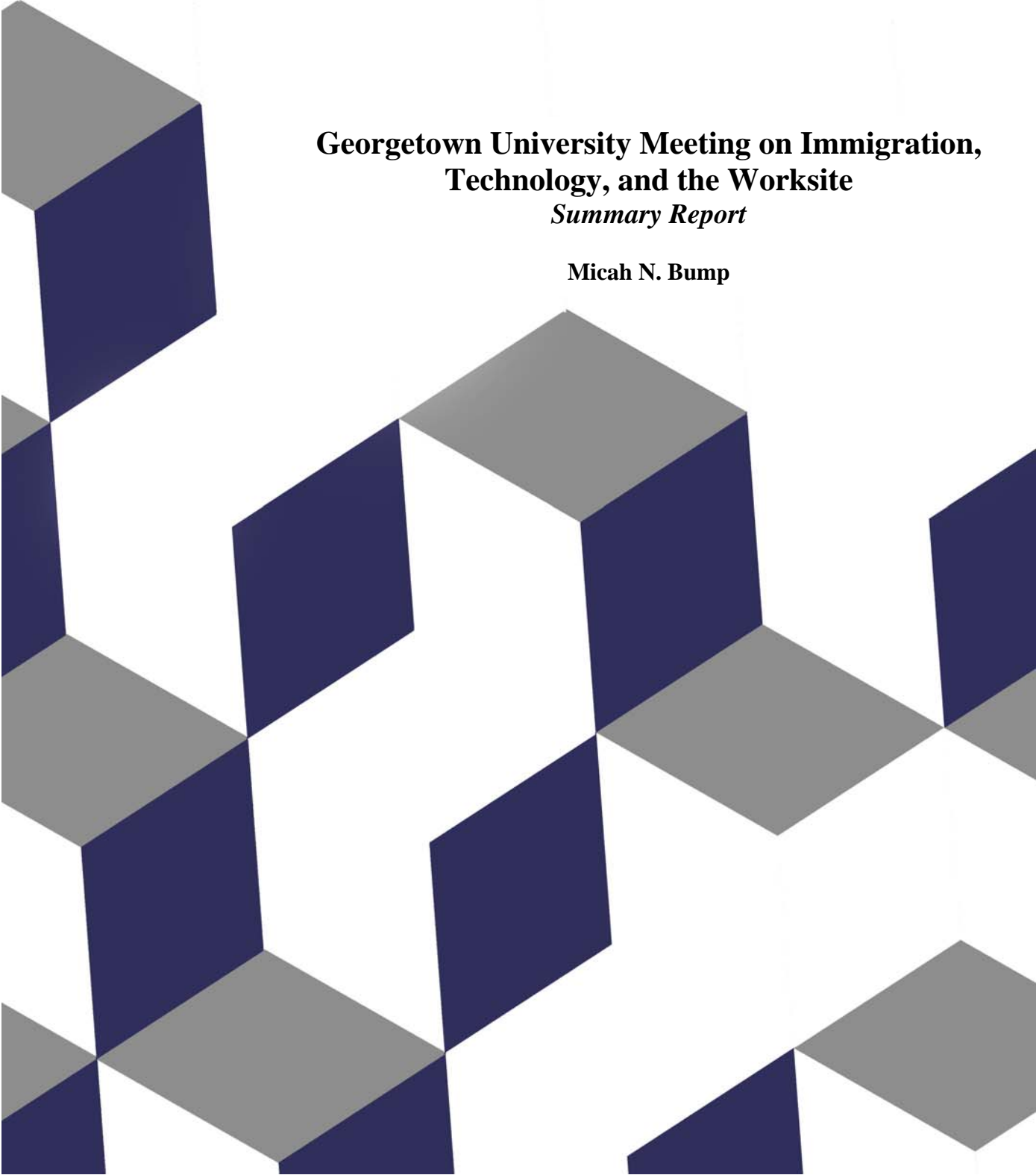


April 2007



**Georgetown University Meeting on Immigration,
Technology, and the Worksite**
Summary Report

Micah N. Bump

Georgetown University Meeting on Immigration, Technology, and the Worksite April 2007

Summary Report

Today, a combination of high levels of undocumented migration, problematic enforcement mechanisms and employer demand for legal workforce, suggest the need for a reformed, credible system to manage immigration at the worksite. Over the course of the past three decades, numerous studies by analysts in government, academia, and the non-governmental community have set forth options and recommendations for systems of verification of work authorization. Some of the options rejected or deemed unfeasible in the past are worthy of reconsideration, especially given the advances in communications, biometric, and database technology over the past decade. At the same time, the possibilities and limitations of current technology must be understood in order to sensibly assess the current options for an electronic employment verification system.

