DOCUMENT SECURITY ALLIANCE

Statement by the Document Security Alliance on Technology for Secure Identity Documents given to the Subcommittee on Government Management, Organization and Procurement of the Committee on Oversight and Government Reform

I. Executive Summary:

This testimony gives an overview of the technical, business process, and public policy recommendations of the Document Security Alliance (DSA) on a host of identity management subjects. This testimony comments on the need for the Federal government and State governments to adopt end-to-end identity management solutions that address the unique security challenges faced by ID issuers today by incorporating five critical elements of secure ID issuance: Data Capture, Identification Verification, Secure ID Production, Secure ID Credentials, and ID Authentication. This testimony provides best practice recommendations on the steps the government needs to take to improve the quality and security of IDs such as Social Security Cards and driver's licenses, and concludes with a number of recommendations. The views expressed in this testimony are the Document Security Alliance's and although experts from government agencies are members of the DSA, no government agency member has endorsed these views on behalf of their agency.

II. Introduction:

On behalf of the Document Security Alliance, I would like to thank Chairman Towns and Ranking Member Bilbray for giving me an opportunity to present the views of the Alliance on technology for secure identity documents, systems and processes.

I am appearing before your Subcommittee to represent the views of the experts of the DSA in the field of secure ID solutions. I currently serve as the Vice Chair of the Government Affairs Committee of the Document Security Alliance (DSA), and I have spoken, testified and worked extensively on document security issues at conferences and with Congressional committees and groups such as the National Council of State Legislatures, American Legislative Exchange Council and a number of U.S. States, and was a key contributor to drafting the SAFE ID Act, which was enacted in 2004.

The Document Security Alliance (DSA) was created by government agencies, private industry and academia to identify methods to improve security documents and related security procedures in order to help combat the growing use of counterfeit documents in acts of identity theft and fraud, terrorism, illegal purchases of controlled substances and firearms, illegal immigration, and other criminal acts. Recognizing the need to continuously improve document security and the issuance process to combat new and existing threats, the DSA is dedicated to work with and educate those responsible for secure document issuance, distribution and use on the value of improving the security and reliability of ID documents. DSA members–in both government and private industry–draw upon the knowledge and detailed technical disciplines of the spectrum of members to accomplish this goal. The group is committed to develop recommendations to appropriate federal and state government agencies, private industry, and policy makers in order to improve the process and procedures surrounding document security.

The DSA membership consists of more than a dozen government agencies and organizations (including the U.S. Secret Service, TSA, DHS, Social Security Administration, FBI, GSA, FDA, and Departments of Treasury and State, and the Government Printing Office), as well as over 75 companies participating in the document security area. Private sector entities and trade associations primarily represent the credentialing industry, including system integrators, card manufacturers, secure printing companies, printer manufacturers; security features producers, and biometric providers.

I am also the Executive Vice President of one of the DSA's industry members, Digimarc, which issues more than 60 million identification documents annually, producing more than 2/3 of all driver licenses issued in the U.S.

III. Worldwide Identity Documents Threats:

Equipment and tools are available today that put counterfeiting ability in the hands of those who previously did not have appropriate graphic or printing skills, making law enforcement's efforts to stop this crime much more difficult. The continuing sophistication of desk top color printers, color laser copiers, high resolution color scanners, imaging and editing software, digital cameras and the exchange of information on the Internet have made document counterfeiting, alteration, and photo substitution able to be performed by the general public. As a result, the ease of obtaining fraudulent identification and phony breeder documents of usable quality has greatly increased as has the need for additional layers of security to be incorporated in the document. The variety of identification document formats has made the visual authentication by humans more difficult and often insufficient to detect fraud. To ensure the ability to discern authentic documents, the use of machine-readable technologies is increasingly necessary.

IV. Elements of a Secure ID System

In order to improve document security it is important understand and improve how an applicant is qualified and how a secure ID is issued and used. DSA believes any secure ID infrastructure must include, at least, the following elements:

Data Capture – Obtain the applicant's photograph, demographic information, supporting documents (such as breeder documents), a digital version of his/her signature, and, if necessary, appropriate biometrics (e.g., facial image or fingerprint).

