The Next Generation of E-Verify
Getting Employment Verification Right

By Doris Meissner and Marc R. Rosenblum
Migration Policy Institute

July 2009

Acknowledgments

The authors wish to express their appreciation for the review of this report and helpful observations offered by James W. Ziglar, Senior Counsel, Van Ness Feldman law firm and former Commissioner, Immigration and Naturalization Service; Gerri Ratliff, Deputy Associate Director, National Security and Records Verification at US Citizenship and Immigration Services, as well as other USCIS staff; Lisa Roney, former Director of Research and Evaluation, Office of Policy and Strategy, USCIS; Michele Waslin, Immigration Policy Center; Tyler Moran, National Immigration Law Center; and Joanne Lin and Chris Calabrese of the American Civil Liberties Union. The authors also thank MPI Director of Communications Michelle Mittelstadt and MPI Intern Nhu-Y Ngo.

We are especially grateful for the support of several funders for the work of MPI's US Immigration Policy Program. In particular we wish to acknowledge the Open Society Institute and the Evelyn and Walter Haas, Jr. Fund. We also thank the Ford Foundation, whose general operating support has been essential to this project and so many others at MPI.

Suggested citation: Meissner, Doris and Marc R. Rosenblum. 2009. *The Next Generation of E-Verify: Getting Employment Verification Right*. Washington, DC: Migration Policy Institute.

Table of Contents

Executive Summary

Effective employer verification must be the linchpin of comprehensive immigration reform legislation if new policies are to succeed in preventing future illegal immigration. The goal of mandatory electronic employment verification is to provide a simple, reliable way for employers to hire only legally authorized workers, as the best way to reduce the jobs magnet that fuels most illegal immigration.

To be effective, an electronic verification system must accomplish two things:

- *Verify authorization to work* by connecting the worker's name and biographical data to a legal status.
- *Authenticate a worker's identity* by connecting the individual to a specific name and identity record, and prevent others from fraudulently claiming that identity.

E-Verify, the government's voluntary electronic verification pilot program, is a great improvement over the 1986 Immigration Reform and Control Act's document-based I-9 system, which is still used by most employers today to assess prospective workers' eligibility to work.

Though deficient in its early performance, E-Verify has been greatly improved and error rates have fallen sharply in recent years. E-Verify has demonstrated that it can reliably meet the first test of effectiveness — verifying authorization to work. But it is not capable of doing the second — authenticating workers' identity — because of the absence of a secure system or systems for identity verification. And thus, E-Verify cannot detect identity fraud. Nonetheless, E-Verify is serving as a valuable laboratory for testing vital immigration policy questions and it is essential that the E-Verify experience inform new legislative measures regarding employer enforcement.

The central recommendations of this report are that in making electronic verification mandatory for all employers as part of comprehensive immigration reform, Congress and the Department of Homeland Security (DHS) should:

- Authorize testing several new voluntary pilots for a next-generation E-Verify system that would reduce employer guesswork and reliably authenticate the identity of newly hired workers; and
- Take immediate steps to strengthen the existing E-Verify system.

New Voluntary Pilots

Immigration reform legislation should provide a statutory framework for mandatory electronic verification that allows E-Verify to become a more employer-neutral system. As with E-Verify, the strengths and weaknesses of new approaches can only be fully assessed by implementing them, so testing through new voluntary pilot projects alongside the existing system should be provided for in reform legislation. We recommend the pilot testing of three concepts: *Secure documents; PIN pre-verification; and biometric scanning.*

Each of these approaches has strong advantages and disadvantages that are outlined in the report. They should be field-tested alongside the current system to determine the best approach for the next generation of E-Verify. DHS and Congress should continue to build, improve, and invest in the existing E-Verify until an alternative proves to be a sufficient improvement to augment or replace it.

Recommendations to Strengthen the Existing E-Verify

The report recommends three sets of reforms that are urgently needed to strengthen the effectiveness, performance, and stakeholder support for the existing E-Verify:

- Strengthen due-process protections and compensate workers when system errors result in the wrongful termination of US citizens and other legal workers — steps that would be particularly important with a mandatory employment verification mandate that would result in the checks of millions of workers, native and foreign born, each year**;**
- Strengthen enforcement of worker protections and employer penalties, training, and oversight; and
- Monitor E-Verify compliance and strengthen auditing to identify patterns of misuse, selective screening, identity fraud, and off-the-books employment. An effective, up-and-running monitoring and compliance unit must be a top DHS priority.

Employers need the best available tools if they are to successfully comply with requirements to hire only legal workers, an essential element in preventing future illegal immigration. Mandatory electronic verification must be part of comprehensive immigration reform legislation if it is to succeed where past policies have failed. Such reforms must also legalize existing unauthorized immigrants, and modernize the employment-based visa system to allow for future immigration flows, so that workers and employers can comply with new laws.

For E-Verify to succeed over time as a mandatory system, Congress should both strengthen the existing system and provide for pilots to test new approaches for a next-generation E-Verify instead of locking in a single approach. Only in this way can E-Verify take advantage of experience and new technologies to best accomplish its vital immigration policy mission.

1. Introduction

Getting it right on employer verification will be the linchpin of an effective, workable immigration reform bill. The goal of electronic verification is to provide a simple, reliable way for good-faith employers to hire legally authorized workers and to deter others from hiring those not eligible to work in the United States. Mandatory verification rests on the proposition that compliance with workplace immigration law by the large majority of the nation's 7.4 million employers is the best way to reduce the jobs magnet that fuels most illegal immigration.[1]

For more than a decade, the United States has tested various systems for electronic verification. The current mostly voluntary system, known as E-Verify, offers important advantages over the document-based I-9 system established by the Immigration Reform and Control Act of 1986 (IRCA). IRCA requires employers to review one or more documents to determine that new employees are eligible to work in the United States and to attest to their identity.

The document-based system has proven highly vulnerable to fraud; E-Verify offers an effective tool to detect the most common types of fake IDs. Yet E-Verify also places a heavy burden on employers to use the system correctly or risk errors. Thus, as lawmakers consider implementing a mandatory electronic verification system, they should enact changes to make E-Verify more robust in reducing errors, monitoring compliance, and providing redress when there is misuse.

At the same time, E-Verify is serving as a valuable laboratory for testing a vital immigration policy question: What kind of electronic verification gives employers a simple, reliable means to ensure they hire only legal workers while also protecting job seekers from employer mistakes, discrimination, and violations of privacy, including identity theft? As Congress returns to issues of immigration reform, it is essential that lawmakers learn from the E-Verify experience in exploring legislative answers to that question rather than locking in a single approach.

To that end, this report:

- Assesses the current strengths and weaknesses of E-Verify and recommends steps to reduce the system's problems and unintended consequences;
- Addresses the need, and proposes options, for better ways to authenticate identity in a verification system if it is to succeed; and
- Proposes next-generation verification pilots that would tap new technologies and practices to overcome the core weaknesses of the current system and strengthen incentives for workers and employers to use the system properly.

The report's analyses and recommendations are rooted in several key principles that have emerged over the course of more than two decades of public policy failures in trying to make verification work.

[1] The US Government Accountability Office estimates that a mandatory verification system would have to accommodate 7.4 million employers; see statement for the record of Richard M. Stana, Director of Homeland Security and Justice Issues, Government Accountability Office, "Employment Verification: Challenges Exist in Implementing a Mandatory Electronic Employment Verification System," GAO-08-895T before the House Judiciary Committee Subcommittee on Immigration, Citizenship, Refugees, Border Security, and International Law, 110th Cong., 2d sess., June 10, 2008, http://www.gao.gov/new.items/d08895t.pdf.

Those principles are:

- Employers should be neutral actors to the greatest extent possible. The verification system should not only be simple and reliable, it should also demand the minimum possible numbers of steps and judgment calls by employers. A red-light/green-light system is the best avenue to unbiased implementation and uniform practices, given the more than 60 million hiring actions employers carry out each year.[2]
- The system must be especially cognizant of privacy and individual rights considerations because new requirements primarily will inconvenience US citizens, who are, by definition, legally eligible to work.[3] At the same time, verification procedures must guard against discriminatory treatment of the foreign born who are eligible to work, whether or not they are citizens.
- Verification pilot programs and testing have been invaluable and should continue as the basis for improvements and changes. Legislation should recognize that a mandatory electronic system would represent a massive new workplace norm to implement and should, therefore, allow for phasing-in, mid-course corrections, and future innovations based on experience and likely new technologies.

This report's central recommendation is that Congress and the Department of Homeland Security (DHS) should take immediate steps to strengthen the existing E-Verify system and Congress should authorize testing several new *voluntary pilots* of a next-generation system: secure, biometric work authorization cards; a PIN pre-verification system triggered by workers; and a biometric scanning system permitting employers to capture biometric data from workers at the point of hire. While E-Verify is a great improvement over the purely document-based IRCA system and E-Verify error rates have fallen sharply in recent years, the system's heavy demands on employers and continuing limitations with respect to authenticating identity raise questions about its suitability as a mandatory system — questions which can best be answered by observing its effects in the real world and comparing its performance to alternative systems.