In the interest of furthering our understanding of immigration and the worksite and developing concrete steps for comprehensive reforms, ISIM hosted a roundtable meeting with experts to discuss the technical issues and policy implications surrounding an electronic worksite employment verification system. The meeting was held on April 9, 2007 and brought together representatives from government, business, non-governmental organizations, and academia.

The technical and policy experts present at the roundtable categorized the specific concerns with the current electronic employment verification system as well as any future system into the following categories:

- **Accuracy and Compatibility of Information:** The reliability of any electronic employment verification system depends heavily on the quality and compatibility of the information stored in the multiple databases used to verify information. If there is inaccurate or incompatible information, the system will be plagued by

errors leading to user frustration. Furthermore, the accuracy and validity of documents or other identifiers presented by a worker is of paramount importance to the success of the system, bringing into question issues of secure document technology and biometrics.

- **Scalability:** Currently, less than one half of one percent of all employers participates in the Basic Pilot, the current electronic verification system. Thus, if a mandatory system were put in place for all employers, there are concerns about how to scale the current system up to meet the demands of approximately 7 million employers. In addition to the scalability of the database architecture, increased staffing and funding needs must be taken into account.
- **Accessibility and Education:** While many employers may prefer a web-based interface for employment verification, smaller employers may not have access to a computer or be computer literate. Even among those who are computer literate, there is a need for training on the proper use and ramifications of misuse of the verification system.
- **Privacy Concerns:** Issues such as database access control, secure data transmission, and concerns about documentation required for the electronic employment verification system being construed as a National ID are important aspects to take into account.

Background

The Immigration Reform and Control Act (IRCA) of 1986 made it illegal to knowingly hire an unauthorized worker and required employers to verify that all employees hired after November 6, 1986 have proper work authorization. The IRCA legislation created a paper based employment verification system, commonly referred to as the I-9 process, in which the employee completes an I-9 form and presents documentation to establish identity and work authorization. The system has been plagued by problems stemming from the counterfeiting and fraudulent use of documents as well as abuse by employers. In an effort to reduce these problems the U.S. Commission on Immigration Reform, which operated between 1993 and 1997, recommended a telephone/computer verification system.

This recommendation was implemented as a pilot under the Illegal Immigration Reform and Immigrant Responsibility Act of 1996. The Basic Pilot Program, as the system came to be known, began operating on a trial basis in five states in 1997 and in a sixth state in

1999. In 2003, Congress extended the functionality of the Basic Pilot program to all 50 states under the Basic Pilot Program Extension and Expansion Act of 2003. In 2007, the Basic Pilot Program's name was changed to Electronic Employment Verification System (EEVS). Unlike the I-9 process, the program remains voluntary and, according to DHS, approximately 17,000 employers (out of 7 million nationally) use the Basic Pilot, representing approximately 56,000 work sites across the country. About 1,000 new users join per month. Beginning in 2004, employers could use the internet to submit verification requests. Its principle purpose is to combat the widespread document fraud that undermines the I-9 process.

The Basic Pilot program allows employers to check the information provided by all employees with the NUDIMENT database at the Social Security Administration (SSA) and 6 different databases at the U.S. Department of Homeland Security (DHS). The program is conducted by the DHS Bureau of U.S. Citizenship and Immigration Services (USCIS) with support from SSA. The system uses social security numbers (SSNs), Alien Registration Numbers (A-numbers), and/or I-94 numbers provided by employees and checks them against the information provided in the government's databases.