Identification Verification – Authenticate an applicant's credentials and the breeder documents they present, as well as comparing select information against the issuing authority's databases or other records (e.g., Social Security Administration data). Note that privacy best practices would suggest this be a point-to-point interaction to validate data as in the current Social Security implementation and not a centralized hub or repository where personal information could be accessed.

Secure ID Production – Utilize processes and technologies that enable secure ID issuance.

Secure ID Credentials – Incorporate a layered, durable architecture that includes both difficult-to-counterfeit materials with sophisticated laminating and finishing processes, as well as a number of overt, covert and forensic security features.

Authenticating IDs – Verify – without infringing on an individual's personal privacy – the authenticity of a proffered government-issued photo ID, no matter where it was issued, at all various points of inspection or transaction – public or private sector (e.g., law enforcement, transportation, DMVs, banks or retail).

The DSA has identified a number of best practices that have already been implemented by government issuers of photo IDs in some sectors within the U.S., including –

- Upgrading requirements in obtaining and authenticating "breeder" documents (birth certificates, social security cards, driver licenses, etc.) used in issuing IDs.
- Incorporating new technologies to enable cross-jurisdictional point-of-inspection machine- readable ID authentication – allowing for quick verification of the ID.
- Moving toward issuance of IDs from secure facilities to enable verification processes and provide better control over materials and security features.
- Establishing systems for facial recognition based image identity verification.

- Implementing capabilities for cross database applicant verification (not necessarily centralized databases, information hubs or national IDs systems).
- Shortening issuance and validity periods (e.g., five years) to ensure accurate records and enable security feature renewal/upgrade.
- Providing appropriate resources, training and equipment to State DMVs and other government issuing authorities to upgrade issuance, authentication and verification processes and incorporate new security features.
- Establishing laws (e.g., SAFE ID Act) to provide law enforcement with tools to combat ID counterfeiting.

V. Identity Credential Security:

Documents and cards may be secured in a number of ways including the use of various features or devices:

- Printing – such as deliberate errors and flaws, non-standard print fonts, background printing patterns, microprinting, rainbow printing, anti-copy features, and hidden images or message.
- Inks – such as chemically reactive, infrared and ultraviolet fluorescent, color shifting, photochromatic, thermocromatic, metallic, and many more.
- Substrate inclusion – such as embedding features like threads and fibers, taggent and/or markers in materials, controlled response to UV light, core inclusion, bonding materials, and opacity marks.
- Optically variable devices – such as holograms, color shifting films, color shifting inks, liquid crystals, transparent and metallic features.
- Additional features – such as biometric characteristics, embedded images, security laminates, digital and visual watermarks, laser-engraved or perforated features, retroreflective features, tactile features, tactile features, machine-readable technologies, and many more.

Security features and devices protect documents and assist in proving document authenticity and/or tamper-evidence at three levels of inspection (some security features protect the document in more than one category or Level):

- Overt (Level 1) – this type of device supports inspection and examination without tools or aids that involves easily identifiable visual (naked eye) or tactile (touch) features.
- Covert (Level 2) – this type of device supports inspection and examination requiring the use of a tool or instrument to discern the feature (i.e., UV light, magnifying glass, machine readable technology reader, scanner).
- Forensic (Level 3) – this type of device is used to prove document genuineness through inspection and examination or destruction requiring the use of expert training and laboratory equipment designed to measure select security features known only to a few often for use in case

preparation by law enforcement and for court use. Closely holding the forensic a secret is also a key.

Security features are used to protect against several types of threats to documents:

- Counterfeit or simulation – the unauthorized copy or reproduction of genuine documents by whatever means.
- Forgery or alteration – the deletion, modification, masking, tampering with biographical data concerning the original or rightful document holder.
- Photo and signature substitution – substitution of an imposter's photograph or signature of the original or rightful document holder.
- Cannibalization – creation of a fraudulent document using components from more than one legitimate document.

