance Security and Privacy?,* U. Ill. J.L. Tech. & Pol'y, Spring 2006.

[7] National Commission on Terrorist Attacks upon the United States. (Philip Zelikow, Executive Director; Bonnie D. Jenkins, Counsel; Ernest R. May, Senior Advisor). *The 9/11 Commission Report, 390* (2004), *available at* http://www.9-11commission.gov/report/911Report.pdf.

[8] Manoj Govindaiah, *Driver Licensing Under the Real ID Act: Can Current Technology Balance Security and Privacy?,* U. Ill. J.L. Tech. & Pol'y, Spring 2006, at 201, 203.

of Transportation (IDOT) initiated a first in the nation pilot program to develop and deploy a mobile DL solution. Noted Paul Trombino, director of IDOT, of the mDL's release:

> *We were very encouraged by the interest generated by our first public announcement of Iowa's Mobile Identity Application…Although we're not yet ready to release the mDL for customer use, the lessons learned in this pilot will demonstrate the use case for our mDL Application to be offered in the future as an option to all citizens across the state, and may help guide other states who want to launch similar digital identity programs. I firmly believe this is an important first step in creating a one person, one identity, one credential opportunity for our customers.*[9]

Several other states have considered adopting mobile DL/IDs in response to and aligned with the pilot program in Iowa. At this time, these include Florida, North Dakota, Delaware, Arizona, Utah, New Jersey, Louisiana, Georgia, and Missouri. State motor vehicle agencies ("MVAs") have demonstrated interest primarily through solicitations. These procurement efforts have run the gamut from preliminary Requests for Information ("RFIs") to integration into larger scale DL/ID Requests for Proposals ("RFPs").[10]

In parallel, several commercial entities have rolled out identity-based mobile applications. These applications appear in multiple commercial sectors, ranging from banking, to e-commerce, to finance, to air travel. At their core, all these systems involve the exchange of personally identifiable information ("PII") while leveraging the user's identity. What they all lack is a clear, cognizable connection to a recognized form of government-issued identification.

Thus, the REAL ID Act, as it stands, presents at least four challenges:

- Is it legally feasible to produce a mobile driver's license/ID that is compliant with the REAL ID Act?
- Will a REAL ID-compliant mobile driver's license mitigate concerns posed by the 9/11 commission?
- Further, will a REAL-ID compliant mobile DL/ID more effectively address the Act's legislative intent by accounting for technological advances?
- Will a REAL ID-compliant mobile DL/ID provide a suitable nexus between a mobile app user's purported identity and his/her proffered credential?

All of these considerations are represented in the multifarious elements of the REAL ID Act, legislation that addresses not only DL/ID design and security, but also the physical security of the facilities involved in the enrollment, issuance, manufacturing and production of secure credentials. Other topics include access control to these facilities, the security of PII, personnel security (including, but not limited to, background checks), emergency/incident response, audit controls, and the handling of sensitive security

[9] *MorphoTrust Launches Nation's First Mobile Driver License Pilot*, Business Wire, http://www.businesswire.com/news/home/20150826005144/en/MorphoTrust-Launches-Nation%e2%80%99s-Mobile-Driver-License-Pilot.

[10] E.g., State of Georgia, Department of Driver Services, Electronic Request for Proposals ("eRFPs"), Card Production System, eRFP (Event) Number: 47500-DDS0000052, p. 43 ("Georgia does not currently offer an Electronic DL/ID or Mobile DL/ID but will consider doing so. Offerors may include an Electronic or Mobile DL/IS in their proposal and, if so, include their estimate not to exceed cost in the Cost Worksheet. Offerors must assume no limit in the volume of Electronic DL/ID or Mobile DL/ID).

information.

In essence, where the Act contemplates a physical form of identification, produced in a secure facility, to serve an official purpose as defined under §201 of the Act,[11] is it possible for a mobile DL/ID to effectuate that same purpose, simply via a virtual means?