Accuracy of Information

Database Management

Updating the databases currently used by the Basic Pilot for employment verification in a timely fashion continues to challenge government agencies. According to a GAO report, the primary reason for non-confirmations are errors caused by delays in entry of employment authorization information into DHS and SSA databases.¹ For instance, when an immigrant naturalizes as a U.S. citizen this information is not automatically updated in the SSA database and often times the individual has to proactively request the SSA to update his file. The Basic Pilot Program Extension and Expansion Act, which authorized the national expansion of the Basic Pilot, required DHS to submit a report by June 2004

¹ Government Accountability Office, Immigration Enforcement: Weaknesses Hinder Employment Verification and Worksite Enforcement Efforts, GAO-05-813, Aug. 2005. <http://www.gao.gov/new.items/d05813.pdf>.

to Congress that addressed whether the problems identified by the 2002 independent evaluation of the Basic Pilot had been substantially resolved, and it should have outlined what steps the DHS was taking to resolve any outstanding problems before undertaking the expansion of the Basic Pilot program to all 50 states.² Advocacy groups argue that the report submitted by DHS to Congress “failed to address the explicit recommendation by the independent evaluation against expanding the Basic Pilot program” into a large-scale national program until the DHS and the SSA address the inaccuracies in their databases that prevent those agencies from confirming the work authorization of many workers.³

Recent reports uphold the assertions of worker advocacy groups. The SSA estimates over 4 percent of its records (approximately 18 million individuals) have errors related to the person’s name, birth date, and citizenship status.⁴ Nine percent of the non-citizens who are authorized to work in the United States are initially incorrectly identified as not authorized.⁵ Database errors currently make foreign-born workers, including naturalized citizens 30 times more likely than U.S. citizens to be incorrectly identified as not authorized for employment.⁶ Congress has authorized the use of the Basic Pilot through 2008, and, given its current expansion, it is likely it will be extended. The immigration reform bills that passed the House and Senate in 2005 and 2006, the Border Protection, Antiterrorism, and Illegal Immigration Control Act of 2005 (HR 4437) and the Comprehensive Immigration Reform Act of 2006 (S 2611), would have mandated use of the Basic Pilot. According to a 2007 report of the SSA’s Inspector General, if the Basic Pilot were to become mandatory and the databases were not improved, database errors

² Written Statement of Tyler Moran, Employment Policy Director, National Immigration Law Center, and House Committee on the Judiciary Subcommittee on Immigration, Citizenship, Refugees, Border Security, and International Law Hearing on: Proposals for Improving the Electronic Employment Verification and Worksite Enforcement System April 26, 2007. Available at http://www.nilc.org/immsemplymnt/cir/eevs_testimony_nilc_2007-05-03.pdf

³ Ibid.

⁴ Congressional Response Report: Accuracy of the Social Security Administration’s Numident File (Office of the Inspector General, Social Security Administration, Dec. 2006), www.socialsecurity.gov/oig/ADOBEPDF/audittxt/A-08-06-26100.htm

⁵ Interim Findings Of The Web-Based Basic Pilot Evaluation (Westat, Dec. 2006)

⁶ Interim Findings Of The Web-Based Basic Pilot Evaluation (Westat, Dec. 2006)

could result in 2.5 million people a year being misidentified as not authorized for employment by SSA.⁷

Timely and accurate resolution of problems is also due to the government databases used for worksite verification which not only include data inaccuracy, but also lack the cross-compatibility of data systems. During the initial phase of the Basic Pilot program, compatibility problems between the former-INS and SSA databases issues hampered the usefulness of the system. For instance, the INS used A-numbers for verification but only 10 percent of INS database members also had the SSN in their database. A two-stage model was implemented as a partial solution to this problem. Currently, the information the employer enters through the Basic Pilot website is verified against the DHS and SSA databases. The SSA checks the person's name, social security number, date of birth, and citizenship status for accuracy. Newly naturalized U.S. citizens often do not appear as such in the SSA database, so these cases are forwarded to DHS for additional verification. DHS handles the verification of employment status for all non U.S. citizens. In most cases, the information provided by the worker will match the information contained in SSA and DHS databases and no further action is required. If however, an employee's information cannot be verified, SSA will send the employer a tentative nonconfirmation. If the verification problem is on the DHS side, the employer will receive notification of "DHS verification in progress."⁸

DHS does not have access to all of the social security numbers of migrants legally authorized to work in their system, and SSA does not have A-numbers in their database, so it still is not possible to have a single seamless system. The lack of matched data increases the need for secondary verifications, which was one of the major criticisms of

⁷Congressional Response Report: Accuracy of the Social Security Administration's Numident File (Office of the Inspector General, Social Security Administration, Dec. 2006), www.socialsecurity.gov/oig/ADOBEPDF/auditxt/A-08-06-26100.htm

⁸ Government Accountability Office, Immigration Enforcement: Weaknesses Hinder Employment Verification and Worksite Enforcement Efforts, GAO-05-813, Aug. 2005. <http://www.gao.gov/new.items/d05813.pdf>.

the 2002 Basic Pilot evaluation⁹ and continued to be of concern to the meeting's participants.

