Stop Issuing Secure Credentials to Imposters!

Imposter fraud is rampant and fueled by easy access to personal data over the Internet.

August 9, 2012

Bruce Monk, Fraud-Free IDentity Solutions
Ron Martin, CPP, Open Security Exchange
Theodore Kuklinski, Ph.D., Advanced ID Detection

Abstract: *Much has been said about the difficulties in screening persons for possible imposter fraud or security concerns based upon use of current identity documents like birth certificates, driver's licenses or passports. The most often reasons given are the lack of standardization of security features and the layout for these documents. This criticism is focused on the inability of even a trained person to recognize valid documents and the specific parameters for each of these documents. In this paper, the focus is on the value of machine screening of the identity documents in circulation and the requirement for a standardized metric for adjudication of the identity assurance process. The distinction is between human screening and the power of machine processing. The diversity of the identity documents and the issuer's attempts to exert their own unique identity for their documents is actually a benefit to machine screening. The rich variety of specific layout and production characteristics provide many examination points for evaluation. The processing power, storage capacity, and imaging options, only recently available at a reasonable price point, make real-time examination of all of the unique properties and a subsequent risk analysis of the results a practical approach.*

INTRODUCTION: Identity documents (IDs) are often issued based on other identity documents and thus the need to authenticate the source documents becomes imperative for each credential issuance process. This is necessary until such time as trust is built that the ID presented can be reliably verified between the credential and the bearer (biometrics). There has been much discussion as to how well current primary IDs can be authenticated given the number, variety, and lack of deliberately added security features. This question is answered very well in the paper "*Automated Authentication of Current Identity Documents,"* presented in 2004 at the IEEE Homeland Security Conference in Cambridge, MA[1]. Very little has fundamentally changed in the interim. The information therein is foundational for this paper. The problem has worsened from the perspective of fraud prevention. The fuel for identity fraud is personal data and the easy accessibility to this information has exploded along with the Internet, social media, and "smart" phones. At the same time, there has been further erosion in the attention paid to the physical identity document and the skill of the examiner in detecting fakes and alterations. The quest for interoperability and faster data capture have driven initiatives like the Personal Identity Verification (PIV) card, ePassports, identity management programs, and the inclusion of 2-D barcodes on driver licenses and identity cards. The addition of biometrics (besides facial) enhances the ability to link the bearer to the credential. These trends are positive steps toward improvement in securing access and granting privileges. They are not very helpful in excluding imposters from being issued these secure IDs.

A "CHAIN OF TRUST" MUST START WITH PROOF OF A "CHAIN OF CUSTODY:" All of these digital identity trends serve to build a "chain of trust" that the credential and the information it carries is secure, is not altered, and belongs to the bearer. The concern is with the start or "anchor" point for this chain. The challenge remains how to assure that the identity claimed during the issuance process is real and belongs to the claimant. The degree of assurance that the claimed identity and the claimant are a match is the "weakest link" in the chain. A layered security approach using all available technologies is critical to ensure that each step in the identity paradigm is managed using the "best practices" available. In a recent draft of the United States Government's Federal Information Processing Standards (FIPS) 201[2] the concept of the Chain of Trust falls short on establishing a link of the identity card (which contains digital Identities) to the claimant. Impostors may assert fraudulent identity cards to establish a credential that would give them access to our nation's most sensitive information and locations. A lot of attention is made to the protection and use of digital identities. However, very little emphasis is made on the source documents used to establish cyber-identities.

The strength of identity assurance is set by the ability to determine an unbroken "chain of custody" for the identity by the claimant. The challenge of establishing a metric for identity assurance was taken up in the IDSP Workshop under the sponsorship of the American National Standards Institute (ANSI). The work of this group was presented in the "*Report of the IDSP Workshop on Identity Verification"*[3] Subsequently; this

[1] "*Automated Authentication of Current Identity Documents,"* Theodore Kuklinski, 2004 IEEE Conference on Technologies for Homeland Security, http://www.advancediddetection.com/uploads/1/0/5/6/10560305/automated_authentication_of_current_identity_documents.pdf

[2] *"FIPS 201-2,"* http://csrc.nist.gov/publications/drafts/fips201-2/Draft_NIST-FIPS-201-2.pdf

[3] "*Report of the IDSP Workshop on Identity Verification,"* ANSI Identity Theft Prevention and Identity Management Standards Panel (IDSP), October 2009, http://webstore.ansi.org/identitytheft/default.aspx

work, Identity Verification (ID-V), is being continued under the sponsorship of the North American Safety Products Organization (NASPO)[4].