Regardless of their format, new electronic verification mandates are only likely to succeed in the context of broader immigration reforms to legalize existing unauthorized immigrants and to modernize the employment-based visa system so that workers and employers have greater incentives to comply. Each of the proposed pilots offers unique costs and benefits, and each is likely to produce unintended consequences for all workers, whether native or foreign born; it is therefore essential that in mandating electronic verification, Congress allow E-Verify to evolve and take advantage of experience and the newest technologies by not locking in a single approach at this stage.

---

[2] GAO estimates that verification of all new hires would require E-Verify to process 63 million queries per year; see Stana, *Employment Verification: Challenges Exist in Implementing a Mandatory Electronic Employment Verification System*, p. 10.

[3] Universal verification would primarily affect US citizens because they represent 85 percent of the workforce. Any new mandates would likely affect citizens and noncitizens alike (or be vulnerable to fraudulent claims of citizenship). And even if errors disproportionately affect noncitizens, as has been the case under E-Verify, most error victims will likely be US citizens as a function of their greater share of the overall workforce.

II. Background

Most illegal immigration is a response to economic factors. Policy efforts to eliminate the jobs magnet have been a mainstay in immigration policy debates going back to at least the early 1970s. In 1981, the Select Commission on Immigration and Refugee Policy recommended sanctions against employers who knowingly hire workers illegally in the country, leading Congress to enact IRCA in 1986, establishing employer sanctions in the realm of immigration for the first time in US history.

However, IRCA failed to reduce unauthorized employment because — against the Select Commission's advice — the legislation failed to create a reliable system for determining whether job seekers were authorized to work in the United States.[4] Instead, the law allowed employers to establish a prospective worker's identity and work eligibility by checking one or two documents from a list of 29 (since reduced to 26) existing documents routinely used for identification, employment, and other purposes. Employers are required to attest on the I-9 form that the documents appear genuine and belong to the new worker.

IRCA's requirements spawned a flourishing market of fraudulent documents that "prove" identity and work eligibility.[5] The vulnerability to document fraud means that many good-faith employers check documents, but still hire unauthorized workers inadvertently. At the same time, bad-faith employers are able to shield themselves from sanctions by going through the motions of compliance (i.e., checking documents) without intending to screen out unauthorized workers; prosecutors typically have a difficult time proving *knowing* employment of unauthorized workers, which was the standard set in IRCA.

Ineffective document provisions also created uncertainty in the verification process, and some employers responded by lowering the wages of unauthorized workers, rather than discontinuing their employment.[6] Some employers also reacted by discriminating against workers who seemed like they might be illegal, especially Hispanics and other ethnic minorities.[7]

---

[4] The Select Commission called for a "system of more secure identification" in support of employer sanctions, and the Senate passed employer sanctions bills in 1982 and 1983 which would have established a national ID card (in 1982) and a national phone-in system (in 1983) to provide employers with new tools for eligibility verification.

[5] See GAO, *Illegal Aliens: Fraudulent Documents Undermining the Effectiveness of the Employment Verification System* GAOT-GGD/HEHS-99-1 75 (Washington, DC: Government Accountability Office, 1999), http://archive.gao.gov/f0902b/162489.pdf; and GAO, *Weaknesses Hinder Employment Verification and Worksite Enforcement Efforts* GAO-05-813 (Washington, DC: Government Accountability Office, 2005), http://www.gao.gov/new.items/d05813.pdf.

[6] Jorge Durand, Douglas S. Massey, and Emilio A. Parrado, "The New Era of Mexican Migration to the United States," *Journal of American History* 86, 2 (1999); Sherrie A. Kossoudji and Deborah A. Cobb-Clark, "Coming out of the Shadows: Learning about Legal Status and Wages from the Legalized Population," *Journal of Labor Economics* 20, 3 (July 2002): 598-628; Julie A. Phillips and Douglas S. Massey, "The New Labor Market: Immigrants and Wages after IRCA," *Demography* 36, 2 (1999): 233-246; and Francisco L. Rivera-Batiz, "Undocumented Workers in the Labor Market: An Analysis of the Earnings of Legal and Illegal Mexican Immigrants in the United States," *Journal of Population Economics* 12, 1 Special Issue on Illegal Migration (1999): 91-116.

[7] Five percent of employers "began a practice, as a result of IRCA, not to hire job applicants whose appearance or accent led them to suspect that they might be unauthorized aliens;" 9 percent of employers said that because of IRCA they "began hiring only persons born in the United States or not hiring persons with temporary work eligibility documents;" and a matched pair survey of job applicants found that Anglo job applicants received 52 percent more job offers than Hispanic job applicants with identical records, see GAO, *Immigration Reform:*

In 1994, the US Commission on Immigration Reform identified ineffective document provisions as a fundamental barrier to effective employer enforcement and a cause of discrimination.[8] The Commission recommended that Congress create an electronic eligibility verification system (EEVS) to curb document fraud. Congress responded in 1996 by calling for three electronic verification pilot programs as part of the Illegal Immigration Reform and Immigrant Responsibility Act (IIRIRA).[9] One of the pilots, termed the Basic Pilot, became a national voluntary program in 2003, and operates today as E-Verify.[10]

To be effective, verification must be a routine part of the hiring process — akin to paying taxes — and noncompliant employers must be targeted for enforcement.

III. E-Verify: How Does it Work? What Are its Limitations?

How it Works

The E-Verify system uses the same biographical information that workers provide when filling out the I-9 form, including name, date of birth, Social Security number (SSN), and for noncitizens the Alien Identification (or I-94) number. E-Verify employers agree to submit this information through a secure website within three days after a worker is hired.[11] These data are checked against the Social Security Administration (SSA) main database, known as Numident, and, in the case of noncitizens, against the Department of Homeland Security (DHS) composite database known as the Verification Information System (VIS).

If the worker's identity data match these records and show either US citizenship or employment authorization for noncitizens, E-Verify returns an immediate confirmation to the employer through the website, stating that the person is authorized to work. When the data cannot be verified through a secondary manual database search by DHS status verifiers — about 3.1 percent of the time during the first quarter of Fiscal Year 2009[12] — E-Verify responds with a tentative nonconfirmation (TNC). A TNC does not prove that a worker is unauthorized, because a nonmatch may be the result

---

Employer Sanctions and the Question of Discrimination GGD-90-62, (Washington, DC: Government Accountability Office, 1990), http://archive.gao.gov/d24t8/140974.pdf. Also see Cynthia Bansak and Steven Raphael, "Immigration Reform and the Earnings of Latino Workers: Do Employer Sanctions Cause Discrimination?" *Industrial and Labor Relations Review*, Vol. 54, No. 2 (2001): 275-295.

[8] US Commission on Immigration Reform, *US Immigration Policy: Restoring Credibility* (Washington, DC: Government Printing Office, 1994), http://www.utexas.edu/lbj/uscir/reports.html.

[9] In addition to Basic Pilot, IIRIRA authorized the Citizenship Attestation Verification Pilot and the Machine-Readable Document Pilot. Both were dropped in favor of the more universal and more effective Basic Pilot.

[10] As of May 2009, US Citizenship and Immigration Services (USCIS) reported that about 2 percent of the country's business establishments (125,000 businesses) are registered to use E-Verify, and about 14 percent of nonfarm hires are screened by the program (6 million queries per year). GAO has previously reported that only half of all registered E-Verify users regularly screen workers through the system; see Stana, *Employment Verification: Challenges Exist in Implementing a Mandatory Electronic Employment Verification System*, p. 10.

[11] USCIS defines "hire" as offer and acceptance of a job, while the I-9 defines it as the first day of paid work.

[12] Westat data published on the USCIS website, http://www.uscis.gov/portal/site/uscis/menuitem.5af9bb95919f35e66f614176543f6d1a/?vgnextoid=f82d8557a487a110VgnVCM1000004718190aRCRD&vgnextchannel=a16988e60a405110VgnVCM1000004718190aRCRD.

of a database or user error. Thus, employers are required to notify workers of the TNC and provide them with instructions to correct the record in case of error.

Workers have eight business days to contact the appropriate federal agency and initiate a challenge to the TNC, which generally requires calling US Citizenship and Immigration Services (USCIS) or visiting an SSA field office. Absent cause, employers are prohibited from taking adverse action against a worker (e.g., to terminate employment, withhold wages, or delay training) while a TNC is pending. USCIS and SSA may take an additional two days (ten days total) to resolve a TNC or will issue a "case in continuance" notice if the TNC cannot be resolved on this timeline.

If a worker fails to act on a TNC within the eight days — as is the case in about 85 percent of TNC cases[13] — or if SSA and USCIS are unable to confirm work authorization after further review, the employer receives a final nonconfirmation notice. That notice indicates the worker is not work authorized, and the employer is encouraged to terminate the worker or risk being penalized for knowing employment of an unauthorized worker.[14]

Limitations of the Current E-Verify

To be effective, electronic verification must accomplish two things:

- The system must *verify authorization to work* by connecting the worker's name and biographical data to a legal status.
- The system must *authenticate a worker's identity* by connecting the individual to a specific name and identity record, and must prevent others from fraudulently claiming that identity.