Furthermore, under the current Basic Pilot system, in the case of any secondary verification, the onus is on the employee to prove that the non-confirmation was an error. This is problematic in the sense that the primary reason for non-confirmations is delays in entry of employment authorization information into DHS databases.¹⁰

Technical experts who participated at the roundtable had differing opinions on whether or government databases could be successfully integrated. One view suggested that two or more databases at two different agencies will never be integrated. Federal computer systems are extremely complex and when multiple agencies are involved there are multiple security perimeters, multiple budgeting issues, political conflicts between agencies, as well as political conflicts outside agencies all working against integration. However, a contrasting view was that agencies can get databases to work together, but it will take significant time and resources to fix them. One participant observed that police officers who make traffic stops are able to access Department of Motor Vehicle databases and those that include information about criminal activity.

Secure Documentation and Biometrics

While the Basic Pilot has been successful in lowering the use of counterfeit documents, participants indicated that the current system cannot effectively detect identity fraud. Any electronic system of worksite employment authorization must take the issues of fraudulent, stolen, or borrowed documentation into account. Current identity verification systems, at the workplace and beyond are based on a person either (1) possessing a document or documents that verifies their identity, or (2) possessing specialized knowledge, such as a password or code to gain access. The first approach is flawed because if a document is lost, stolen, or counterfeit, it can be used by another person to

⁹ INS Basic Pilot Evaluation Summary Report." January 2002. Prepared by Institute for Survey Research, Temple University, Washington, DC and Westat, Rockville, Maryland.

¹⁰ Government Accountability Office, Immigration Enforcement: Weaknesses Hinder Employment Verification and Worksite Enforcement Efforts, GAO-05-813, Aug. 2005. <http://www.gao.gov/new.items/d05813.pdf>.

falsify an identity. The flaw of the second system is that if the password is too short it can be cracked and if it is too complicated it is hard to remember, leading the owner to write it down, which, in turn, could lead it to be lost or stolen. Moreover, the proliferation of passwords for a numerous societal purposes leads owners to record even simple passwords in writing.

The use of biometrics, defined as the study of methods for uniquely recognizing humans based upon one or more intrinsic physical or behavioral traits, is often seen as a solution to the weaknesses of current verification systems because if a person's physical traits are used as an access key, it will be more difficult to use documentation obtained through theft, fraud, and misuse. Biometric traits cannot be forgotten, lost, are difficult to copy, share or distribute and require the person requesting validation to be present.

Furthermore, when used with traditional verification techniques biometrics enhances existing systems without the need to replace them. Biometric systems for identification have been implemented by many countries, including the U.S. For instance, the U.S. Department of Defense Common Access Card is an ID card issued to all US Service personnel and contractors on US Military sites. The ID card contains biometric data and digitized photographs. There have been over 10 million common access cards issued as of April 2007.

While using biometrics technology to create more secure documents and identity verification systems is often proposed as a solution to secure documentation challenges, participants at the roundtable were quick to point out that biometrics should be viewed as a tool, rather than a solution and that there are risks to placing excessive trust in a technological solution. The first issue discussed was how the U.S. would enroll all eligible workers in a biometric system, given that there are a little over 150 million workers in the U.S. economy. Presumably, individuals would have to present documentation verifying their identity and work eligibility to initially join the system, which means the biometric system would be dependent on the quality of breeder documents.

Reliance on “breeder documents,” which are documents designed to verify other documents or identity, is one of the major weaknesses of a biometric system. The most common breeder documents are birth certificates, social security cards, and driver’s licenses. If the breeder documents do not match the person presenting them, then biometric data will not be tied to the proper identity. Problems arise because there is no standardized means to verify that information contained in breeder documents is legitimate. The primary ways in which breeder document fraud occurs are by obtaining breeder documents under false pretenses or counterfeiting/altering breeder documents. If too much faith is placed in a biometric system based on insecure breeder documents, the resulting problems could make the situation worse than it is at present.