HUMAN INSPECTORS CANNOT AUTHENTICATE THE MANY IDs IN CIRCULATION: There are two concerns identified in the IDSP Report. First, the process is very extensive and is largely reliant upon the skills and training of adjudicators to determine the level of identity assurance. Secondly, it places little emphasis on the authentication of the source or "breeder" documents (BD) in the process. Every day, passport and driver license application processing, border entry, and airline screening points are staffed by "adjudicators" who, at their digression, based on their training, determine if the person seeking a credential or entry privilege meets an acceptable "standard." There have been notable problems with this approach. As witnessed by many experts, "humans cannot deal with the volume and variety of the breeder documents." These experts include Asa Hutchison, Under Secretary, Department of Homeland Security in testimony before the Senate Committee on Finance September 9, 2003[5] and Michael Everitt, Unit Chief, Forensic Document Laboratory U.S. Immigration and Customs Enforcement, Senate Committee on Finance August 2, 2006.[6] A video of the full testimony for the August 2 hearing is available on CSPAN (the Everitt testimony begins at the 00:26:52 mark.) Other sources confirming the impossibility of manual breeder document authentication (BDA) and the challenges represented can be found in Appendix A.

These hearings and other Congressional committees were prompted by series of reports from the GAO regarding failures in the passport issuance process and border/airline screening processes to detect fraudulent documents (See A.8 General Accounting Office (GAO): Related Reports).

The results of the tests conducted included the issuance of passports and entry into the country based on completely fabricated identities. The fraudulent documents were immediately detected in each instance when scanned by a modern electronic reader-authenticator system.

The reality is that the Immigration form 9 or I-9[7] list of documents is all we have specified for authentication! Data is transportable, but the materials, manufacturing process and security/layout features are not. If these are verified it raises the security bar for imposters who must get genuine documents, alter stolen documents, or forge new ones. Machine (electronic) authentication is the "must have" consensus for organizations specifically concerned with credential issuance, document security, and document authentication whenever possible. Currently, the PIV issuance process is dependent on the same source documents and relies on ID proofing processes which are data-based and "breeder document" (BD) examination which is generally manual and has not been standardized across all issuers.

MACHINE AUTHENTICATION IS A MUST: The Document Security Alliance (DSA)[8] has published several documents and on Page 1 of "*DSA: Report to the Nation; An Analysis of Document Security Vulnerability*"[9] recommends, "Implementing electronic verification of breeder/source documentation as required by the Real-ID Act." In *"DSA: Call to Action: The Growing Epidemic of Counterfeit Documents and Practical Steps to Combat It"* [10], it states: "Better understanding and usage of advanced authentication technologies…" and for "ID scanning technology for routine inspections of IDs to detect counterfeits" the "Use of technology that does more than verify a barcode. Because sophisticated ID counterfeits produce bar codes that are impossible to differentiate from valid IDs, ID readers MUST be able to verify security."

Document reader-authenticators are "tools" to help the inspectors and to automatically audit the process. When humans are foundational to the process, then their limitations of skill, training, memory, emotion, intimidation, health, attention/alertness, and temptation become variables that cannot be quantified to a set standard between individuals or from one instance to the next. Automated machine processes remove human factors from the tedious tasks and can automatically audit and prompt the steps best done with human involvement.

Source "documents" should not just be those chosen from the I-9 list of primary "breeder" documents. Each of these documents is vulnerable to forgery, alteration, and imposter theft (genuine document, but wrong person!). These credentials document a point in the "chain of custody" for the claimed identity. Consideration should be given for inclusion of expired government issued IDs. These are usually traceable and often include photos to establish a biometric link over a period of time. State and federal IDs issued over the last 15 years can be read and authenticated automatically.[11] There are many such points which can be used to establish the

[4] North American Safety Products Organization, NASPO, http://www.naspo.info/idsp

[5] Testimony of Asa Hutchinson, Undersecretary, Department of Homeland Security, Directorate of Border and Transportation Security, before the Senate Committee on Finance, September 9, 2003.