## IV. REAL ID and Mobile DL/IDs: Standards and Technological Issues

The REAL ID Act is arguably aligned with federalist principles, delegating most of the duties to the States, with DHS retaining only oversight and federal regulatory authority. Pursuant to Section 202(b), the states are required to design and produce DL/IDs that satisfy the minimum federal requirements. The State is also required, pursuant to section 202(c), to comply with requirements for establishing valid documentary evidence that the applicant is lawfully present in the United States.

The Act authorizes the Secretary of DHS, in consultation with the States and Secretary of Transportation, to promulgate regulations to implement the requirements under the Act. While the Secretary of DHS is permitted to waive certain requirements, these waivable requirements are never those enumerated under Section 202(b). These mandatory provisions are, in short, basic demographic information, physical security features designed to prevent tampering, counterfeiting, or duplication of the DL/IDs for fraudulent purposes, and common machine readable technology.

The practical elements of the REAL ID Act are rooted in best practices for the secure credentialing industry. Both statutory and regulatory language reveals near-mirror image verbiage between American Association of Motor Vehicle Administrators (AAMVA) requirements and those mandated by the federal law. Indeed, DHS and U.S. Citizenship and Immigration Services acknowledge that DHS collaborated with the Department of State and were guided by State's "passport verification module"[12] and with AAMVA in drafting and implementation. DHS participated with the states and territories in drafting the Personal Identification - AAMVA North American Standard - DL/ID Card Design to ensure that states and territories can implement the REAL ID requirements for card design by means of common, consensus-based data formats and card technologies endorsed by all states and territories."[13]

Relying upon the DHS "Minimum Standards for Driver's Licenses and Identification Cards Acceptable by Federal Agencies for Official Purposes,"[14] AAMVA experts state that the AAMVA Card Design Standard ("CDS") is consistent with the implementation of the REAL ID Act and indicated that their shared "…goal is to improve the security of state-issued driver's licenses by requiring:

- Information and physical security features that must be incorporated into each card;

[11] Pub. L. No. 109-1, §201(3) ("The term `official purpose' includes but is not limited to accessing Federal facilities, boarding federally regulated commercial aircraft, entering nuclear power plants, and any other purposes that the Secretary shall determine").

[12] Written Testimony Of Office Of Policy Assistant Secretary David Heyman For A House Committee On The Judiciary, Subcommittee On Crime, Terrorism, And Homeland Security Hearing Titled "Secure Identification: The Real ID Act, 2012 WL 949598.

[13] Written Testimony Of Office Of Policy Assistant Secretary David Heyman For A House Committee On The Judiciary, Subcommittee On Crime, Terrorism, And Homeland Security Hearing Titled "Secure Identification: The Real ID Act, 2012 WL 949598.

[14] *See* Minimum Standards for Driver's Licenses and Identification Cards Acceptable by Federal Agencies for Official Purposes, 73 Fed. Reg. 5,270-5,340 (Jan. 29, 2008) (codified at 6 C.F.R. §37).

- Specific application information to establish an applicant's identity and lawful presence in the United States before a card can be issued;
- Verification of certain source documents provided by an applicant with the document issuing agencies; and
- Issuance and physical security standards for locations where licenses and identification cards are issued."[15]

REAL ID-compliant mobile solutions are not only a reasonable advancement in technology, but align with the best practices put forth by AAMVA in the CDS.

## A. REAL ID, AAMVA, and Printed Data

Both REAL ID ACT and AAMVA CDS mandate the location and format of certain printed information. The REAL ID Act mandates this in 6 CFR 37.17, Requirements for the surface of the driver's license or identification card. This same information is governed by Annex A within the CDS. The table below highlights the similarities.

*Table 1: Required Printed Data: AAMVA v REAL ID – Identical Requirements Permit Transferability*

| 6 CFR 37.17 - Requirements for the surface of the driver's license | CDS Annex A |
|---|---|
| Full legal name (a) | A.7.3 Zone II |
| Date of birth (b) | A.7.3 Zone II |
| Gender (c) | A.7.3 Zone II |
| Unique driver's license or identification card number (d) | A.7.3 Zone II |
| Full facial digital photograph (e) | A.7.4 Zone III; A.7.8.1 Portrait |
| Address of principal residence (f) | A.7.3 Zone II |
| Signature (g) | A.7.3 Zone II; A.7.4 Zone III; A.7.8.2 Signature |
| Physical security features (h) | A.8 Signature |
| Machine-readable technology on the back of the card (pursuant to §37.19) (i) | A.7.6 Zone V |
| Date of transaction (j) | A.7.3 Zone II |
| Expiration date (k) | A.7.3 Zone II |
| State or territory of issuance (l) | A.7.5 Zone IV |
| Printed information (m) | A.3 Dimensions and character set; A.4 Functions; A.5 Common Recognition; A.7 Contents of Zones |
| DHS approved security marking (n) | A.9 DHS Compliance Indicators |