Birth certificates are commonly used to get other breeder documents such as social security cards and drivers licenses. A 2000 study conducted by the Office of the Inspector General concluded that “efforts to make the birth certificate into a reliable identity document are complicated by the more than 14,000 different legitimate versions in existence, and the more than 6,000 entities which issue them and the processes they use to do so. Efforts are also complicated by the ease with which birth certificates can legitimately be obtained and counterfeited, and the fact that the majority of fraud is now being committed by imposters.”¹¹ Furthermore, any effort to use technology and tighter access control to improve the birth certificate integrity must be balanced with the original purpose of providing the public easy access to the documentation and record of a birth

Fraudulent or stolen birth certificates can be used to gain access to a social security card. Social security cards can, in turn, be used to verify employment eligibility. There have been numerous legislative efforts to safeguard Social Security cards from counterfeiting, tampering, alteration, and theft; improve the system of verification of documents submitted for the issuance of primary cards and replacement cards; and increase enforcement against the fraudulent use or issuance of Social Security numbers and cards.

¹¹ United States Office Department of Health and Human Services, Office of Inspector General, <http://oig.hhs.gov/oei/reports/oei-07-99-00570.pdf>

Nevertheless, the social security card remains vulnerable to fraud and the database used to store and verify information is flawed.¹² This problem is exacerbated by the existence of multiple valid versions of the card; some of them over 20 years old and easily counterfeited.

A third type of breeder document, the driver's license, has historically been easily obtained with a birth certificate or a social security card. Many states have implemented stricter measures for obtaining drivers licenses after the events of September 11, 2001. At the same time, many states have upgraded the security features of driver's licenses using security features such as biometrics, holograms, magnetic strips, and scanable bar codes. In 2005, Congress passed the Real ID Act which created national standards for the issuance of state driver's licenses and identification cards. The Real ID Act stipulates that driver's license and state ID card applicants must prove that they are either U.S. citizens or lawfully present in the U.S.¹³ These standards are to be met by states by the end of 2009.

Participants expressed concerns about the usefulness of the Real ID Act for purposes of worksite verification. While most observers support the notion of creating more secure documents, they see the Real ID act as an imperfect solution to the problem of worksite verification because "one in ten working Americans does not drive,...not everyone who is eligible for a REAL ID license is also work-authorized, and...the cards still leave 51 different state-level designs in place."¹⁴ The legislation was not created with the purposes of creating a secure document to be used for worksite verification, but rather to provide greater control over the access to government buildings and airports. Thus, any attempt to use a more secure driver's license as an employment verification document would need to take into account the differences that would still remain even after states produce Real ID compliant cards. For instance, although Real ID compliant cards would have

¹² See 2002 Supplemental Appropriations Act for Further Recovery From and Response to Terrorist Attacks on the United States (P.L. 107-206); The Intelligence Reform and Terrorism Prevention Act of 2004 (P.L. 108-458); and The Real ID Act, (P.L. 109-13).

¹³ The Real ID Act, (P.L. 109-13).

¹⁴ Rosenblum, Marc. US Immigration Reform: Can the System be Repaired?, The Center for Comparative Immigration Studies, University of California, San Diego. Working Paper 132, January 2006. p. 15. <http://www.ccis-ucsd.org/publications/wrkg132.pdf>,

swipeable magnetic strips there is still a problem of standards and lack of encryption. Any document presented by a driver's license/ID applicant to prove his or her identity, date of birth, Social Security number, and residence will have to be verified by the agency that issued the document. This again raises concerns about the reliability and expediency of government databases. The lack of encryption is a problem because of the need to safeguard private information.

Biometrics specialists participating at the roundtable explained that there are several different types of biometric characteristics that could be used in a secure document or other types of identification system. The most common biometrics currently in use today are physiological and the most common are based on a person's fingerprints. Participants discussed recent research from the Institute of Electrical and Electronics Engineers, Inc., indicating that there is a certain degree of non-uniqueness to fingerprints and preferably 10 but at least more than one print is necessary to have an acceptable level of assurance. Other examples of physiological based biometrics include face recognition, hand geometry and iris recognition, but only face recognition, in addition to finger prints, is being developed for immigration related documentation purposes.