Document security features facilitate the task of verification and authentication by officials and inspectors throughout the world, making the task as easy as possible under all practical circumstances and conditions. Before a document's security features are selected, a risk assessment must be performed by each issuing authority appropriate to the environment and to meet and combat known and anticipated security concerns. Documents may then be designed using information and features that are "layered" and "linked" on the document. Layering features and devices means providing various types of security devices on each component used in the construction or assembly of the card or document (e.g., certain features on the core and others on the laminates). Layering security features means the document does not become authentic until all of the components are included at the point of manufacturing. Features are designed to work together in the final document so that one complements another (e.g., overlapping features, overlaying features from various layers) creating conditions of extreme difficulty for a credential to be altered and/or successfully counterfeited. In addition, security features that self-destruct and clearly show evidence of tampering are highly desirable to protect against the alteration of data and the reuse of credential by forgers.

The information on the various elements of the document is linked together by repetition of all or a portion of the data in various human and machine-readable portions. Linking ties one part of the document to another to authenticate and secure the document itself (e.g., a birth date, identifying number, or other variable personalized data may appear in printed fashion as an overt feature - readable by the naked eye - and be repeated in a machine-readable bar codes or covert features that can be automatically read and matched for consistency to help provide authentication as genuine). The criminal counterfeiter and forger are defeated by the multiple and varied features necessary to replicate to construct a document that will pass inspection of all security checks. It becomes cost prohibitive for most fraudsters to overcome all of the techniques and technologies thereby allowing law enforcement to concentrate their resources on the more organized criminals.

The DSA recommends the use of at least a minimum number of security features in each of the overt, covert, and forensic levels designed to combat the risk threats identified for each level for document use.

Machine-Readable Technologies

The key to machine-readable technology is interoperability. In the real world, dependence solely upon visual inspection of a document is not sufficient, just as sole reliance on an automated technology without examining and linking to the document holder would be insufficient. In order for identification documents to work both intra- and inter-jurisdictionally, common technologies with interoperating data elements on all credentials facilitate use. The issues of standardization, vendor independence, the logical transition from legacy systems and methodologies, and the migration paths for evolving technologies must all be considered as part of the machine-readable technology selection. Interoperability of document information is essential in any environment where the receiving party or agency is different from the issuer. Common sets of operating rules must be in place to ensure that documents can be accepted and their authenticity validated. Cost-appropriate technologies that secure the assessed risks and threats are required. Currently, most U.S. driver's licenses use one or more machine-readable features, including two-dimensional (2D) bar codes, digital watermarks and magnetic stripes, with 2D bar codes in use by most jurisdictions. This does not preclude the continued use of any other machine-readable technology already or the addition of others as improvements in technology develop.

V. Securing Social Security Cards: Past, Present, and Recommendations:

The Past

Since 1936, the primary audience for Social Security cards issued by the Social Security Administration (SSA) has been employers. The purpose of the card is to carry a unique identification number assigned to an individual, so that earnings can be accurately tracked and attributed to that individual in anticipation of future benefits. As such, SSA maintains that the primary role of the Social Security Number (SSN) is to accurately report the earnings of people who work in jobs covered under FICA so that social security benefits can be properly paid to them.

Congress has consistently maintained that the SSN card is not an identity document and the SSA recognizes that the SSN card is routinely accepted by outside entities as a breeder document for other identification documents. These entities include or have included:

- State Motor Vehicle Administrations (drivers' licenses)
- The U.S. Department of State (passports)

By the 1980s it was becoming apparent that many non-governmental entities were using the SSN and Social Security card as a personal identifier for individuals. Since October 1983, as required by the Social Security Act, the card is made of banknote paper and incorporates a number of other security features designed to prevent counterfeiting.