[6] Michael Everitt, Unit Chief, ICE Forensic Document Laboratory, U.S. Immigration and Customs Enforcement, , Senate Finance Committee: Border Insecurity, Take Two: Fake IDs Foil the First Line of Defense. Wednesday, August 2, 2006

[7] I-9 List of Documents, http://www.uscis.gov/portal/site/uscis/menuitem.eb1d4c2a3e5b9ac89243c6a7543f6d1a/?vgnextoid=e8e31921c6898210VgnVCM100000082ca60aRCRD&vgnextchannel=e8e31921c6898210VgnVCM100000082ca60aRCRD

[8] Document Security Alliance, http://www.documentsecurityalliance.org/

[9] "*DSA: Report to the Nation; An Analysis of Document Security Vulnerability*," Document Security Alliance, 2009, http://www.documentsecurityalliance.com/forms/rtn.pdf

[10] "*Call to Action: The Growing Epidemic of Counterfeit Identity Documents and Practical Steps to Combat It*", Document Security Alliance, 2012, http://www.documentsecurityalliance.com/forms/counterfeit_solutions.pdf

[11] AssureTec Technologies, Inc.; Advanced ID Detection, LLC

continuity and strength of the chain. These events, transactions, or information points are often supported by documents or recorded in accessible databases. Pragmatically, based on time and life-cycle expense, a manual process of extensive interviews, document examination, and event/activity determination is not realistic. Simply put, there are not enough skilled people who can be kept perpetually motivated to perform the required task in an acceptable time and at the level of quality and consistency needed for mass applications, such as the issuance process for the PIV card. The terrorist or criminal will find the weakest link and exploit it. If 80% of the documents can be automatically authenticated, then much more time will be available for manual checking of those documents that do not have the attributes which can automatically authenticated. (e.g. older birth certificates, Native American Identity Documents and other paper-based records).

There has been a myth promulgated for the last 15 years that the weakness of the security features in drivers licenses, other breeder documents, and, especially birth certificates, make them impossible to authenticate and, hence of little value in verifying the identity of an individual. As described in the original paper, diversity is an aid to machine authentication and not a hindrance. 14,000 variations or 140,000 variations of a document have little meaning in terms of cost or time to process. Once trained, reader-authenticator technology can classify, extract data, and check layout/security characteristics ("documetrics") in a matter of seconds. The price point is so low for processor power, memory, storage, network bandwidth, and powerful image processing, making any breeder document authentication challenge worth taking!

MACHINE AUTHENTICATION FACILITATES AUTOMATION AND PROTECTS PRIVACY: The key to consistency, reliability, accuracy, privacy, and cost (hence security) is automation. The starting point is the collection of as much information (data and images) as possible and then verifying the consistency and accuracy of the information, all automatically. Privacy protection requires a process of information verification and not information sharing. This "trust authority" approach is described in the paper *"The Road to a More Secure Life"* [12] The concept is much the same as the Social Security Number Verification Service (SSNVS)[13] The issuance agency passes the name and social security number (SSN) provided by the claimant to the SSNVS and it returns with the status of a match. Thereby, the only information gained by the issuance agency is confirmation of agreement.

The same procedure can be followed for any information provided by the applicant in support of their claim to an identity. Privacy is fully protected since the only information sent or received is what already should be mutually known by both parties. If this is done without human intervention, then there is even further protection.

Currently; AAMVA provides eight verification applications[14] which can be queried from extracted data. One of these is the SSNVS and another is the National Association for Public Health Statistics and Information Systems (NAPHSIS) Electronic Verification of Vital Events (EVVE) system.[15] EVVE allows immediate confirmation of the information on a birth certificate presented by an applicant to a government office anywhere in the nation, irrespective of the place or date of issuance. The birth certificate issue is also addressed in a DSA paper entitled *"Call to Action: Birth Certificate Security."* [16] The authentication system could be expanded to include verification of the documetrics of the birth certificates and other vital records documents as well. Ideally the security and standardization of vital records will be improved over time. However, for a lifetime after that, there will still be a need to extract data and authenticate existing source documents.

LEGAL FOUNDATION: Anonymity is the greatest ally of those who present false identification breeder documents. From the illegal standpoint, the uses of aliases have served criminals well over the years. Because of the delay in detection, the "commonly-used" identity of a person has allowed aliases to be used to obtain privileges and access to environments for deceptive and illegal purposes.