[15] American Association of Motor Vehicle Administrators (AAMVA) Card Design Standard Committee, AAMVA DL/ID Card Design Standard – Personal Identification – AAMVA North American Standard (2013), http://www.aamva.org/DL-ID-Card-Design-Standard/ (pp. xii-xiii).

## B. Portraits, Facial Recognition, and Mobile Deployment

One of the most striking similarities between the two is not the demographic requirements, but rather the stringent mandates on and around the full facial digital photograph. Specifically, the CFR states that "States shall follow specifically ISO/IEC[16] 19794-5:2005(E) Information technology—Biometric Data Interchange Formats—Part 5: Face Image Data."[17] The purpose of this particular standard, adopted by both AAMVA and DHS, is:

> *To enable many applications on a variety of devices, including devices that have limited resources available for data storage, and to improve face recognition accuracy, this part of ISO/IEC 19794 specifies not only a data format, but also scene constraints (lighting, pose, expression, etc.), photographic properties (positioning, camera focus, etc.) and digital image attributes (image resolution, image size, etc.).*[18]

A primary goal of both AAMVA and DHS is facial recognition. This could be achieved by a mobile solution, perhaps even more effectively than a printed credential. AAMVA's Driver Standing Committee & Law Enforcement Standing Committee Facial Recognition Working Group issued a white paper in August 2015 on Facial Recognition Program Best Practices. In the paper, the Working Group noted that "(f)acial recognition (FR) is a fraud prevention, fraud detection, business integrity, and risk mitigation tool used by the majority of U.S. and Canadian Departments of Motor Vehicles (DMVs). FR software automates the process of photo image matching and is designed to determine whether the person shown in one photograph is likely to be the same person shown in another photograph."[19]

More importantly, AAMVA notes that this is more effectively achieved in a central issuance system because the infrastructure permits a more thorough vetting process of the individual against all prior images and data within the state database.[20] Mobile technology is necessarily central issuance; all credentials are all deployed from a single, secure source. Facial recognition software deployed through technological means can be more effectively maintained through a technological and mobile solution. This is consistent with REAL ID's stated mission – to ensure that each person carrying a DL/ID is who they say they are.

## C. Physical Security for a REAL ID Compliant Mobile Credential

The requirements for physical security for the driver's license or identification card are enumerated in 6

[16] This is one of the standards promulgated by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC), a nonprofit standards organizations responsible for developing an international system of standardization in both private and governmental organizations.

[17] 6 CFR 37.17(e)(1).

[18] ISO/IEC 19794-5:2011(en)
Information technology — Biometric data interchange formats — Part 5: Face image data; https://www.iso.org/obp/ui/#iso:std:iso-iec:19794:-5:ed-2:v1:en; 4/26/16; this is a second edition of the first edition (ISO/IEC 19794-5:2005), provisionally retained.

[19] American Association of Motor Vehicle Administrators (AAMVA), AAMVA's Driver Standing Committee & Law Enforcement Standing Committee Facial Recognition Working Group, Facial Recognition Program Best Practices (August 2015), http://www.aamva.org/best-practices-and-model-legislation/) (p. 6).

[20] American Association of Motor Vehicle Administrators (AAMVA), AAMVA's Driver Standing Committee & Law Enforcement Standing Committee Facial Recognition Working Group, Facial Recognition Program Best Practices (August 2015), http://www.aamva.org/best-practices-and-model-legislation/) (p. 17).