Given that fingerprinting is the most commonly used biometric identifier and may not be 100 percent unique, any employment verification system using biometrics would have to set a threshold rates for false positive rates and false negative identifications. The false positive rate is the probability that the biometric verification system would incorrectly indicate a positive match between the biometric input and a record stored in the database. The false negative rate is the probability that the system would incorrectly indicate a negative match between a biometric input and the data stored on the system. Setting a threshold for both rates is critical because non-permitted individuals must be kept out of the system and permission must be granted to those with access.

While the discussion focused heavily on the limitations of biometrics, participants acknowledged the importance of "not letting the best be the enemy of the good." There was widespread agreement that any improvement over the current situation would be

welcome and that the focus should remain on raising the costs to unauthorized employment. As part of this discussion, a representative of USCIS indicated that DHS had just begun a Photo Screening Tool Pilot Program as an enhancement to the Basic Pilot Program. The program, which was designed for a three month pilot allows employers to compare Lawful Permanent Residence cards and other employment authorization documents containing photographs presented by new employees during the hiring process to the official photographs stored in DHS databases. While the program adds another level of security for employers during the hiring process, worker advocates expressed concern that it would be used to discriminate against foreign sounding or looking workers with work eligibility and stated that it was unclear how much this would decrease identity theft.

Scalability:

The roundtable participants highlighted the fact that to date, the Basic Pilot has only functioned as voluntary pilot system. The system has approximately 17,000 users, representing about 0.2 percent of all employers nationwide. Although the system is garnering around 1000 new employers per month, about half of the current users are deemed to be inactive. If the current system were made mandatory it would have to be successfully scaled to meet the demands of about 7 million employers. Recent expert testimony on this topic indicated that “as a general rule, each time a system grows even ten times larger, serious new technical issues arise that were not previously significant.”¹⁵

Given the concerns about current levels of data accuracy, data compatibility, and employer misuse of the Basic Pilot, there are serious questions about the efficacy of a massively scaled-up version. Even if the current system were flawless, the fact that it would work for a small number of employers does not necessarily imply that it would work for a large number of employers. A mandatory nationwide system would scale the number of queries on the system up about 20 to 30 times the current level, but would scale the number of employers up approximately 400 times the current level. Since many

¹⁵ Neumann, Peter, Testimony Before the Subcommittee on Social Security of the House Committee on Ways and Means - Security and Privacy in the Employment Eligibility Verification System (EEVS) and Related System, June 07, 2007. <http://waysandmeans.house.gov/hearings.asp?formmode=view&id=6099>

of problems are with employer non-compliance this is a relevant economy of scale problem—especially since smaller/more informal employers would begin to participate.¹⁶

Representatives from DHS and SSA reported that, at present, approximately 92 percent of all current queries on the SSA database get an automatic response within three seconds. In Fiscal Year 2005, SSA handled approximately 980,000 queries; in FY 2006, over 1,740,000 and as of May in FY 2007, more than 1,800,000 queries, an increase of 96 percent over the same period in 2006.¹⁷ If the current pace continues for FY 2007, there will be over 3,000,000 inquiries. If the system was scaled up from the current level of 17,000 employers to approximately 7 million employers the number of queries on the system would increase exponentially. Thus, the current rate of 8 percent of non-automatic response would need to be reduced significantly in order to keep levels of frustration among employers and the need to conduct manual reviews to a minimum.

Approximately 1-2 percent of the 8 percent of individuals who do not receive immediate confirmation personally appear to contest their cases in SSA office. The foreign born are disproportionately represented in this sample because when a foreign-born resident naturalizes, the new citizenship status is not automatically updated in the SSA database. Currently, manual review of the queries that do not receive an automatic confirmation take considerable time, usually 8-10 days to complete. A government representative at the meeting stressed that if the current system were to become mandatory on a national scale, more flexibility beyond the 8-10 days would be required. Apart from being expensive, manual review is troublesome to some because it is an unevaluated, unmonitored system.

Participants expressed the need to accurately budget for the additional costs implied by the expanding human resources, associate programming, and equipment necessary to

¹⁶ ISIM, Georgetown University Experts Roundtable on Immigration, Technology, and the Worksite, April 9, 2007.