There is uncertainty and potential for errors attendant to both of these functions, as is the case for all automated information systems. E-Verify has demonstrated that it can reliably meet the first test of effectiveness — verifying authorization to work — but it is not able to do the second — authenticate workers' identity — because of the absence of a sufficiently universal and secure system or systems of identity verification to incorporate into the E-Verify design and procedures. Further discussion of these issues follows.

A. Verification of Eligibility to Work

Much has been written and debated about error rates in E-Verify. Database errors may prevent US citizens and other legal workers from initially — or occasionally ever — being confirmed by the

[13] See Westat, *Findings of the Web-Based Basic Pilot Evaluation*¸ (Rockville, MD: Westat, 2007), pp. 44-49, http://www.uscis.gov/files/article/WebBasicPilotRprtSept2007.pdf.

[14] Civil penalties for knowing employment of unauthorized workers range from $250 to $10,000 per violation, and employers may face criminal penalties for engaging in a pattern or practice of repeated violations; see INA §§274A(e)-(f). According to the E-Verify Memorandum of Understanding signed by each employer (p. 5), "If the employee does not choose to contest a tentative nonconfirmation or a photo nonmatch or if a secondary verification is completed and a final nonconfirmation is issued, then the employer can find the employee is not work authorized and terminate the employee's employment," http://www.uscis.gov/files/nativedocuments/MOU.pdf. Also see USCIS, E-Verify User Manual, p. 34-35, http://www.uscis.gov/files/nativedocuments/E-Verify_Manual.pdf.

system, thus creating problems for a legal worker who is either not notified of the TNC by the employer or who fails to resolve it. False nonconfirmations result from the following types of errors:

- *Basic database errors.* All large databases — Numident, for example, contains 449 million records and the Verification Information System (VIS), the operating system for E-Verify, checks against 80 million records — are subject to human error.[15] Some records accessed by E-Verify consist of paper files, and are still being converted to electronic formats, resulting in potential errors.
- *Database maintenance and aggregation*. Databases accessed by E-Verify are constantly evolving as citizens, legal residents, and work-authorized nonimmigrants change their names (including through marriage) and immigration status. To keep pace with these changes, which may occur at many different points in the system, the VIS database aggregates eight different DHS and legacy Immigration and Naturalization Service (INS) databases.[16]
- *Misspellings and incorrect name order*. Many names have multiple possible spellings, especially in the case of transliterations from non-Latin alphabets. Some immigrants come from cultures in which naming and name-order conventions differ from those in the United States, making them more prone to such errors.[17]
- *User error*. E-Verify relies on employers to input workers' I-9 data. Employers make mistakes with complex names, through carelessness, or in reading handwriting and documents.

When such errors lead to a TNC, correcting records may be a burden. Although individuals have a strong self-interest in ensuring the accuracy of their government records, workers may also unexpectedly have to take time from work — typically unpaid — to contact USCIS (usually by phone) or SSA (usually in person) to correct errors that are often no fault of their own.[18] Such problems disproportionately affect legal immigrants, foreign-born citizens, and other minority groups, who are all more likely than other workers to be affected by each of the above errors.[19]

---

[15] See Elizabeth Pierce, "Modeling Database Error Rates," *Data Quality* 3, 1 (1997).

[16] USCIS reports it uses the following databases to confirm employee work authorization: DHS Central Index System, Computer Linked Automated Information Management System 3, Interagency Border Inspection System I-94 data, Image Storage and Retrieval System, SSA Numerical Identification File, Interagency Border Inspection System Real Time Arrival, Computer Linked Automated Information Management System 4, and the Reengineered Naturalization Automated Casework System.

[17] This problem is mitigated by SSA algorithms which allow for some variation in name order, and by manual checks by USCIS status verifiers. Nonetheless, name-order errors remain problematic, a problem also observed during the 2004 and 2008 elections when many Asian Americans were denied voting rights due to name-order errors on voter roles. See Asian American Legal Defense and Education Fund, "Asian American Access to Democracy in the 2008 Elections," http://aaldef.org/docs/AALDEF_Election_2008_Report.pdf.

[18] See Westat, *Findings of the Web-Based Basic Pilot Evaluation*¸ Appendix E, http://www.uscis.gov/files/article/WebBasicPilotRprtSept2007.pdf. According to SSA, most US citizens correct TNCs by visiting SSA field offices, and the average correction requires 1.5 visits. Here and throughout, our statistics on E-Verify's performance are mainly derived from Westat's published data. These data were commissioned by DHS in response to a congressional mandate for assessments of the program.

[19] The known error rate (i.e., corrected TNCs) in 2006-2007 was *30 times* higher for foreign-born than native-born workers, and *98 times* higher for naturalized US citizens than for native-born citizens. See Westat, *Findings of the Web-Based Basic Pilot Evaluation*, pp. xxv-xxvi. Reforms enacted in 2007 reduced these disparities, and DHS reported that the error rate for naturalized citizens had fallen 39 percent as of May 2008, though new comparative data are unavailable; see statement for the record of Michael Aytes, Acting Deputy Director, US Citizenship and Immigration Services, "Priorities Enforcing Immigration Law" before the House Committee on Appropriations, Subcommittee on Homeland Security, 111th Cong., 1st sess., April 2, 2009,

False nonconfirmations are also costly to employers because they create inefficiencies in the employment process. Despite the ten-day timeline for resolving TNCs, the average time from date of hire to closing a TNC in 2006-2007 was 39.7 days.[20] Erroneous TNCs and delayed resolution of TNCs have been employers' most frequent complaints following the implementation of mandatory E-Verify in Arizona.[21]

Erroneous Nonconfirmations: Scope of the Problem

Recognizing that no automated information system will ever be error-free, how serious is the false nonconfirmation problem?

The precise scope of the problem is not known, because some legal workers fail to correct erroneous nonconfirmations. Legal workers may fail to correct TNCs because their employers do not provide needed information or actively discourage them from doing so. When workers are informed about a TNC, they may find it too costly or inconvenient to correct the record, or they may lack the documents needed to do so.[22] Workers often may continue working without correcting a TNC, either at the same employer or a different job. Statistical models also underestimate nonconfirmation error rates because they cannot account for identity fraud.[23]

Still, the available evidence is that about 1 percent of all E-Verify queries result in false nonconfirmations for legal workers, out of a total nonconfirmation rate of 3.1 percent during the first quarter of 2009. This figure includes about 0.3 percent of workers who successfully corrected

---

http://www.uscis.gov/portal/site/uscis/menuitem.5af9bb95919f35e66f614176543f6d1a/?vgnextoid=d3ace7c336c60210VgnVCM1000004718190aRCRD&vgnextchannel=75bce2e261405110VgnVCM1000004718190aRCRD.

[20] Westat, *Findings of the Web-Based Basic Pilot Evaluation*, p. E-4. The actual time to resolve TNCs may have been even longer, as two employers in the sample did not comply with proper reporting requirements.

[21] Arizona was the first of three states (followed by South Carolina and Mississippi) to require employers to use E-Verify, and eight additional states require certain employers to use the system; see Marc Rosenblum, *The Basics of E-Verify, the US Employer Verification System, Migration Information Source*, (Washington, DC: Migration Policy Institute, 2009). Employer complaints about delayed verification primarily concern the requirement that workers not be placed in probationary status (e.g., suspending wages and training expenses) pending resolution of a TNC; see USCIS Ombudsman, *Observations on the E-Verify Experience in Arizona & Recommended Customer Service Enhancements* (Washington, DC: US Department of Homeland Security Office of the Citizenship and Immigration Services Ombudsman, 2008), http://www.dhs.gov/xlibrary/assets/cisomb_everify_recommendation_2008-12-22.pdf. Also see Christina Boomer, "Some Valley workers having trouble with E-Verify," ABC 15 TV, March 24, 2008, http://www.abc15.com/news/local/story/Some-Valley-workers-having-trouble-with-E-Verify/VdTlB1vZu0--Qy0e5zGJcg.cspx; Ronald Hansen, "Economy Serves Up Unhappy Meal: Worst Lull in 2 Decades is Hurting Valley Restaurateurs," *Arizona Republic*, March 3, 2008; and Becky Pallack, "Small Businesses Bump into E-Verify Obstacles," *Arizona Daily Star*, April 8, 2008.

[22] The Brennan Center for Justice estimated that 21million US citizens lacked valid identity documents in 2006, and 13 million do not have access to passports, birth certificates, or naturalization papers needed to prove their citizenship. See Brennan Center for Justice, *Citizens without Proof: A Survey of Americans' Possession of Documentary Proof of Citizenship and Photo Identification* (New York: New York University, November 2006), http://www.brennancenter.org/page/-/d/download_file_39242.pdf. At least four out of 326 workers (1.2 percent) who received TNCs in 2006-2007 Westat case studies were legal workers who were unable to contest the findings because they did not understand how to do so or who tried to do so but were unsuccessful (see Westat, *Findings of the Web-Based Basic Pilot Evaluation*, p. E-3, E-13).