- The card is currently printed on an optically dead 90 lb. card stock with high cotton content and randomly placed fluorescent planchettes (multi-colored dots)
- The card is printed on high-speed impact printers producing microscopic breaks in the paper fiber and the ink penetrates the surface
- A chemical stain is present to protect against alterations
- It includes intaglio print on the columns
- A microprinted signature line (repeating the words "Social Security Administration") is on the card face
- A blue tint marbleized pattern printed in erasable ink
- A previous version of the card included a VOID pantograph behind the marble camouflage pattern on the card face
- The back of the card includes a red-fluorescing 9 digit alpha-numeric control number

Recently, the REAL ID legislation mandated that State motor vehicle agencies verify an applicant's SSN but not that the applicant must present the card. DHS has not yet completed their rule making for this provision of the law and they could decide to include a requirement for mandatory presentation of the applicant's Social Security card. So, for the time being a State would be compliant with REAL ID if they asked for an applicant's number and performed a verification of the name/number with the SSA, without seeing the physical card itself. Some States currently require presentation of the physical card and they may therefore capture an image of this and retain the image of the SSN card with the images of the applicant's other breeder documents.

The Present

SSA currently issues approximately 20 million cards annually. This number is not expected to increase appreciably. The current price of a card is about 5 cents. The card is relatively easy to mimic, and some trained inspectors are able to spot fraudulent ones. While the primary threats to the SSN card today involve counterfeits, tampering and false issuance, much of the fraud reported today involves the use of the SSN and not specific attacks on the physical card itself (95% of the identity theft is as the result of obtaining a SSN and name through fraudulent methods, such as internet fraud, telephone solicitations and illicit use of personalized documentation). Many employers are not equipped, empowered, or authorized to assess the authenticity of the card or the legitimacy of the card holder.

Some members of Congress have requested that security improvements be implemented on the card, alleging that the current features are not effective in protecting against counterfeits or enabling employers to determine authenticity for work authorization purposes.

The SSA approached the DSA and requested assistance in developing guidelines concerning a more secure Social Security card. A DSA project team reviewed the current and anticipated security threats faced by the card, the expectations of the SSA, and existing legislation (Intelligence Reform and Terrorism Prevention Act of 2004) regarding improvements to the card in order to develop actionable security recommendations to the SSA.

DSA believes the current card should not be considered as a secure credential. There are too few controls and linkages to the intended card holder to offer confidence in the identification value. There are now 54 versions of the card in circulation. Prior to 1978 many cards were issued without proof of age, identity, or immigration status. Large numbers of cards issued pre-1983 are versions without counterfeit, alteration, or tamper-resistant and tamper-evident security features.

Today, to obtain a SSN and card, applicants fill out an application and submit evidence of their age, identity, and citizenship status or lawful immigration status. Non-citizens must provide DHS documentation authorizing them to work in the United States or provide proof of a valid non-work reason for needing a SSN, such as receipt of federal benefits. Applicants age 12 or over are required to have an in-person interview and explain why they never obtained a SSN before. The SSA's 'Enumeration at Birth program' allows parents to obtain a SSN for newborn babies through the hospital during the birth registration process. Applicant information is transmitted through the State to SSA, and a SSN and card are issued.

When an individual's Social Security card is lost or mutilated or the individual reports changes to information contained in SSA's records (such as a legal name change after marriage), SSA issues a replacement card. However, unlike the process for issuing original cards, SSA does not verify the citizenship of individuals who indicate to SSA that they were born in the United States, as long as the citizenship information they previously provided to SSA supports their assertion. As a result, the process for issuing replacement cards may not provide for the cards to be reliable proof of the number holder's entitlement to work in the United States.

Today there are three types of Social Security cards issued:

- Allowing unrestricted work – U.S. citizens and those lawfully permitted who have DHS permission to work

- Not valid for employment – non-citizens who do not have DHS permission to work and state or local laws or a federally funded benefit program require a SSN
- Valid for work only with DHS (INS) authorization – non-citizens who have DHS (formerly INS) permission to work temporarily in the U.S.

Current Attack Data

Most allegations of fraud come from the SSA, law enforcement and the public.

- 81% Identity Theft – Contacts from victims alleging others were using their SSN for unlawful purposes.