¹⁷ Streckewald, Frederick G., Assistant Deputy Commissioner for Program Policy Office of Disability and Income Security Programs, Testimony Before the Social Security Administration Testimony Before the Subcommittee on Social Security of the House Committee on Ways and Means, June 07, 2007. <http://waysandmeans.house.gov/hearings.asp?formmode=view&id=6093>

carry out such a system. One participant highlighted the results of recent research on the costs of the Systematic Alien Verification for Entitlements (SAVE) Program,¹⁸ indicating that each automatic verification costs between 20 and 48 cents, but that each manual verification cost conducted by an Immigration Status Verifier (ISV) costs 6 dollars. Approximately 10 million queries on the SSA database would cost about 6 million dollars, most of which would be in manual response. Nevertheless, another government representative reported that models for a mandatory national scaling suggest there would be no need to have more than 60 verification staff or ISVs.

Accessibility and Education

The implementation of a nationwide system for employment verification needs to take into account the fact that there will be many different types of employers remotely accessing the system. Participants pointed out that there is a large range in employers and employees as well as the location of employers. The employer who hires a day laborer to work in construction or agriculture will often not have the same resources or computer literacy as a business hiring an executive. Many of the smaller employees may lack the computer access or high-speed Internet access necessary to run a real-time verification system. Thus, any verification system would have to consider the start-up costs for these small businesses as well as alternatives such as telephone verification. It is equally important to consider the vulnerabilities to internet identity theft scams that inexperienced users, and the system as a whole, would face as a result of a mandatory system.

Moreover, education on the proper use of the system will be necessary given the levels of employer confusion and misuse with the current system. The GAO, as well as two independent reviews of the Basic Pilot Program conducted by WESTAT and Temple

¹⁸ The SAVE Program is responsible for administering programs involving customer access to information contained in the Verification Information System (VIS) database. This database is a nationally accessible database of selected immigration status information on over 60 million records. The SAVE Program enables Federal, state, and local government agencies and licensing bureaus to obtain immigration status information they need in order to determine a non-citizen applicant's eligibility for many public benefits. The Program also administers employment verification pilot programs that enable employers to quickly and easily verify the work authorization of their newly hired employees.

University has found unacceptably high instances of employer misuse that diminish the effectiveness of the system and which can adversely affect potential hires. Problems such as employers circumventing training on the use of the system by sharing entrance passwords, using the program to prescreen potential employees, reverify employees already approved, limiting work hours or training until permission is obtained, entering the same information for multiple workers have all occurred. Adequate training must be carried out in order to avoid abuses and focus limited resources on employers with malicious intent to skirt the system.

Several workshop participants pointed out that employers, more than anything else, want to be able pre-screen their applicants. They have this desire because they do not want undocumented workers on their payroll for liability reasons and they do not want to train someone they will have to fire. The Basic Pilot specifically requires that the employer *not* pre-screen. The fact that they cannot use the systems to check eligibility before hire has left some employers wondering whether it is worthwhile to participate in the Basic Pilot. While it is important to ensure that the program not be used for discriminatory purposes, the needs of employers to quickly and accurately verify their workforce must also be considered.

Privacy Concerns

There was universal agreement that the type and level of information that would be communicated across networks and stored on government databases would include the most important identity variables used for individuals residing in the U.S. Thus, the threat of destruction, misuse, loss, theft, or modification of identifiable information carried on an electronic employment verification database could be devastating to the individuals affected; and it could be harmful to the overall effectiveness of the system depending on the level of the breach. Therefore it is critical that the data on the system be highly protected. The security of the data stored on the system is of paramount importance and should take precedence over speedy processing times. The tradeoff between privacy and effective, non-discriminatory verification is complex. The semblance that a secure employment verification document would have to a National ID system is important to

take into account because of the strong backlash that would come from the civil liberties lobby.

While the participants did not delve deep into technical detail on the exact methods of securing data, they highlighted the need to secure data during transmission over the internet, educate users on internet identity theft and internet scams, secure the data on government as opposed to private databases, and conduct staged and ongoing evaluations of data security both during and after implementation. The privacy concerns of individuals must be upheld and thus, the system should have a method for notifying individual if their identity is compromised. A nationwide employment verification system would be accessible by tens of millions of individuals, which highlights the challenge of maintaining accountability for access to the system and controlling unauthorized access. The system should be able to log user access and have strong security measures controlling access.