[23] The erroneous nonconfirmation rate is equal to the number of false nonconfirmations divided by the number of accurate confirmations. As we have seen, the denominator in this calculation (the number of confirmations) includes an unknown number of unauthorized workers, making the observed error rate appear smaller than the actual rate.

TNCs — the minimum observed error rate — and our estimate that about 0.6 percent of workers likely failed to correct erroneous nonconfirmations.[24]

This error rate represents a 90 percent improvement since 1998 as a result of enhancements USCIS has made to the system. Advances include new filtering software that alerts employers to data-entry errors, and fuller integration of DHS and State Department databases that ensures that recent immigrants and citizens are more likely to be confirmed. USCIS deserves considerable credit for these important and successful reforms.

Through such reforms, USCIS has successfully addressed most of the readily correctable sources of error in the system,[25] and has a plan for further reductions. Most remaining false nonconfirmations are likely a result of employer mistakes and "root errors" in the actual databases, rather than miscommunication among the databases or other problems which can be addressed by USCIS.[26] Thus, substantial further reductions in the rate of false nonconfirmations seem unlikely.

Error Rates in a Mandatory System

In a mandatory electronic system, a 1 percent error rate would affect about 600,000 workers per year. The rate could increase with new E-Verify mandates because growing the system would place added strain on the system's infrastructure and staffing, and could lead to new types of errors.[27]

---

[24] The 1 percent error rate is a "best guess" estimate; the exact error rate cannot be measured with available data, and some sources suggest it is a good deal higher. Westat, *Findings of the Web-Based Basic Pilot Evaluation,* Appendix C, p. C-1 – C-5, estimates a total erroneous nonconfirmation rate of 0.81 percent. This estimate assumes that 61 percent of US citizens and 85 percent of work-authorized noncitizens who receive erroneous TNCs choose to appeal; and it does not control for the problem of false confirmations in the denominator. Using Westat's 2006-2007 data and assuming that 20 percent of workers lack the information to appeal — as employer surveys suggest — yields a total estimated erroneous nonconfirmation rate of 1.65 percent. Westat's detailed case studies of five employers identified at least six workers out of 326 TNCs (1.8 percent) who were erroneously nonconfirmed, and 31 out of 364 (8.5 percent) who were able to correct an erroneous TNC (total erroneous nonconfirmation rate of 10.3 percent; see Appendix E). Other employers have reported error rates similar to those observed in the Westat case studies: Intel Corporation reported that slightly over 12 percent of its workers received TNCs in 2008 even though *all* of them were ultimately found to be work authorized; see Intel Corporation, "Comments on Proposed Employment Eligibility Regulations Implementing Executive Order 12989 (as amended)," August 8, 2008. And the American Council on International Personnel describes a large firm with a TNC rate of 15 percent; see American Council on International Personnel, "Comments on Proposed Rule Published at 73 Fed. Reg. 33374 (June 12, 2008)," August 11, 2008. All of these studies predate reforms implemented by USCIS in 2007-2008 which have likely reduced false nonconfirmations. Also see footnote 22.

[25] The main exception is data on derived US citizens (such as children born abroad who are eligible for US citizenship through their parents), for whom USCIS still only has paper files. Derived citizens who do not get certificates of citizenship do not appear as citizens in their paper A file. While they are work authorized, as any other citizen would be, there is a mismatch on citizenship which causes TNCs and potentially problems at SSA.

[26] "Root errors" are mistakes in the underlying SSA and DHS databases which can only be detected during the verification process. A 2006 SSA study found that *4.1 percent* of SSA records contained data mismatches that could result in E-Verify nonconfirmations: *Accuracy of the Social Security Administration's Numident File,* A-08-06-26100 (Washington, DC: Social Security Administration, 2006), http://www.ssa.gov/oig/ADOBEPDF/A-08-06-26100.pdf. In the case of DHS, GAO found that between 1 and 4 percent of migrants' A files, the primary record for all immigrants in the United States, could not be located; and error rates were much higher in busier regions, including a 20 percent missing-record rate in the San Diego field office. See GAO, *Immigration Benefits: Additional Efforts Needed to Help Ensure Alien Files Are Located When Needed* GAO 07-85 (Washington, DC: Government Accountability Office, 2006), http://www.gao.gov/new.items/d0785.pdf.

[27] GAO estimates that verification of all new hires would require E-Verify to process 63 million queries per year; see Stana, *Employment Verification: Challenges Exist in Implementing a Mandatory Electronic Employment*

Resource strains may be especially severe where US citizens are required to contact SSA, which is at its lowest staffing level since the early 1970s and facing a looming baby boom retirement workload bubble.[28]

Erroneous nonconfirmations would also likely increase as a function of the changing makeup of E-Verify employers. As a mostly voluntary program, E-Verify attracts mainly good-faith employers who want to comply with immigration law. A mandatory program would include a higher proportion of employers who might inadvertently or intentionally misuse the system.

At the same time, as a mandatory system is phased in and experiences greater and greater use, TNCs should lead to corrections in the records of substantial numbers of workers who do not now know that errors exist in their government database records. Similarly, the government agencies that administer such records have important interests in improving the accuracy of their information systems. Over time, therefore, error rates should be expected to diminish and become a manageable element of the system, as with analogous large-scale electronic information systems.

B. Authenticating a Worker's Identity

E-Verify lacks a reliable mechanism for authenticating an individual's identity because the system continues to rely on the I-9 process where employers review existing identity documents, such as driver's licenses, to match individuals to their identities. E-Verify can tell if a particular name, date of birth, SSN, or alien registration number match its databases. But it is not able to confirm that the name, date of birth, or number on a proscribed identification document belong to the individual presenting them. The employer is unlikely to catch anything but possibly a mismatch where there is

---

Verification System. Although USCIS reports that E-Verify can already handle 65 million queries a year and that stress tests indicate that the system can handle up to 240 million queries a year, data security experts warn that even a tenfold increase in the scale of a program like E-Verify may produce "serious new technical issues…that were not previously significant." See Stana, *Employment Verification: Challenges Exist in Implementing a Mandatory Electronic Employment Verification System*; and testimony of Peter Neumann, Principal Scientist, Computer Science Lab SRI International, before the House Committee on Ways and Means, Subcommittee on Social Security, June 7, 2007, http://usacm.acm.org/usacm/PDF/EEVS_Testimony_Peter_Neumann_USACM.pdf. USCIS estimated in 2008 that the 2009-2012 cost of running all new hires through E-Verify would be $765 million, increasing to $838 million to also cover re-verification of existing employees. These estimates do not include USCIS staffing costs, and the agency would be required to scale up its status verifiers, compliance oversight, and related services. SSA estimated its costs in a mandatory E-Verify program at $281million for 2009-2013, and that the program would require SSA to hire 700 additional personnel. See Stana, *Employment Verification: Challenges Exist in Implementing a Mandatory Electronic Employment Verification System*, p. 10-11.

[28] The retirement bubble will add 1 million new cases a year to SSA's workload for the next decade. SSA estimates that requiring all employers to screen new hires through E-Verify would result in between 1.3 million and 3.6 million US citizens being required to visit SSA field offices per year to resolve TNCs. The larger number is based on an estimate which precedes the 2008 procedural changes that allow naturalized citizens to resolve TNCs through their passport records; see "The Facts on Employment Verification: Current Proposals are Unworkable for SSA, Threaten Progress in Reducing Disability Claims Backlog." Letter from Rep. Michael McNulty (D-NY) and Rep. Charles Rangel (D-NY) to Democratic colleagues, March 27, 2008, http://www.nationalwatermelonassociation.com/docs/Electronic%20Employment%20Verification%20is%20Unworkable%20for%20SSA%20and%20threatens%20progress.pdf. The smaller estimate reflects the projected reductions in TNCs from this procedural change; see Stana, "Employment Verification: Challenges Exist in Implementing a Mandatory Electronic Employment Verification System," p. 12, http://www.gao.gov/new.items/d08895t.pdf. USCIS reimburses SSA for each TNC handled by SSA.

no resemblance of the presenter to the photograph or there is a significant age discrepancy, such as a child presenting a parent's document.

As a result, the system is vulnerable to identity fraud: unauthorized workers may be confirmed by the system by using borrowed or stolen identity data that belong to someone else. Such identity fraud may be initiated by employers, workers, or middlemen, and may occur with or without the knowledge of the worker, and with or without the knowledge of the legal worker whose identity data are being misused.

The vulnerability of the system to identity fraud undermines its ability to accomplish either of its core immigration enforcement goals.

- If good-faith employers cannot get reliable confirmation of *whom* they are hiring, verification of eligibility to work is inaccurate.
- Inaccurate verification allows bad-faith employers and unauthorized workers to go through the motions of compliance (by submitting data to E-Verify) while still violating the law (by hiring workers whose data belong to someone else).