Identity theft allegations were further examined to identify the types of activity reported. These were:

- Credit – Use of the SSN to obtain credit cards
- Work – Use of the SSN or card to obtain work, permits or licenses
- Services – Use of the SSN to obtain phone, utilities or cable television
- Benefits – Use the SSN to fraudulently obtain: supplemental Income, disability insurance, workers comp, unemployment, welfare, and tax refunds
- Banking – Use the SSN to open a bank account
- Multiple Identities – Use the number or card to create multiple identities. This activity is presumed to be indicative of future unlawful activity
- Loans – Use of the SSN to obtain a loan under the legitimate card holder ID and not that of the perpetrator
- Child Support – Use of a fraudulent SSN to avoid making mandated support payments
- Avoid Identification – Use of a fraudulent SSN to avoid identification by law enforcement
- Misc. – Unknown use of the SSN by the perpetrator

Discussions with federal law enforcement indicate that most of the counterfeit cards obtained are a result of counterfeit plant suppressions. There are two types of document plants, one that will sell a 'wallet' containing various documents, such as a driver's license, credit card, Social Security card and proof of insurance and the second that specializes in illegal immigrant documentation, such as resident alien cards, driver's licenses, Social Security cards and visas.

Card Consolidation & Replacement

Re-designing security for new cards has an immediate impact only upon new cards issued and those lost, stolen or re-issued. The balance would require approximately 16-18 years evolving into regular use. For new security features to be most effective, a complete re-issuance of cards would be necessary. Yet DSA recognizes the significant costs and impact associated with implementing such a program.

A plan might be devised to replace some card-types based on the estimated number of these cards in circulation combined with the age range of the card

holders. Specifically, those card holders with card-types issued prior to 1983 (without significant security features) and born, say, after 1952 (those between the ages of 25 and 55, who have not been re-issued a newer card-type) might be re-issued with the new card format. Additionally, since there would need to be public education on the re-issuance, it may be easier to explain reissuing cards to younger people rather than to the older card holders.

The DSA team also considered periodic re-issuance of the Social Security card as part of an ongoing process. It was noted that the longevity of the card inherently detracts from the ability to adapt to ever-changing security threats. Reducing the validity period of the card allows for security advances to be added to the card as circumstances require, and the periodic consolidation of card formats for easier recognition. Yet periodic card replacement would likely require additional funding and the development of processes not currently in place.

Education

Education for the issuers and users of a secured item is probably the single most powerful security technique available. Currently with 54 valid designs of Social Security cards in circulation, it is difficult to think of how an employer (motor vehicle clerk, etc.) could, in a short period of time, adjudicate a document presented to them. A secured web site could illustrate two or three overt security features present on the particular card type that could more easily be checked by the employer (inspector) at that time. The site would also give the SSA an opportunity to inform employers of actions that can be taken and the appropriate parties to contact upon receipt of counterfeit card. Requiring employers and/or their employees to register and log-on to this secured site would give SSA the ability to electronically monitor and audit this system.

Recommendations

Given the multitude of security technologies available, and the wide range of costs, placement and effectiveness of those technologies, some might question why one or more available security features were not recommended. Further, the specific choices of technologies are sometimes subjective and can be vulnerable to challenges by individuals with differing views. It is understood that ongoing changes in legislation, increased cost, Congressional appropriations, and technological advances may directly impact the recommendations provided herein.

The goals of the DSA team were several in their evaluation and included:

- Allowing employers to more easily ascertain, without considerable additional costs, card legitimacy
- Features visible to the naked eye were important
- The SS card is not an identity card
- Assume that the federal statutes will continue to require banknote paper.
- No major funding was provided for any increase in SS Card security

- New cards will likely not be reissued to the universe of all 300 million current number holders (more likely only to those requesting originals or replacements)

If it is the intent for the Social Security card to be relied upon as a credential to help establish individuals' identities, more serious consideration of how to enable significant upgrades to the security of the card will be required. The DSA project team focused its efforts on providing a set of recommendations that are neutral in respect to potential vendors, robust, cost-conscious and actionable. The following recommendations, considered in combination, create a version of the Social Security card that is better protected against the threats it faces today and for its continued use in employee verification. In no particular order, the recommendation summary is:

The continued use of:
- Chemical protection
- Both intaglio and offset print technologies
- A manufacturer's control number
- Card production by a security printer
- A microprinted signature line
- Impact as the source of variable print
- Optically dull or dead paper

The removal of:
- Planchettes

The addition of:
- The concurrent introduction of all implemented changes to the card
- Replacing as many versions of the Social Security card as possible with the improved security version
- A hidden message pantograph (for copying protection)
- A strong overt security feature
- Intentional imperfections
- Variable height microprinting
- Slight changes in screen tint
- Ink protection of variable data
- Year of birth and date of issue
- A personalized control number
- Auditing of security protocols
- A signature line for parent or guardian
- Expanded educational content for employers
- Expansion of the SSA website
- Ongoing threat assessments

In addition to the recommendations submitted above, there were a number of recommendations that warranted mentioning, but were outside the interpreted scope of the project. These are:

- Requesting a moratorium on the use of the full SSN on documentation
- An expansion of the SSA's on-line verification system
- An integration of the SSA's on-line verification system with law enforcement databases
- The inclusion of the card control number on IRS and other federal forms where the number is used

VI. Driver's Licenses

Driver's licenses and ID documents issued by motor vehicle agencies are used throughout North America and the world as a "right-of-access". That is, the DL/ID document is used to board airlines, to enter buildings, and to establish identity by government and financial institutions, by corporations, retail, and many other agencies charged with maintaining security and the identification of individuals. One of the greatest uses of the driver's license is to identify citizens party to a commercial transaction, and therefore, a key requirement is to protect citizens from identity theft and fraud. In addition, the events of 9/11 and the 9/11 Commission's Report leading to legislative changes in how states will issue driver licenses and ID cards in support of Homeland Security have become a major issue and States are still waiting final Rulemaking from DHS to find out what their proposed final requirements will be. DSA, using identification security principles, has recommended some of the following items to help the States and DHS combat identity theft and improve security:

Present Day Driver License Issuance

Standards and rules for card production should be applicable to all three existing production/distribution methods for issuing driver licenses and identification cards; over-the-counter, central, and hybrid issuance systems. While DSA favors central issuance production for its greater security and control value, it recognizes that all forms of issuance can be secured and time must be granted for transitioning from current to future systems.

The DSA recommends the current functional uses of the DL/ID documents must continue to be accommodated. These are: evidence of the privilege to drive, identification of the bearer, age verification, address/residence verification, and automated administrative processing.

Verification, Authentication, and Information Capture Considerations

DSA supports the electronic verification of source document information as required by the REAL ID Act, but suggests to DHS that this must only be required when the electronic systems are available (e.g., SSOLV currently is available and

should be used, but the EVVE, SAVE, and State-to-State systems must be developed), and must take active steps to protect citizen privacy. The current Social Security system is a good example where information can be validated but not retrieved using a point-to-point system without centralized hubs or data repositories that may interject additional privacy risks.

Verification is only one part of a complete validation process. It provides information matching and current status, but does not determine if the document is authentic or tie it to the card holder. DSA endorses all three forms of verification (legitimate document issuance, document authenticity, and rightful-holder) with a solution in all cases to each part.

A comprehensive and continuous training program is recommended to empower verification staff to recognize different types of identification documents. Using currently available automated equipment and machine-readable technologies will greatly help verify that the documents presented are genuine.

Use of biometric technologies (i.e., facial recognition and finger images), PINs, and digital image exchange between jurisdictions can help tie the applicant to the document.

DSA continues to strongly recommend an upgrade in the requirements for the production of and security features of "breeder documents" such as birth certificates, Social Security cards, and other documents commonly used in identification proofing for issuing driver licenses and identification cards (the DSA has also prepared a whitepaper and recommendations on birth certificates which is available upon request).

DSA continues to endorse the electronic scanning and archiving of source documents used to prove individual identification. Images should be captured in a digital format for subsequent use in authorized verification, employee training and monitoring/auditing and investigative purposes.