CFR 37.15. Specifically, the Code of Federal Regulations requires “at least three levels of integrated security features.” 6 CFR 37.15(b). These “integrated security features” would “provide the maximum resistance to a person’s efforts to…” such malfeasance as counterfeiting, deletion, substitution, and fraud. 6 CFR 37.15(b)(1)-(4). The regulations were clearly drafted in contemplation of a physical card. This is near identical to AAMVA’s own language around the physical security of a card as described primarily in the tables of Annex B. Below is a table comparing the requirements:

*Table 2: REAL ID Act & AAMVA 2013 CDS Threats*

| **REAL ID Act – 6 CFR 37.15(b) Integrated Security Features - REAL ID driver's licenses and identification cards must contain at least three levels of integrated security features that provide the maximum resistance to persons' efforts to** | **AAMVA 2013 CDS – Annex C – Categories of Threats** |
|---|---|
| (1) Counterfeit, alter, simulate, or reproduce a genuine document; | A.1 Document Design Attacks |
| (2) Alter, delete, modify, mask, or tamper with data concerning the original or lawful card holder; | A.2 Substitute Material/Personalization attacks |
| (3) Substitute or alter the original or lawful card holder's photograph and/or signature by any means; and | B.1 Falsification by physical modification of existing valid documents |
| (4) Create a fraudulent document using components from legitimate driver's licenses or identification cards. | B.2 Falsification by Recycling |

By aligning the regulatory requirements with industry best practices, DHS mandates that state governments and agencies “…include physical security features to prevent tampering or use of the DL/ID for fraudulent purposes and a common machine-readable technology element as well.”[21] The AAMVA CDS provides several card security features to combat each threat. These security features are each assigned a category – card body design; security design, resistant to reproduction; security ink/pigment; and protecting personalized data.

However, it is incumbent upon the vendor’s team of secure card experts to design a secure, REAL ID compliant credential that balances security concerns against often competing jurisdiction-specific interests (e.g., aesthetic, political). Most, if not all, of these security features easily transition to a mobile credential. Guilloche design[22] is one such example of a security design feature capable of resisting attacks governed by §37.15(b)(1)-(3). The feature is visible to the naked eye and easily replicated on a mobile device.

[21] Manoj Govindaiah, *Driver Licensing Under the Real ID Act: Can Current Technology Balance Security and Privacy?*, U. Ill. J.L. TECH. & POL'Y, Spring 2006, at 201, 203.

[22] American Association of Motor Vehicle Administrators (AAMVA), Driver Standing Committee, Card Design Standard Committee, Design Principles And Guidelines For Secure Cards (August 2014), http://www.aamva.org/best-practices-and-model-legislation/ (Guilloche is defined as, “A pattern of continuous fine lines, usually computer generated, and forming a unique pattern that can only be accurately re-originated by access to the software and parameters used in creating the original design”).

### D. Machine Readable Technology and the Mobile Credential

Another such example is machine readable technology. Under the REAL ID Act, this is regulated by 6 CFR 37.19, which requires that "[f]or the machine readable portion of the REAL ID driver's license or identification card, States must use the ISO/IEC 15438:2006(E) Information Technology—Automatic identification and data capture techniques—PDF417 symbology specification."[23] PDF417 was adopted as an AAMVA best practice in the CDS. The CDS defines machine-readable technology (MRT) as "Magnetic stripe, smart card, bar codes, OCR, optical WORM media, etc." that "verifies the authenticity of the document, the data or the person presenting the card by the use of a reader and comparison of the stored data to other machine or visual information."[24] Annex D of the Standard describes the requirements for compliant PDF417 symbols at length. Effectively, a compliant symbol will allow for the maximum amount of data. The mandatory minimum under the REAL ID Act is expiration date, full legal name, date of transaction, date of birth, gender, address, unique driver's license or identification card number, card design revision date, inventory control number, and state or territory of issuance.[25]

One critique of the Act's barcode provision has been the purported vulnerability of an unencrypted barcode. However, the transition to a mobile solution provides a tested machine readable alternative to card barcode technology. One scholar posits that creating an alternate barcode specifically for REAL ID would mitigate the security risks: "the use of a proprietary barcode, along with proprietary scanning and decoding technology, would reduce the ability of unauthorized users to access barcode data."[26]
This is reasonable. Machine readable technology is appearing increasingly on commercially available mobile applications for other industries. In terms of the capability to "flip" the mobile DL/ID so that the machine readable zone ("MRZ") is, in fact, readable (i.e., so both front and back of the DL/ID is ascertainable), this technology should be well within our means. Electronic boarding passes over the past few years have contained a host of information ranging from ticket holder identity, to airline, to flight number, and everything in between.