Identity Fraud: Scope of the Problem

How serious are false confirmation and identity fraud problems? About 9.9 million Americans were victims of identity theft in 2008. Most involved credit and financial fraud.[29] There is anecdotal evidence that unauthorized workers and some employers have relied on identity fraud to obtain employment through E-Verify.[30] There is no precise estimate of such false confirmations because measuring the phenomenon would require follow-up (an additional round of identity authentication) on workers after they have been confirmed by the system. Such workers have been work authorized, and follow-up inquiries are rarely conducted.[31]

Identity fraud is a growth industry, and false confirmations as a result of identity fraud are likely to persist, and probably increase, as E-Verify expands. "Full identities," including name, date of birth, and SSN, may be purchased online for as little as 70 cents (if purchased in bulk) to as much as $60, and the 1.6 million malicious code threats detected in 2008 were more than double the total detected

---

[29] Javelin Strategy and Research, *2009 Identity Fraud Survey Report* (Pleasanton, CA: Javelin Strategy and Research, 2009). Javelin estimates that costs of identity fraud to US victims were $48 billion in 2008. http://www.javelinstrategy.com/products/A87547/127/delivery.pdf.

[30] In one high-profile case in 2006, 1,282 employees at six Swift & Co. meat processing plants were detained despite the company's use of the Basic Pilot/E-Verify program to screen its workers; many had relied on identity fraud to obtain employment. See US Immigration and Customs Enforcement, "53 former employees at Swift & Company meat processing plant in Cactus, Texas, charged in federal indictments," (Washington, DC: US Immigration and Customs Enforcement 2007), http://www.ice.gov/pi/news/newsreleases/articles/070110amarillo.htm; and media accounts from Arizona report that some workers there have used borrowed identity data to obtain employment in the wake of that state's E-Verify mandate, often with the assistance, or at the direction of employers. See Daniel González, "Illegal workers manage to skirt Arizona employer-sanctions law. Borrowed identities, cash pay fuel an underground economy," *Arizona Republic*, November 30, 2008, http://www.azcentral.com/news/articles/2008/11/30/20081130underground1127.html.

[31] On the technical challenges of measuring false confirmations see Westat, *Findings of the Web-Based Basic Pilot Evaluation*, p. 39. Westat's forthcoming (2009) analysis of E-Verify will include a model-based estimate of the system's vulnerability to identity fraud.

during the previous six years.[32] Even the US passport, traditionally seen as the gold standard for identity security, has been shown to be vulnerable to identity fraud by criminals or terrorists with basic counterfeiting skills.[33]

While most identity theft is now related to credit card and financial fraud, growth in E-Verify is likely to expand the market for employment-based identity fraud. Expanded markets for stolen data would be especially likely if new E-Verify mandates are not accompanied by broader immigration reforms to legalize existing unauthorized workers and to provide more legal opportunities for future employment-based migration. That is because most unauthorized workers create fictitious SSNs. Mandatory electronic verification would create incentives and new markets for real but stolen numbers.

In addition to creating new markets, an electronic eligibility verification system (EEVS) also makes stolen identity data more accessible by providing employers and system administrators with reliable information about workers' status and making the data available in electronic format, substantially lowering the costs for E-Verify employers — or identity thieves posing as employers — to participate in identity theft schemes.

Combating Identity Fraud

Two new programs seek to combat the problem, but neither is expected to be fully operational in the near term.

a) In September 2007, USCIS added a photo screening tool to E-Verify to provide employers an electronic copy of many DHS-issued identification document photos along with a worker's authorization confirmation. By comparing the photo provided by the system to that on the document presented by the worker, employers can confirm that the document belongs to the new hire. But photo screening is limited to images from recently issued Employment Authorization Documents (EADs) and legal permanent residents' green cards, which number about 15 million, or about 5 to 7 percent of job applicants.[34]

USCIS has raised the possibility of using state department of motor vehicle (DMV) data for E-Verify. Such data would cover far more workers. However, the addition of 50 or more state and county-level databases would make the system far more vulnerable to database errors, false nonconfirmations, and identity theft and raises significant problems with state laws that may prohibit data sharing and related issues.[35] And no states have agreed to provide photos at this time.

---

[32] Symantec, *Symantec Internet Global Security Threat Report – Trends for 2008*, (Cupertino, CA: Symantec, 2009) p. 10, http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xiv_04-2009.en-us.pdf.

[33] GAO, *Department of State: Undercover Tests Reveal Significant Vulnerabilities in State's Passport Issuance Process* GAO-09-447 (Washington, DC: Government Accountability Office, 2009), http://www.gao.gov/new.items/d09447.pdf.

[34] See Stana, "Employment Verification: Challenges Exist in Implementing a Mandatory Electronic Employment Verification System." Stana reported that the photo screening tool covers 5 percent of workers queried by the system. See also *Regulatory Impact Analysis, Employment Eligibility Verification* (Federal Acquisition Regulation Case 2007-013), October 2008, p. 49.

[35] About 205 million Americans have driver's licenses; see US Department of Transportation Federal Highway Administration, *Licensed Drivers by Sex and Ratio to Population – 2007*" (Washington, DC: Department of Transportation Federal Highway Administration, 2008), http://www.fhwa.dot.gov/policyinformation/statistics/2007/dl1c.cfm. Hawaii and Kentucky delegate license-

To be effective, photo screening would likely require implementation of a common national identification system, possibly through the proposed PASS ID Act[36] or an enhanced eligibility verification database (see below). While expanded photo screening would reduce identity theft, it also would result in more false nonconfirmations (including of US citizens) as a result of data errors and possible misuse of the photo screening tool.

b) A second initiative, still in the planning stage, would allow USCIS to "block" an individual worker's identity data to prevent its fraudulent use. A worker whose data is blocked would receive a TNC, requiring contact with DHS to authenticate his or her identity in order to be confirmed by the system. Data blocking would limit identity theft because unauthorized workers would be unable to successfully contest a TNC.

To succeed on a large scale, data blocking would have to cover most legal workers, all of whom would be required to contact USCIS or SSA to unblock the data following an initial TNC as a result of the blocked data. E-Verify is not designed to accommodate such a large number of TNCs. Thus, in the near term, data blocking will likely be limited to individuals who request it to protect their records, and possibly to suspected cases of identity theft identified by USCIS.

Overall, then, E-Verify lacks effective tools to combat identity fraud and is not designed for, or capable of, authenticating identity in a manner that would prevent false confirmations based on stolen identities. Because identity verification is one of the two key attributes of an effective electronic verification system, E-Verify as currently designed can only be partially effective in achieving reliable employer verification. In addition, absent strengthened identity authentication measures and broader immigration reforms, new E-Verify mandates are likely to contribute to increased levels of identity fraud.

IV. The E-Verify Model: Is it Right for Mandatory Electronic Verification?

Any EEVS will produce false nonconfirmations and confirmations. The challenge is to minimize them and develop effective methods for managing how and why they occur. Measures to address the verification program's inability to authenticate identity are certain to spark hot debate when immigration reform legislation is again in consideration. Nonetheless, these problems can ultimately be resolved by lawmakers if Congress can find consensus on issues of identity verification.

The deeper question that emerges from the considerable E-Verify experience to date is whether the E-Verify model is the right model for a mandatory electronic system. Given the history of E-Verify, it has never been possible to examine that question with a clean slate.

When INS developed Basic Pilot (since renamed E-Verify) under the mandates of IIRIRA, it and its two companion pilots (since terminated) were given modest short-term funding for testing. At the

---

issuance to county DMVs, so a system to screen license photos would have to aggregate 48 state and 124 county databases.

[36] The Providing for Additional Security in States' Identification (PASS ID) Act of 2009 (S.1261) would establish a common machine-readable format for DMV data.

time, INS was one of the least automated, least technology-savvy agencies in government. In designing Basic Pilot, the agency looked to the 1980s Systematic Alien Verification for Entitlements (SAVE) system. SAVE enables federal, state, and local benefit and licensing agencies to query INS/USCIS about the immigration status of applicants so only ineligible noncitizens are denied. SAVE remains in use today. Although E-Verify accesses largely the same databases as government agencies under SAVE, the mode of access and processes are different.

Nevertheless, in E-Verify, the employer occupies much the same place that government agencies play with SAVE. As a result, the design looks to employers to exercise key judgments and to potentially be responsible for multiple steps in the verification process. As such, E-Verify is an employer-centric model, not an employer-neutral model. The evolution of E-Verify is antithetical to what should be seen as a core principle of employer verification, which is to eliminate guesswork by establishing an employer-neutral, red-light/green-light system for determining work authorization.

The E-Verify experience with an employer-centric model has important implications for the future, which are outlined below.