Validity Period and Durability for Credentials

DSA believes that eight years is too long a time for credential validity. It gives too much time for counterfeiters and forgers to find successful attacks to simulate and alter cards in circulation. As technology improves, the fraudster acquires new tools to perform fraudulent activities that are closer to authentic older credential issuances. Durability is another issue. As credentials naturally deteriorate in appearance due to wear over time, it is far more difficult to differentiate a genuine item from a fraudulent one. It makes the counterfeiter's and forger's job much easier since the quality of their criminal products can be much lower to "pass" inspection and examination. We urge DHS to strongly recommend that the States adhere to a shorter time period than the maximum eight years allowed by the REAL ID Act. We continue to suggest no more than a maximum five-year validity period.

DSA also recommended that document durability and performance standards be initiated that include the use of all appropriate substrate materials and that DHS not prescribe one component security product over another. This would allow the continued compatibility of current personalization equipment now in use for secure card issuance as well as allow the migration to more secure materials developed in the future.

Machine-readable Technology Choice

DSA continues to endorse the use of the 2D bar code known as PDF 417 as a common machine-readable technology to start this program. It is already in use by almost all jurisdictions, is very low cost to apply, and is being used currently to facilitate other automated administrative activities by law enforcement in production of traffic citations and accident reporting systems. As stated before, this is not meant to limit other machine-readable technologies from placement on credentials. It is to standardize on one feature that all credentials will contain, allowing universal interoperability. DSA recommends the information in the bar code that matches the information on the human-readable portion of the item not be encrypted. Rather, laws prohibiting collection and use should be enacted to prevent privacy infringement. To encrypt the data currently being used by motor vehicle and law enforcement agencies to validate and authenticate the information will be counterproductive or will result in encryption key management issues that will raise costs of the system while not materially improving security and privacy. Additional machine-readable technologies are being broadly deployed by the States, such as digital watermarking, which provides an effective, low-cost and covert capability to authenticate and prevent the alteration of IDs, and chip-based features, which are being tested for border crossing applications. Both features should be considered as complementary and in addition to the recommended 2D bar code that the DSA proposes as a standard feature.

Physical Security

DSA has established a set of recommended physical and material security standards and procedures/best practices for consideration. They include such areas as manufacturing, resale, shipping, handling, storage, inventory control, and issuance of components and finished products used for identification documents. Some of the DSA specific recommendations fall into the areas of:

Standards: DSA believes the NASPO-ANSI standards should be met in the design and qualification process of motor vehicle card issuance.

DSA Support

DSA and its member government and corporate alliance have volunteered to work with DHS and other agencies as needs arise in Taskforce Groups and Expert Advisory Working Groups to bring their knowledge and experience to address issues and problems in document security. DSA members represent the current and future suppliers of security documents to a wide range of State and Federal governments and stand ready to provide security counsel as needed.

VI. Public Policy Recommendations:

The DSA was created by government agencies, private industry and academia to identify methods to improve security documents and related security procedures in order to help combat the growing use of counterfeit documents in acts of identity theft and fraud, terrorism, illegal purchases of controlled substances and firearms, illegal immigration, and other criminal acts. The group is committed to develop recommendations to appropriate federal and state government agencies, private industry, and policy makers in order to improve the process and procedures surrounding document security. We encourage policy makers to further invest the appropriate resources – mindshare, time, people, and funds to ensure that our nations' identity management systems become best in class.

DSA encourages Congress to adequately fund the implementation of security initiatives for the driver's license and identification cards issued by the states. The communication of information and the realization of the goal "one driver–one license–one record" are achievable. It is important for not only security, but also highway safety, prevention of identity theft and protection of citizen privacy.

VII. Conclusion:

In conclusion, Chairman Towns, Ranking Member Bilbray, and Members of the Subcommittee, I would like to again thank you for giving the Document Security Alliance this opportunity to present our views on a wide range of document security challenges and solutions. As an alliance, we are dedicated to helping policy makers and government executives improve the security cards, systems, and processes that our nation depends on to help protect its citizens. We take this mission seriously and we hope that our discussion today has helped inform the debate in a positive way.