### E. Are REAL ID Compliant Mobile Credentials as Resistant to Intrusion as Physical DL/IDs?

A principle underlying the Act is that no individual shall create a fraudulent credential. This includes counterfeiting a genuine document; manipulating data concerning the original card holder; changing the original/lawful card holder's photograph/signature; or creating a fake credential using components from other legitimate documents (a "Franken-license," of sorts).

Section B.4.2.1 of AAMVA's CDS addresses card body design:

> *Card body design refers to the security of the card construction and in particular to the properties of the materials used in the manufacture of card blanks. It should be noted that the chosen card construction cannot be determined in isolation and must also take into account the operational profile of the card. For example the construction of the card must be suitable for the*

[23] 6 CFR 37.19.

[24] American Association of Motor Vehicle Administrators (AAMVA) Card Design Standard Committee, AAMVA DL/ID CARD DESIGN STANDARD – PERSONAL IDENTIFICATION – AAMVA NORTH AMERICAN STANDARD (2013), http://www.aamva.org/DL-ID-Card-Design-Standard/ (pp. 43).

[25] 6 CFR 37.19.

[26] Geoffrey D. Kravitz, *Real ID: The Devil You Don't Know*, 3 HARV. L. & POL'Y REV. 431, 444 (2009).

> *intended method of personalization, also, if a chip is to be included within the card body the construction must allow either for an inlay (contactless interface) or for milling and embedding (contact interface) of the card body.*[27]

Specific features such as a tamper evident card body[28] and taggants[29] would have to be redesigned for the purposes of a mobile solution. This is because mobile devices are individually vulnerable to attack by bad actors; applications are porous. Nevertheless, the goals of the REAL ID Act would be achieved by a mobile application by implementing linked and layered features native to mobile devices such as encryption and strong user authentication. The issue will not be cannibalization, but hacking. The proposed solution is arguably as capable of satisfying the regulatory requirements as a physical card because it is capable of minimizing intrusion attempts provided that security features emphasize encryption of data in transit and at rest. Examples of new security include document authentication as a cloud service, liveness photo testing, and face locked applications. The goal is not to replicate present physical security features, but rather to develop intelligent applications built to secure the device. Thus, if monitored and encrypted effectively, the average fraudster may not hack and manipulate a credential to infiltrate border crossings and other vulnerable facilities.

## F. One Person, One Credential: Simultaneous Issuance Risks & Immediate Revocation

Central to the Act's mission is ensuring that each citizen is issued only one REAL ID card. Pursuant to the regulations, "[a]n individual may hold only one REAL ID card. An individual cannot hold a REAL ID driver's license and a REAL ID identification card simultaneously."[30] Thus, it is incumbent upon each jurisdiction to decide the manner in which any hypothetical mobile REAL ID compliant DL/ID program is rolled out. Additionally, Congress should consider modifying the CFR to include language permitting simultaneous ownership of both physical cards and mobile credentials where they are REAL ID compliant and comply with all other jurisdiction-specific requirements.

## G. Renew, Revise, and Revoke in Real Time

In that same vein, mobile identification technologies offer an additional level of security-enhancing capabilities. Specifically, motor vehicle agencies vis-a-vis the state are empowered to revoke or grant privileges in real time.  This provides the most up-to-date information to such key stakeholders as law enforcement officers and bartenders.

[27] CDS, p. 34. American Association of Motor Vehicle Administrators (AAMVA) Card Design Standard Committee, AAMVA DL/ID Card Design Standard – Personal Identification – AAMVA North American Standard (2013), http://www.aamva.org/DL-ID-Card-Design-Standard/ (pp. 34).