A. The Employer Role in Verification of Authorization to Work

E-Verify makes employers the unique point of contact when new hires receive a TNC, the means by which the system is designed to prevent erroneous nonconfirmations. TNC requirements are counterintuitive, and many employers mistakenly believe they are required to terminate or suspend a worker until a TNC has been resolved. In addition, employers generally would rather invest training and other resources in a worker who has already been work authorized, and avoid continuing to employ a worker facing a TNC, whom they fear ultimately may prove to be not authorized to work.

Despite E-Verify rules, the TNC process creates perverse incentives that often lead to adverse employment actions against a worker while a TNC is pending. For example, although the E-Verify memorandum of understanding (MOU) signed by participating employers requires them to verify workers within three days *after* an employee has been hired, between a quarter and one half of employers enrolled in E-Verify sometimes prescreen job applicants so that workers are less likely to learn of a TNC, fail to notify workers of a TNC, or actively discourage workers from contesting a TNC.[37] One quarter of employers admit to violating program rules following a TNC by suspending training or employment, cutting wages, mistreating workers, or terminating employment.[38] In these

[37] In its 2006-2007 survey of employers enrolled in E-Verify, Westat found that 47 percent of employers put workers through E-Verify before the employees' first day at work (16 percent used it for job applicants and 31 percent after a job offer but before the employee's first day of paid work); 9.4 percent of employers did not notify workers of a tentative nonconfirmation notice, 7 percent who gave workers the notice did not encourage them to contest it because the process of contesting the notice was seen as too time-consuming (Westat, *Findings of the Web-Based Basic Pilot Evaluation*, p. 71-77).
These violations were not mutually exclusive. These numbers likely underestimate employer noncompliance since they are based on voluntary self reporting, and likely exclude cases of intentional noncompliance. A 2008 survey of 376 immigrant workers (including an unknown number of unauthorized workers) in Arizona found that 126 had been fired, apparently after receiving an E-Verify TNC, but that *none* had been notified by employers that they had received a TNC and been given information to appeal the finding; see Caroline Isaacs, *Sanctioning Arizona: The Hidden Impacts of Arizona's Employer Sanctions Law* (Washington, DC: American Friends Service Committee, 2009), http://www.afsc.org/tucson/ht/a/GetDocumentAction/i/74700.

[38] According to the 2006-2007 Westat survey, 22 percent of employers admitted to restricting work assignments while TNCs were pending, 16 percent delayed job training, and 2 percent reduced pay based on tentative

ways, the employer's role as the central actor in managing a TNC increases the frequency of erroneous nonconfirmations and the cost to workers of employer errors. Federal law protecting workers has not kept pace with employers' verification responsibilities, and offers workers no recourse if employers violate hiring and employment rules during the verification process.

The cost to workers falls heavier on Hispanics, other minority groups, and foreign-appearing and -sounding persons, as they are the most frequent targets of prescreening and other violations of E-Verify rules.[39] Employer responsibility for managing TNCs also creates conditions for employer abuse based on increased knowledge of information about workers' employment authorization status. Such information opens the door to selective screening of workers and to wage cuts or demands for other concessions from these workers.[40] As new employers are required to enroll in the system through federal or state mandates, including those who have not voluntarily used E-Verify, a higher proportion of employers may mistakenly or intentionally misuse or abuse the E-Verify rules.

B. The Employer Role in Authentication of Identity

E-Verify also makes employers the primary defense against identity fraud by giving them unique responsibility for identity authentication. This responsibility opens the door for engaging in intentional noncompliance by accepting fraudulent identity data to go through the motions of verification. Indeed, there are cases where employers, not workers, have orchestrated identity fraud.

The employer's role in identity authentication, dating back to the 1986 IRCA law, also perpetuates the defensive hiring electronic verification was intended, in part, to address. Employers may avoid hiring workers who appear to them to be unauthorized, so as to minimize the risk that they will face a future penalty or a workforce disruption as a result of hiring unauthorized workers. At the same time, laws designed to prevent discrimination forbid employers from subjecting documents to more than a facial review — a task for which employers also lack appropriate knowledge and training — and employers may be prosecuted for refusing to accept valid documents. Many employers believe they face an all-but impossible situation in attempting to reconcile these competing requirements. E-Verify does little to ameliorate that longstanding dilemma since it supplemented rather than replaced the I-9 process.

Giving employers the responsibility of authenticating identity is also costly for them. Large employers with multiple hiring sites and centralized human resources (HR) departments find identity authentication especially problematic because worker hiring and use of E-Verify may occur at different locations, which can make it difficult to accommodate the E-Verify process and required timeframes. E-Verify and I-9 compliance jobs are often filled by entry-level employees with high

---

nonconfirmation notices (Westat, *Findings of the Web-Based Basic Pilot Evaluation*, p. 71-77). These data may underreport noncompliance where employers know they are violating program rules. In their detailed case study of five unnamed employers during the same period, Westat found that three out of five employers systematically failed to comply with some TNC requirements (Westat, *Findings of the Web-Based Basic Pilot Evaluation,* p. E-6).

[39] Westat, *Findings of the Web-Based Basic Pilot Evaluation*, pp. 96-100.

[40] A 2008 survey of immigrant workers in Arizona found evidence of intentional employer misuse of E-Verify: 30 percent of workers were rescreened by employers after the three-day period during which screening is permitted, 16 percent were denied back wages, 10 percent were threatened with firing, 12 percent had their wages cut, 5 percent reported harassment on the job, and 7 percent reported that employers had threatened to call ICE. See Isaacs, *Sanctioning Arizona,* p. 10.

turnover rates and limited training, subjecting employers to legal risks, and further undermining effective employment verification.

C. Off-the-Books Employment

A final problem with making employers the central actors in employment verification is that it makes the system especially vulnerable to off-the-books employment. Intentionally noncompliant employers who know or suspect a worker is unauthorized can simply opt out by not submitting the worker's identity data to E-Verify. Indeed, whereas the current enforcement regime encourages employers of unauthorized workers to deduct payroll taxes and Social Security in order to go through the motions of compliance and protect themselves from prosecution for knowingly employing unauthorized workers or for violations of tax law, the shift to E-Verify makes this strategy more difficult by nonconfirming incorrect Social Security numbers.[41]

Anecdotal evidence and media reports suggest that some employers in states with mandatory E-Verify have responded by taking some or all of their workers off the books.[42] As with identity fraud, off-the-books employment as an unintended consequence of E-Verify deepens the broader negative effects of unauthorized employment. In addition to lost federal revenues and Social Security payments, employers who hire workers informally may be more likely to violate environmental, wage, and safety regulations to the detriment of all Americans.[43]

Taken together, the evolution of E-Verify as an employer-centric, rather than an employer-neutral, system has created conditions and incentives for:

- Higher rates of erroneous nonconfirmations and adverse consequences for workers who receive — or seem to employers likely to receive — TNCs;
- An imbalance in knowledge between employers and employees regarding the responsibilities of employers and the rules of E-Verify and a lack of remedies for workers subject to adverse actions that violate E-Verify program rules;
- Continued identity fraud and discriminatory "defensive hiring" by employers, in addition to continued guesswork and cost burdens for employers; and
- Increased potential for off-the-books employment as an unintended consequence of mandatory electronic verification.

---

[41] Thus, the Congressional Budget Office (CBO) has estimated that requiring employers to participate in E-Verify without a legalization program would decrease federal tax revenues by $17.3 billion over a ten-year period. See Peter Orszag, "Letter to the Honorable John Conyers, Jr.," (Washington, DC: Congressional Budget Office, April 4, 2008), http://www.cbo.gov/ftpdocs/91xx/doc9100/hr4088ltr.pdf.

[42] Daniel González, "Illegal workers manage to skirt Arizona employer-sanctions law – Borrowed identities, cash pay fuel an underground economy," *Arizona Republic*, November 30, 2008, http://www.azcentral.com/news/articles/2008/11/30/20081130underground1127.html.

[43] See Fiscal Policy Institute, *The Underground Economy in the New York City Affordable Housing Construction Industry*, (Albany, NY: Fiscal Policy Institute, 2007), http://www.fiscalpolicy.org/publications2007/FPI_AffordableHousingApril2007.pdf. Also see Donald Kerwin, *The Efficacy of Labor Standards Enforcement as an Immigration Enforcement Tool*" (Washington, DC: Migration Policy Institute, forthcoming 2009).

Unfortunately, the frequency of these problems and their adverse effects would be exacerbated under mandatory electronic verification if the current E-Verify model continues to be used. The absence of a reliable identification mechanism and to a lesser extent root database errors, cause E-Verify to produce both false confirmations and nonconfirmations.

The system's exclusive reliance on employers to manage the confirmation process exacerbates these problems and deepens their negative effects. USCIS has done an impressive job of reducing error rates and rapidly expanding the numbers of employers who have voluntarily enrolled in the system. However, further substantial database improvements will be difficult to accomplish in the near term. Hence the dilemma: there is a clear public policy imperative in growing E-Verify, but a clear risk that requiring participation in an employer-centric system — as presently designed — will not achieve the vital immigration policy goal of effective compliance to achieve employer enforcement as an essential tool of immigration control.