The Federal Bureau of Investigation (FBI) states: "…*A stolen identity is a powerful cloak of anonymity for criminals and terrorists…and a danger to national security and private citizens alike…"*[17]

The primary database used by the FBI is their fingerprint database. The Integrated Automated Fingerprint Identification System, or IAFIS, is a national fingerprint and criminal history system that responds to requests 24 hours a day, 365 days a year to help our local, state, and federal partners to solve and prevent crime as well as to catch criminals and terrorists. IAFIS provides automated fingerprint search capabilities, latent search capability, electronic image storage, and electronic exchange of fingerprints and responses.

[12] "The Road to a More Secure Life," Bruce Monk, Theodore Kuklinski, PhD, Fraud-Free Identity Solutions, 2010, http://www.fraudfreeid.com/Pages/VISIONforPROSPERITY.aspx

[13] The Social Security Number Verification Service, http://www.ssa.gov/employer/ssnv.htm/

[14] **AAMVA:** Fraud Prevention and Detection, http://www.aamva.org/Fraud-Prevention-and-Detection/

[15] National Association for Public Health Statistics and Information Systems (NAPHSIS) Electronic Verification of Vital Events (EVVE) system, http://www.naphsis.org/index.asp?bid=979

[16] *"Call to Action: Birth Certificate Security,"* Document Security Alliance, http://www.documentsecurityalliance.com/forms/Birth_Certificate_Paper.pdf

[17] http://www.fbi.gov/about-us/investigate/cyber/identity_thef t

The primary challenge organizations will face will be the verification and authentication of the breeder documents used to validate and record the identity of the person being fingerprinted, whether the applicant's fingerprints get a "hit" on the IAFIS system or not. If a fraudulent credential is accepted as genuine, the resulting identity information sent to an organization would be highly suspect.

An additional challenge an organization will face is to require them to report all suspected fraudulent documents or false official papers to the cognizant law enforcement agency. Chapter 47 of Title 18 of the United States Code (USC) Fraud and False Statements[18] provide possible criminal sanctions against those individuals presenting false documents used to establish their identity to obtain or provide U.S. Federal Services. Key sections of this chapter are:

Sec. 1002: Possession of false papers to defraud United States:

> -STATUTE- Whoever, knowingly and with intent to defraud the United States, or any agency thereof, possesses any false, altered, forged, or counterfeited writing or document for the purpose of enabling another to obtain from the United States, or from any agency, officer or agent thereof, any sum of money, shall be fined under this title or imprisoned not more than five years, or both.

Sec. 1035: False statements relating to health care matters:

> -STATUTE- (a) Whoever, in any matter involving a health care benefit program, knowingly and willfully - (1) falsifies, conceals, or covers up by any trick, scheme, or device a material fact; or (2) makes any materially false, fictitious, or fraudulent statements or representations, or makes or uses any materially false writing or document knowing the same to contain any materially false, fictitious, or fraudulent statement or entry, in connection with the delivery of or payment for health care benefits, items, or services, shall be fined under this title or imprisoned not more than 5 years, or both. (b) As used in this section, the term "health care benefit program" has the meaning given such term in section 24(b) of this title.

Sec. 1038: False information and hoaxes:

> -STATUTE- "… Criminal Violation. - In general. - Whoever engages in any conduct with intent to convey false or misleading information under circumstances where such information may reasonably be believed and where such information indicates that an activity has taken, is taking, or will take place that would constitute a violation…"

One important initiative of the Federal Government that will embrace the identity evolution is The National Strategy for Trusted Identities in Cyberspace, (NSTIC)[19] The NSTIC program central tenet is *"Trusted Identities"*. "… *NSTIC provides a framework for individuals and organizations to utilize secure, efficient, easy-to-use and interoperable identity solutions to access online services in a manner that promotes confidence, privacy, choice and innovation…"*[20]

Therefore, the establishment of trusted identities is a security imperative for online transactions. The chain of trust mandated by this initiative will require responsible source/breeder document authentication.

STANDARD DOCUMENT EXAMINATION PROCESS AND FRAUD DETECTION TRAINING NECESSARY: The resolution of "exception" cases and the final decision as to issuance of the document remains in the hands of an adjudicator. In instances of questionable documents, auto-escalation of exception cases to higher-authority takes place. A directory of government agencies providing forensic document services can be found in Appendix A.12 Document Fraud Detection and Training and Services. Also listed in Appendix A are various organizations offering document fraud detection training.

Standardization of the process and the qualifications and capabilities of the equipment and people are absolute requirements in order to have a minimum consistent level of assurance.