The discussion on privacy touched on the difference between a “data-heavy” and “data-light” approach to identity management. Solutions requiring a secure identity card such as the REAL-ID or the Department of Defense Common Access Card are “data-heavy” approaches in the sense that they require an ID that contains high levels of personally identifiable information. From a privacy protection point of view, “data-heavy” approaches are not ideal. Participants suggested that the debate should move beyond the notion that a secure “data-heavy” document is needed for worksite verification. They argue that the need for secure documents is an artifact of a system which did not have ability to do real time verification. Furthermore, documents are expensive, they wear out, must be replaced, and no matter how secure they are made, they are still vulnerable to problems caused by counterfeiting and fraud, which leads to the vulnerability of private information. This is the approach used by the United States Visitor and Immigrant Status Indicator Technology (US-VISIT) immigration and border management system. While the person using US-VISIT needs to provide the government with biometric and other personal data, each individual is assigned a random number and that number was the only thing anyone outside of government could see. Individuals carry a black card with a

number printed or embedded in it and allows the user to access certain rights and privileges.

A similar program could work in the realm of worksite enforcement. Instead of requiring the worker to present a secure document at the worksite, the potential employee would first present themselves at a federal government office (such as a post office) where they would present biometric data and other documentation supporting their work eligibility. In exchange, they would be issued a secure number like that used in US-VISIT and that number would be presented to a potential employer. The employer could, in turn, enter that submit that number electronically to verify that the number matches the individual. The employer initiated query would produce a biometric such as a picture that would aid in verifying the worker's identity. While this program would still be susceptible to breeder document fraud and require database improvement, it is lens for viewing approaches to worksite enforcement that would, in large part, remove the employer from the document verification process. The criticism is that the employer would still have to make a judgment about the information returned to them after running a query on the number presented by the worker.

Conclusions

It is safe to assume that the need for an effective method to quickly verify employment eligibility will continue into the foreseeable future. The immediate need for an effective, fast, and reliable system must be balanced against privacy concerns and the reality that it will take significant time and resources to update and integrate existing databases, as well as to develop and test a new architecture for employment verification. There is a sentiment among some policymakers and members of the public that advances in biometric and database technology can allay the problems faced by current systems. The discussion left no doubt that technology in general and biometrics in particular should not be viewed as a panacea but rather as a tool in a more comprehensive approach. Given the pitfalls of the current system, the implementation of an electronic employer verification system should be gradual, taking into account issues related to scalability, education, user management, data quality and control as well as privacy. Implementation in the near term

should not cause detriment to what may need to be done a decade in the future. Some participants reminded the group, however, that Basic Pilot was legislated more than ten years ago—which should have given ample time to work out existing problems. They hoped we would not be meeting ten years from now to discuss these same issues, with little progress towards full implementation of a reliable employment verification system.

PARTICIPANTS

Steve Barry

MITRE

Josh Bernstein

National Immigration Law Center

Darrell Blevins

U.S. Social Security Administration

Micah Bump

Institute for the Study of International Migration

Kevin Copping

U.S. Government Accountability Office

Tony Cresswell

University at Albany, State University of New York

Lisa Cugini

Citigroup

Joan Friedland

National Immigration Law Center

Bruce Friedman

Department of Homeland Security

Jim Harper

Cato Institute

Robert C. Hill

Hill & Associates, PLLC

Tamar Jacoby

Manhattan Institute

Barry Kefauver
Fall Hill Associates, LLC

Nadia Khawaja
U.S. Department of Homeland Security

Rey Koslowski
University at Albany, State University of New York

Kathy Lotspeich
U.S. Department of Homeland Security

Lindsay Lowell
Institute for the Study of International Migration

Michael Martin
MITRE

Susan Martin
Institute for the Study of International Migration

Robert Mocny
U.S. Department of Homeland Security

Tyler Moran
National Immigration Law Center

Bruce Morrison
Morrison Public Affairs Group

Cassandra Ogren
International Brotherhood of Teamsters

Yvette Pena Lopes
International Brotherhood of Teamsters

Amelia Post
Institute for the Study of International Migration

Gerri Ratliff
U.S. Citizenship and Immigration Services

Jaime Roberts
U.S. Government Accountability Office

Lisa Roney

U.S. Citizenship and Immigration Services

Marc Rosenblum

University of New Orleans

Andy Schoenholtz

Institute for the Study of International Migration

Michele Waslin

National Council of La Raza

Brian Zimmer

Kelly Anderson & Associates, Inc.