The remainder of this report examines ways to resolve this dilemma, both through fielding pilot programs that test alternatives for building a next-generation E-Verify which may be better equipped to avoid errors, and through making improvements to the existing E-Verify system.

V. A Next-Generation E-Verify: What Would an Employer-Neutral System Look Like?

As Congress and the administration take up immigration reform, there is the opportunity to provide a statutory framework for electronic verification that allows E-Verify to become a more employer-neutral system. The following describes three possible strategies for implementing such a system. The approaches are not mutually exclusive, and may be considered in combination. The goals of a next-generation E-Verify would be to:

- Remove the guesswork in authenticating the identities of new hires;
- Reduce the incentives and potential for identity fraud; and
- Streamline the steps employers are required to take in confirming the authorization to work of new hires.

Such approaches also employ newer technologies that have been successfully used in the private sector since the E-Verify model was designed. As with E-Verify, the strengths and weaknesses of new approaches can only be fully assessed by implementing them, so testing through voluntary pilot projects alongside the existing system should be provided for in reform legislation as its new mandates are phased in. Our recommendation that Congress authorize voluntary verification pilots alongside E-Verify is similar to the Secure Employment Eligibility Verification System proposal in the New Employee Verification Act (H.R. 2028) authored by Rep. Sam Johnson (R-Texas), though our proposed pilots would not depend on private-sector verification firms.[44] Testing should also be

[44] The Johnson legislation, known as NEVA, would also redesign the basic E-Verify system, shifting responsibility from DHS to SSA and requiring employers to use the National Database of New Hires (NDNH) as the verification portal. We have argued elsewhere that use of NDNH would be problematic; see Rosenblum, *The Basics of E-Verify, the US Employer Verification System*, http://www.migrationinformation.org/Feature/display.cfm?ID=726 and Michael Fix, Doris Meissner, Randy Capps, Elizabeth Dennison, and Roberto Suro, *Mandatory Verification in the*

guided by dialogue with all types and sizes of employers and employer groups to elicit information and buy-in regarding what would and would not work for them in the workplace.

Recommendation: **Test up to three new voluntary pilot programs to help determine the next generation of E-Verify.**

Reforms to improve the current E-Verify and the next-generation reforms described below are not mutually exclusive. A combination of these proposals should be field-tested on a pilot basis alongside the current system. Pilot testing could be managed relatively seamlessly by re-designing E-Verify's opening portal to allow employers to choose among multiple acceptable systems. The existing E-Verify system (with the improvements outlined in section VI) should remain in place unless and until one of the alternative systems proves through pilot testing to be a sufficient improvement to merit replacing it. Allowing multiple verification systems to operate in parallel would provide an important opportunity to evaluate their strengths and weaknesses as the United States seems poised to adopt mandatory electronic verification; one of these systems may or may not emerge as the best fit for workers and employers.

Components of possible pilot programs are described below, presented in no particular order of preference.

Pilot 1: Authentication of Identity through Secure Documents

The single biggest weakness of E-Verify is the inability of the system to authenticate the identity of individuals whose work eligibility it confirms or nonconfirms. E-Verify (like the I-9 system) relies on employers to determine that the new hire presenting an identity document, such as a driver's license or green card, is the rightful owner of the document. Over the years, many lawmakers, distinguished commissions, analysts, and others have called for improved identity documents, possibly to include the creation of a national ID card or a secure Social Security card, to strengthen employment verification. Most recently, Senate immigration subcommittee Chairman Charles Schumer (D-NY), in announcing seven principles for immigration legislation, called for biometric identification as an essential feature of employer verification and enforcement.[45]

A verification system built on a secure card could consist of a new work authorization card, or it could allow for a limited number of existing secure documents — green cards and work authorization cards for work-authorized noncitizens, US passports for US citizens, and the development of PASS ID-compliant licenses or a secure Social Security card for other US citizens and work-eligible noncitizens The first four all contain (or would contain) digital photos, which, with photo screening, can tie the identity of the cardholder to the card with reasonable reliability. A new, secure Social Security card would need to contain similar features.

States: A Policy Research Agenda, December 17, 2008, Appendix II, http://www.uscis.gov/files/nativedocuments/e-verify-mandatory-impl-evaluation.pdf. NEVA's verification system also would include a number of important improvements to prevent employer misuse and wrongful nonconfirmation, some of which are similar to those we recommend. This report does not provide a detailed analysis of NEVA or any other pending legislation.

[45] Remarks by US Senator Charles Schumer (D-NY) at the 6th Annual Immigration Law and Policy Conference, Migration Policy Institute, June 24, 2009, http://schumer.senate.gov/new_website/record.cfm?id=314990.

A. Advantages

In principle, a secure card offers an elegant solution to identity and work authorization verification.

- With a secure card issued to all legal workers, most of the guesswork in the current system would disappear. Employers would examine an individual's work authorization document — or possibly swipe its magnetic strip or scan its biometric chip — to receive confirmation of a person's identity and authorization to work. Indeed, a perfect card system would eliminate the need for electronic verification altogether; verification would be embodied in the card itself as a result of the work authorization and identity authentication that would be required in the enrollment process that would have to be established to issue secure cards.
- Americans have become increasingly accustomed to requirements for producing various kinds of identification documents for ordinary purposes, such as boarding airplanes, entering buildings, and checking into hotels. So, identity document requirements have become customary and are no longer seen as unreasonable or un-American. In the aftermath of 9/11, many Americans see cooperation with document requirements as being an essential feature of efforts to protect public safety and national security.
- Identity fraud has become a serious personal privacy and law enforcement challenge that secure identity documents could help to mitigate.
- Rules, procedures, and accountability measures that would be required of government agencies charged with managing the databases underlying a secure card system — either a new card or a combination of existing cards — are well known and have been successfully practiced in other realms where sensitive information must be collected to serve important public policy goals, e.g. protections against misuses of tax and IRS data.
- Card requirements could contribute to building public confidence that Congress and the government are committed to effective immigration enforcement and controls against illegal immigration.

B. Disadvantages

Although there is a clear logic to a work authorization card there are also significant downsides to a card-based system:

- There has long been deep political and philosophical opposition to the idea of new identity document requirements overall and the databases that would be created to support them.
- There is no such thing as a fraud-proof card. A secure card or cards would raise the cost of document fraud, but sophisticated criminals will crack card security features as soon as markets for fraudulent cards emerge. Linking the verification process to secure cards thus creates a false sense of security, and perhaps even builds in failure and the necessity of revisiting verification again in the near future.
- Any card-based system would be more prone to employer misuse because cards permit prescreening.
- A secure card system relying only on digital photos would not provide full certainty of identity authentication because appearances can change — even with periodic re-issuance requirements. Conversely, some cardholders could be improperly denied work with valid cards due to changes in appearance from the photo on the card.

- Employers, especially small businesses that only hire a handful of new employees a year or less, might balk at having to purchase swiping or scanning equipment.
- The cost to the federal government of issuing a new identity document would be substantial, as evidenced by the discussions concerning the achievability of the REAL ID mandate.
- Whatever the disclaimers, a secure card is likely to create demands to use the card for other purposes, such as managing medical records, boarding airplanes, or gaining access to public buildings. A card-based system would also raise significant broader privacy issues and be seen as a massive new government intervention. For better or worse, the better a card requirement works, the more likely its role would expand to other uses.

C. The Hidden Costs and Benefits of Secure Cards

The burden of obtaining a new secure card would be greatest for US citizens. Many lawful noncitizens already possess cutting-edge, secure identification documents — a green card or work authorization document — and the US-VISIT program has collected biometric data (fingerprints) for 90 million permanent and temporary immigrants. Most US citizens depend on state-issued driver's licenses of varying formats with disparate security features, and some also have passports. Yet an estimated 11 percent of adult US citizens (about 22.5 million people in 2007) do not have current government-issued identity documents of any kind, a rate which increases to 18 percent among elderly citizens, 16 percent among voting-age Hispanic citizens, 25 percent among voting-age African Americans, and 15 percent among citizens earning less than $35,000 per year.[46]

The operational challenge — and most of the cost — of a new or improved card would come from the *enrollment process* required to issue and obtain the new cards.[47] US workers (citizens and work-authorized noncitizens) would be required to visit a government agency or office to authenticate their identity, a process which would have to prevent unauthorized immigrants from fraudulently claiming US identities and enrolling in the system.[48] Enrollees would submit a digital photograph and fingerprints, or other biometric data.

---

[46] Brennan Center for Justice, *Citizens without Proof: A Survey of Americans' Possession of Documentary Proof of Citizenship and Photo Identification* (New York: New York University, 2006), http://www.brennancenter.org/page/-/d/download_file_39242.pdf.