A.11 Travel Document and Travel Document Examination References gives several references for such processes. The Real-ID Act also provides guidance for the state driver license and ID issuance process.

The *"Report of the IDSP Workshop"*[21] provides the conceptual basis for the steps in final adjudication of an applicant's credential/access request. Given the caveat expressed above, it is a good foundation to build on. It is a risk-based scoring model based on quantity and quality of information and a trained adjudicator's assessment of

[18] http://uscode.house.gov/download/pls/18C47.txt

[19] The National Strategy for Trusted Identities in Cyberspace, (NSTIC) http://www.nist.gov/nstic/

[20] http://www.nist.gov/nstic/NSTIC-Why-We-Need-It.pdf

[21] *"Report of the IDSP Workshop on Identity Verification,"* American National Standards Institute's (ANSI) Identity Theft Prevention and Identity Management Standards Panel (IDSP), October 2009, http://webstore.ansi.org/identitytheft/default.aspx

applicant behavior according to a consistent questioning and observation procedure.

Each time a new credential is to be issued to an applicant who has not previously undergone such an identity assurance process and had their identity sealed with a biometric (preferably at least two), the applicant is outside of the federated chain of trust and must go through such a rigorous process. Once the assurance process has been completed to a specific level of trust then issuance of a new or renewal credential within the same tier or lower would only need biometric validation and a check for revocation or restriction.

Higher security tiers will additionally require more extensive background checks and, possibly greater proof.

CONCLUSION: Since we are a nation of immigrant heritage and there is no birth to death biometric national identity system, as there are in some countries, there will always be a certain level of uncertainty in the proofing of a claim to an identity. The lack of such a tracking system means that all information available must be examined with the best technology available to render a judgment "beyond a reasonable doubt." Automation, quantification, standardization, and auditing reduce the number of variables that are the responsibility of the final human adjudicator. This minimizes the inconsistencies that would naturally be present if personal foibles or "corporate" preferences were allowed to determine the process and metrics used by the various organizations in a federated system, such as the PIV system. Issuing secure and interoperable credentials and tightly controlled identity management according to strict standards, loses its integrity if it allows imposters to circumvent the enrollment process using fake, altered, or stolen identities. This can be largely prevented using machine authentication of source documents and a well trained organization.

APPENDIX A: Document Fraud Related Resources

This index is a compendium of references for further research and study

TOPICS

A.1 Identity Fraud News and Data

- "*Postscript 9-11: Media Coverage of Terrorism and Immigration*"*,* William McGowan, Center for Immigration Studies, April 2003, http://www.cis.org/articles/2003/back603.html

- *"America's Identity Crisis: Document Fraud Is Pervasive and Pernicious*," Marti Dinerstein, Center for Immigration Studies, April 2002, http://cis.org/IdentityIssues-DocumentFraud

- *"Federal Jury Finds Argentinian Guilty of Producing False U.S. Military Identification Documents,"* March 20, 2012, http://www.fbi.gov/sanantonio/press-releases/2012/federal-jury-finds-argentinian-guilty-of-producing-false-u.s.-military-identification-documents

- *"Criminal Identity Theft Facts and Figures,"* Identity Theft and Fraud Resources, http://www.identityfraudresources.com/stolen_identity/criminalidentitytheft.html

A.2 Papers of General Interest

- *"Authentication, 20003,"* Center for Strategic and International Studies (CSIS), 2003, http://csis.org/files/media/csis/pubs/030501_authentication_report.pdf
- *"Document Fraud and Technology, a Double-Edged Sword,"* Barry Zellen, Jan 15, 2008, http://enterpriseinnovator.com/index.php?articleID=14174&sectionID=25
- *"The DLR ("Don't-Look-Right") Standard,*" Ron Martin, Security Today, Feb 01, 2012, http://www.security-today.com/articles/2012/02/01/the-dlr-standard.aspx/

A.3 Advanced ID Detection Papers and Presentations

_(Used with permission of AssureTec Technologies, where appropriate.)