[28] American Association of Motor Vehicle Administrators (AAMVA) Card Design Standard Committee, AAMVA DL/ID Card Design Standard – Personal Identification – AAMVA North American Standard (2013), http://www.aamva.org/DL-ID-Card-Design-Standard/ (pp. 45) (Card showing evidence of destruction or modification caused by an attack. One such example is Security Bonding).

[29] American Association of Motor Vehicle Administrators (AAMVA) Card Design Standard Committee, AAMVA DL/ID Card Design Standard – Personal Identification – AAMVA North American Standard (2013), http://www.aamva.org/DL-ID-Card-Design-Standard/ (pp. 45) (Special materials and/or chemicals hidden inside the card core (plastic, composite paper or synthetic material) which can only be detected and authenticated with special equipment).

[30] 6 CFR 37.29(a)

As discussed above, Section 207 of the Act specifically limits the authority of the Act to its enumerated powers, empowering States to govern appropriately. Indeed, the federal regulations permit remote reissuance where permitted by the applicable State[31] and allow remote renewal where permitted by the State (with some limitations).[32]

That said, although the Act does not specifically mandate any timeline for changes in license information (including changes of address or name, privilege revocation and reissuance), a mobile solution would enhance security. Providing current information about an individual's identity and restrictions[33] supports both state and homeland security efforts. In central issuance jurisdictions, data may be "pushed" to mobile credential users as an update from a secure location without reprint; it's simply a modification of a preexisting design. In allowing states to have immediate control of this process, mobile identification systems further standardize the security regimen.

## V. Conclusions: Stakeholder Recommendations & Long-term Considerations

In the Federal Register, DHS responded to positive and negative comments. One commenter noted: "REAL ID correctly specified a set of performance standards rather than listing static prescriptive standards, and that enhanced document security is essential to combat terrorists, can help improve transportation safety, and can combat identity theft or other criminal acts."[34] DHS agreed with the assessment, responding:

> *States that fully implement these rules will improve national security by improving the security and reliability of a key document carried by many Americans. Both the REAL ID Act and the REAL ID regulations focus on improving the reliability of State-issued driver's licenses and identification cards and decreasing the likelihood that an individual can fraudulently obtain an identity document or alter a legitimate identity document to create a false identity. The availability of better and more reliable security documents means that government and law enforcement officials have a greater opportunity to prevent terrorists and other unauthorized persons from gaining access to commercial airplanes and Federal facilities.*[35]

Indeed, this is aligned with the above proposal. The response from DHS highlights the central goal of the REAL ID Act, as well as the key tenets of the regulatory mandates. It indicates that industry's focus should be on achieving border security while concurrently ensuring lawful compliance.

It is feasible to develop a mobile DL/ID solution, compliant with the aforementioned REAL ID requirements that would achieve DHS' considerations. If the goal is to improve the reliability of state-issued credentials and decrease the likelihood of fraud, therein is the focus. This is evident in the AAMVA requirements that have been integrated into the regulations. DHS and U.S. DMVs should accept the proposal that mobile DL/ID solutions are compliant with both REAL ID Act and regulatory requirements. If they do, the results will be more consistent with the spirit of the law and recent innovation in mobile technology.

[31] 6 CFR 37.23

[32] 6 CFR 37.25(b)

[33] 6 CFR 37.33(a)(4) ("States must maintain a State motor vehicle database that contains, at a minimum…Motor vehicle driver's histories, including motor vehicle violations, suspensions, and points on driver's licenses.").

[34] *See* 73 Fed. Reg. at 5.281 (Jan. 29, 2008) (codified at 6 C.F.R. § 37).

[35] *See* 73 Fed. Reg. at 5.281 (Jan. 29, 2008) (codified at 6 C.F.R. § 37).

## About the Center for Cyber & Homeland Security

The Center for Cyber & Homeland Security (CCHS) at the George Washington University is a nonpartisan “think and do” tank whose mission is to carry out policy-relevant research and analysis on homeland security, counterterrorism, and cybersecurity issues. By convening domestic and international policymakers and practitioners at all levels of government, the private and non-profit sectors, and academia, CCHS develops innovative strategies to address and confront current and future threats.