- *"ID Reader-Authenticators - A Survey of New Technologies to Read and Validate IDs,"* Theodore Kuklinski, AssureTec Systems, International Security Conference (ISC West, April 2009), http://fraudfreeid.com/Documents/Ted%20K%2009ISCWest_DI02.pdf
- *"The Use of ID Reader-Authenticators in Secure Access Control and Credentialing,"* Theodore Kuklinski; Bruce Monk, AssureTec Systems, IEEE International Conference on Technologies for Homeland Security, 2008, http://www.advancediddetection.com/uploads/1/0/5/6/10560305/the_use_of_id_reader-authenticators.pdf
- *"Improved ID Security Using Reader Authenticators,*" Theodore Kuklinski, AssureTec Systems, Safety & Security International, Edition III, 2008, http://www.advancediddetection.com/uploads/1/0/5/6/10560305/improved_id_security_using_reader-authenticators.pdf
- *"Automated Authentication of Current Identity Documents,"* Theodore Kuklinski, AssureTec Systems, IEEE Conference on Technologies for Homeland Security, 2004, http://www.advancediddetection.com/uploads/1/0/5/6/10560305/automated_authentication_of_current_identity_documents.pdf
- *"Designing Identity Documents for Automated Screening,"* Bruce Monk, IEEE Conference on Technologies for Homeland Security, 2004, http://www.advancediddetection.com/uploads/1/0/5/6/10560305/designing_identity_documents_for_automated_screening.pdf

A.4 Fraud-Free Identity Solutions Papers and Presentations

(Used with permission of AssureTec Technologies, where appropriate.)

- *"The DMV as an Identification Document Issuer,"* Bruce Monk, AssureTec Systems; Steven J. Harrold, 3M; David Wells, Unisys; AAMVA Presentation Miami, 2002, http://www.fraudfreeid.com/Documents/AAMVAPresentationMiami.pdf

- *"Improved Border Security, Now!,"* Bruce Monk, AssureTec Systems, August 2003, http://www.fraudfreeid.com/Documents/BorderSecurityNowRev3.pdf

- "*Importance of Travel Document Authentication Technologies*," Bruce Monk, AssureTec Systems, IEEE Conference on Technologies for Homeland Security, Spring 2003, http://www.fraudfreeid.com/Documents/IEEE%20Homeland%20Security%20Presentation.pdf

- *"Document Authentication for Identity Verification,"* Bruce Monk, AssureTec Systems , GATF Advanced Security Printing Symposium, August 28, 2002, http://www.fraudfreeid.com/Documents/GATF%202002.pdf

- *"Secure Document Design,"* Bruce Monk, AssureTec Systems, Gorham International Conference on Travel and Identification, 2004, http://www.fraudfreeid.com/Documents/SECURE%20DOCUMENT%20DESIGN.pdf

- *"Building Better Security Into Identity Documents,"* Bruce Monk, AssureTec Systems , January 2004, http://www.fraudfreeid.com/Documents/BUILDINGBETTERSECURITYINTOIDENTITYDOCUMENTS.pdf

- *"Survey of New Technologies to Read and Validate IDs,"* Theodore Kuklinski, AssureTec Systems, ISC West March 31-April 2, 2009, http://www.fraudfreeid.com/Documents/Ted%20K%2009ISCWest_DI02.pdf

- *"Better Intelligence is Key to Better Security and Behavioral Profiling is Key to Better Intelligence,"* Bruce Monk, Fraud-Free Identity Solutions, 2009, http://www.fraudfreeid.com/Documents/Behavioral%20Profiling.pdf

- *"Improving On the Current Watch List Approach," ,"* Bruce Monk, Fraud-Free Identity Solutions January 2010, http://www.fraudfreeid.com/Documents/Improving%20On%20the%20Current%20Watch%20List%20Approach.pdf

- *"Improving Aviation Security,"* LinkedIN Global Security Professional Group, February 19, 2010, http://www.fraudfreeid.com/Documents/Improving%20Aviation%20Security%20Rev%20A%202_22_10.pdf

- "*Improving Security-Protecting Privacy,"* Bruce Monk, AssureTec Systems, May 2002,http://fraudfreeid.com/Documents/IMPROVING%20SECURITY_PROTECTING%20PRIVACY.PDF

- *"The Road to a More Secure Life*," Bruce Monk, Fraud-Free Identity Solutions; Theodore Kuklinski, Advanced ID Detection, LLC, December 20*10,* *http://www.fraudfreeid.com/Pages/VISIONforPROSPERITY.aspx*

A.5 Other Automated Travel Document Authentication Solution Suppliers

- 3M Safety and Security, http://solutions.3m.com/wps/portal/3M/en_US/Security/Security_Systems/
- AssureTec Technologies, www.assuretec.com
- MorphoTrust USA, http://www.morphotrust.com/pages/1009-transactions

A.6 Document Security Alliance (DSA) Papers

- *"Report to the Nation; An Analysis of Document Security Vulnerability,"* Document Security Alliance, November 2010, http://www.documentsecurityalliance.com/forms/rtn.pdf
- *"Call to Action: Birth Certificate Security,"* Document Security Alliance, November 2010, http://www.documentsecurityalliance.com/forms/Birth_Certificate_Paper.pdf
- *"Call to Action: The Growing Epidemic of Counterfeit Identity Documents and Practical Steps to Combat It",* Document Security Alliance, January 2012, http://www.documentsecurityalliance.com/forms/counterfeit_solutions.pdf

A.7 American National Standards Institute's (ANSI) Identity Theft Prevention and Identity Management Standards Panel (IDSP) Papers and Presentations

- *"The Need for Identity Verification Standards Report from the Identity Theft Prevention and Identity Management Standards Panel (IDSP), "* Graham Whitehead, NASPO,Project Leader, IDSP Workshop, Interagency Advisory Board Meeting, December 2, 2008, http://www.fips201.com/resources/audio/iab_1208/Whitehead.pdf
- *"Report of the IDSP Workshop on Identity Verification,"*American National Standards Institute's (ANSI) Identity Theft Prevention and Identity Management Standards Panel (IDSP), October 2009, http://webstore.ansi.org/identitytheft/default.aspx

- *"Report of the IDSP Workshop on Identity Verification*" Presentation: Jim McCabe, Senior Director, IDSP. American National Standards Institute; Brian Zimmer, President, Coalition for a Secure Driver's License; Graham Whitehead, NASPO, IDtrust 2010, April 13, 2010, http://websearch.internet2.edu/cs.html?url=http%3A//middleware.internet2.edu/idtrust/2010/slides/04-mccabe-id-proofing.ppt&charset=iso-8859-1&qt=Report+of+the+IDSP+Workshop+on+Identity+Verification&col=i2sites&n=1&la=en

- *North American Security* Products Organization (NASPO), ID-V Working Group, http://www.naspo.info/

- *Interagency Advisory Board Meeting Agenda*, FIPS, July 29, 2009, http://www.fips201.com/resources/audio/iab_0709/iab_072909_whitehead.pdf

A.8 General Accounting Office (GAO) Related Reports

- *"Improvements Needed to Strengthen U.S. Passport Fraud Detection Efforts,"* GAO Report: GAO-05-477, May 20, 2005, http://www.gao.gov/products/GAO-05-477

- *"Undercover Tests Show Passport Issuance Process Remains Vulnerable to Fraud."* GAO Report: GAO-10-922T, Jul 29, 2010, http://www.gao.gov/products/GAO-10-922T

- *"Undercover Tests Reveal Significant Vulnerabilities in State's Passport Issuance Process,"* GAO Report, GAO-09-447, March 2009, http://www.gao.gov/new.items/d09447.pdf

- *"Summary of Covert Tests and Security Assessments for the Senate Committee on Finance, 2003–2007,"* GAO Report: GAO-08-757, May 2008, http://www.gao.gov/new.items/d08757.pdf

- *"Security of New Passports and Visas Enhanced, but More Needs to Be Done to Prevent Their Fraudulent Use,"* GAO Report: GAO-07-1006, Jul 31, 2007, http://www.gao.gov/new.items/d071006.pdf

- *Federal Agencies Have Taken Steps to Improve E-Verify, but Significant Challenges Remain,* GAO Report: GAO-11-146, December 2010, http://www.gao.gov/new.items/d11146.pdf

- *"Continued Weaknesses in Screening Entrants into the United States*," GAO Report, GAO-06-976T, Aug. 2, 2006, http://www.gao.gov/products/GAO-06-976T

A.9 Identity Management Documents

- *"Federal Identity Management Handbook,"* Version 0.1, General Services Administration (GSA): Office of Management and Budget and the Federal Identity Credentialing Committee, December 2005, http://www.hss.doe.gov/HSPD12/ficc/FederalIdentityManagementHandbook.pdf

- *"Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance,"* Version 1.0, prepared by the Identity, Credential, and Access Management Subcommittee (ICAMSC) under the auspices of the CIO Council and at the request of the Federal Enterprise Architect, November 10, 2009; http://www.idmanagement.gov/documents/FICAM_Roadmap_Implementation_Guidance.pdf

- *Identity Management: Building Trust, Mitigating Risks, Balancing Rights*, ITAA White Paper: October 2005, http://www.techamerica.org/identity-management-building-trust-mitigating-risks-balancing-rights

- Homeland Security Presidential Directive-12 (HSPD-12), August 27, 2004; http://www.dhs.gov/xabout/laws/gc_1217616624097.shtm#1

- Real-ID Act, Public Law 109-13, 109th Congress, http://www.gpo.gov/fdsys/pkg/PLAW-109publ13/html/PLAW-109publ13.htm

- FIPS 201-1, FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION, Personal Identity Verification (PIV) of Federal Employees and Contractors, http://csrc.nist.gov/publications/fips/fips201-1/FIPS-201-1-chng1.pdf

- FIPS 201-2 (DRAFT), FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION, Personal Identity Verification (PIV) of Federal Employees and Contractors, http://csrc.nist.gov/publications/drafts/fips201-2/Draft_NIST-FIPS-201-2.pdf

A.10 Related Congressional Testimony

- *Testimony of Asa Hutchinson, Under Secretary, Department Of Homeland Security, Directorate of Border and Transportation Security, Before the Senate Committee oOn Finance, September 9, 2003,"* http://www.finance.senate.gov/imo/media/doc/091003ahtest.pdf

- *"Border Insecurity, Take Two: Fake IDs Foil the First Line of Defense,"* Senate Finance Committee Hearing, August 2, 2006, http://www.finance.senate.gov/hearings/hearing/?id=e6bcd781-dd07-7dba-c160-8c9f1ae63e89

A.11 Travel Document and Travel Document Examination References

- *"Standards for the Examination of Travel Documents,"* Asia-Pacific Economic Cooperation: *2001* http://www.immigration.govt.nz/NR/rdonlyres/5B431A87-E667-489E-8D2F-1C9C5FFC3420/0/APECBMGTravelDocExaminationStandardsFINAL.doc

- *"ICAO Guide for Assessing Security of Handling and Issuance of Travel Documents,"* International Civil Aviation Organization (ICAO), October 28, 2009, http://www.icao.int/Security/mrtd/Pages/Assessment-Guide.aspx

- *Guide for the Development of Forensic Document Examination Capacity,* Laboratory and Scientific Section, United Nations Office on Drugs and Crime, http://www.unodc.org/documents/scientific/Forensic_Document_Examination_Capacity.pdf

A.12 Document Fraud Detection and Training and Services

- ICE: Forensics Document Lab; Department of Homeland Security, Immigration and Customs Enforcement, http://www.ice.gov/hsi-fl/

- Fraud Prevention and Detection, AAMVA, http://www.aamva.org/Fraud-Prevention-and-Detection/

- *Fraudulent Document Detection and Traveler Identification Security Measures,* Customs and Border Patrol (CBP), Department of Homeland Security, http://www.cbp.gov/linkhandler/cgov/newsroom/fact_sheets/travel/frad_doc_detect.ctt/frad_doc_detect.doc

- *"Training to Identify Fraudulent Travel Documents,"* GAO Report: List of Agencies, http://www.gao.gov/modules/ereport/handler.php?1=1&path=/ereport/GAO-12-342SP/data_center/International_affairs/21._Training_to_Identify_Fraudulent_Travel_Documents

- *"Fraudulent Document Recognition Training E-Learning Implementation Guide,"* AAMVA, http://www.aamva.org/WorkArea/DownloadAsset.aspx?id=1310

- Fraudulent Document Recognition Training Program, AAMVA, http://www.aamva.org/FDR-Training/

- Fraudulent Document Recognition Training: Helps Staff Spot Fake or Altered Proof-of-Identity Documents – Morphotrust, http://www.l1id.com/pages/628-fraudulent-document-recognition-training

- *"Guide to U.S. Travel Documents*," Department of Justice, M-396, 11-2011, http://www.justice.gov/crt/about/osc/pdf/publications/FormM_396.pdf

- *Electronic Verification of Vital Events (EVVE),* National Association for Public Health Statistics and Information Systems (NAPHSIS), http://www.naphsis.org/index.asp?bid=979

- The Social Security Number Verification Service, http://www.ssa.gov/employer/ssnv.htm/