[47] SSA estimated in 2006 that it would cost a total of $10.3 billion to reissue cards to 240 million SSN cardholders over the age of 14 ($9.5 billion plus an additional $3 per card), with processing costs representing almost all of this expense. See Statement of the Honorable Jo Anne B. Barnhart, Commissioner, Social Security Administration, before the House Committee on Ways and Means, July 26, 2006, http://www.ssa.gov/legislation/testimony_072606.html. Also see GAO, *Social Security Administration: Improved Agency Coordination Needed for Social Security Card Enhancement Efforts* GAO-06-303 (Washington, DC: Government Accountability Office, March 2006), http://www.gao.gov/new.items/d06303.pdf. These numbers do not account for the lost productivity in the US workforce: If it takes the average worker four hours to enroll in a new identity database, enrollment for 160 million workers would result in 320,000 work-years of lost productivity, and the total cost in lost wages (billing at the Bureau of Labor Statistics' April 2009 average hourly wage rate of $18.51) would be $11.8 billion.

[48] Many experts see the prospect of unauthorized immigrants fraudulently enrolling in the system as one of the greatest threats to any new identity system, but the problem would be mitigated by two factors: unauthorized immigrants would be reluctant to visit a DHS office and submit their biometric data; and fraudulent enrollments would be detected when the real holder of the identity seeks to register the same information, allowing the fraudulent ID to be blocked (following resolution of the identity dispute). The most powerful tool for preventing this type of fraud would be to link enrollment in a new identity database to comprehensive immigration reform, eliminating the largest source of demand for employment-related stolen identities.

While costly, the enrollment process would provide an opportunity to detect and correct most remaining "root error" problems in government databases that lead to TNCs, though new errors would likely emerge, including as a result of legal name changes. Enrollment would also be the basis for other forms of more employer-neutral verification that could build an enhanced E-Verify database, and a next-generation E-Verify that would not depend on secure cards at all.[49]

Pilot 2: PIN Pre-Verification

A personal identification number (PIN) pre-verification system would give individual workers responsibility for managing their own eligibility verification, rather than relying exclusively on employers as E-Verify currently does. Employers would be responsible for verifying that a worker had checked in with the system and for photo screening those they hire.

A. Enrollment and Verification

Prior to employer verification in a PIN pre-verification system, a worker would be required to enroll with the system as described above. As with the other pilot alternatives, work authorization and identity would be established during the enrollment process. Workers would provide a digital photo and would select a PIN number, which would allow them to manage their identity record in the future by phone or online. At the point of enrollment, the worker's identity data would be locked to prevent identity theft.

Verification would then be a two-stage process as follows:

- **First stage.** Workers would use their PIN number to "check in" with the system by phone or Internet prior to accepting a new job and would receive a single-use code and a printed receipt, which would be proof that the worker had self-verified and is work authorized. A worker could only receive the single-use code and verification receipt after s/he is confirmed by the system; any nonconfirmation would have to be corrected at this point in the process.
- **Second stage.** The worker provides the code to an employer instead of filling out an I-9 form after accepting a job. The code on the worker's verification receipt is proof of work authorization. The system would provide the employer with automated verification that the worker's code is valid. As a protective measure, a verification code would expire after a single use, so that the worker would be required to check in with the system again prior to accepting additional employment and being verified by an additional employer. With verification that the worker's code is valid, employers also would receive an automated copy of the photo submitted by the worker during enrollment to allow for photo screening to verify identity.

[49] Another possibility is "knowledge-based" or "biographic" screening, in which the worker answers one or more identifying questions (e.g., "What was your mother's maiden name?" or "Where did you attend high school?") to authenticate his or her identity. Knowledge-based screening may be viewed as less intrusive than biometric screening, and large private-sector databases already contain relevant data for many US workers; but covering the entire workforce through knowledge-based screening may be problematic, and the use of private-sector databases for EEVS identity authentication would raises a number of technical, political, and privacy challenges.

B. Advantages

The advantages of a PIN pre-verification system are as follows:

- The system would reduce identity theft by locking a worker's identity data until the worker checks in with the system. Workers also would register a phone number or email address with the system, allowing them to be notified if someone fraudulently checks in using the worker's identity and PIN number. The premise is that workers are the best defenders of their own identity data.
- Americans are accustomed to having their photos taken and stored for purposes of identity protection and document integrity. Driver's licenses and passports, for example, and many workplace IDs contain photos for similar purposes. Likewise, PIN number processes have become familiar and constitute personal protection devices that are in widespread use in the private sector and are used successfully by most people in numerous commercial realms.
- Worker ownership of the first stage of the verification process should result in fewer false nonconfirmations because workers would correct erroneous TNCs during the enrollment process and first-stage self-verification.
- Workers would emerge from the first stage of a PIN pre-verification system armed with information about their own legal status and how to correct a TNC in case of employer error. This information should be printed in the worker's native language on their self-verification receipt. In this way, the first stage of the process should sharply reduce employer mistakes or misuse. DHS could establish a special toll-free number and expedited appeals process for workers who have already pre-verified but then face tentative nonconfirmation during the second (employer verification) stage.
- By front-loading the correction of TNCs during enrollment, a PIN pre-verification system would exempt employers from responsibility for the resolution of TNCs. Because workers would self-verify prior to accepting employment, a PIN pre-verification system could permit employers to verify new hires before they actually begin their jobs — a change which would represent a large cost savings and address one of employers' major complaints about E-Verify. During the second stage (employer verification), the system would almost always offer employers a clear red-light/green-light response.
- This system would not require new identification cards. Photo screening could be supplemented by reviewing a physical card, but photo screening makes the same image available that would be on a card, while avoiding many of a card's disadvantages.

C. Disadvantages

The disadvantages of such a system are that:

- The enrollment process would be costly for the government to administer and burdensome for workers, especially those of limited means who may encounter difficulties in gathering the information required to authenticate their identity. The system likely would be required to issue provisional work authorization to workers who face delays during first-stage verification.
- A PIN number system would not prevent *collaborative* identity fraud (identity "sharing"), as when a legal worker willingly loans or sells his or her identity data (and PIN number, in this case) to another worker. The system would depend on diligent photo screening by the

employer and data analysis (auditing of the pre-verification process) by system administrators to prevent this type of identity fraud.

- Photographs as the biometric for identity authentication are not as reliable as other biometrics, such as fingerprints. People's appearances may change or those perpetrating fraud may intentionally make themselves appear different.

Pilot 3: Biometric Scanning

A biometric scanning system would permit or require employers to collect biometric data beyond digital photos directly from workers as part of the verification process. Biometric data would be captured at the worksite and compared to biometric data stored in a central database or on a card, or used as an encrypted biometric key to confirm the worker's identity. The capture of biometric data would replace or supplement the employer's review of documents as a tool of identity authentication.

A. Enrollment and Verification

Like a secure card or PIN pre-verification system, a biometric scanning system would require workers to enroll in an enhanced E-Verify database. For biometric scanning, workers would also submit additional biometric data, most likely fingerprints or an iris scan. (Identifiers such as facial or voice recognition have higher error rates.) Biometric data could be stored on a card and later retrieved by a user with a card reader, and/or it could be stored in a central database and retrieved through E-Verify system procedures.

Matching a card or a biometric record to its owner would require the additional step of retaking a finger print or iris scan and comparing the data to that stored on the card or in the database. To verify work authorization, employers would capture a biometric identifier, such as a fingerprint, rather than reviewing a worker's identity document. In principle, biometric scanning could replace and eliminate the requirement that employers review a photograph; the worker's fingerprint would be used for identity authentication instead.

The biometric data captured from the worker by the employer could either be matched with the same data stored in a central database through the E-Verify system, or it could be matched with the same biometric data stored on a work authorization card.[50] In either case, for the purposes of meeting employment verification requirements, the employer would be responsible for capturing the worker's fingerprints or other biometric data, but the government would be responsible both for identity authentication and work authorization verification.

B. Advantages

The advantages of a biometric system are as follows:

- A biometric scanning system would be the surest way to prevent identity fraud, and the best defense against collaborative identity sharing in particular.

[50] On storing biometric data in a card, rather than a centralized database, see Jim Harper, *Identity Crisis: How Identification is Overused and Misunderstood* (Washington, DC: Cato Institute 2006), pp. 227-229.

- Removing any burden of responsibility for identity authentication from employers would eliminate most opportunities for employer mistakes during identity authentication and should reduce defensive hiring and related offenses.
- By producing highly reliable verification, such a biometric system would give employers a state-of-the-art tool to screen out unauthorized workers and contribute to building confidence among employers in the legality of their workforces. The system would also likely contribute to public confidence in the validity and effectiveness of controls to combat illegal immigration.
- A biometric scanning system based on a biometric card, rather than a centralized biometric database, would address many of the privacy concerns associated with biometric scanning.

C. Disadvantages

There are also serious limitations to such a biometric system:

- Like a PIN pre-verification system, the use of biometrics would require that workers enroll in an enhanced E-Verify database. The costs of enrollment, both to the government and to enrolling workers, would be higher than in the PIN number process because of the added costs of collecting biometrics beyond photos.
- Employers would have to purchase biometric-capture hardware or pay for scanning services, which would add to overall program costs, especially in the case of small businesses which hire only a few people a year.[51] Such issues could result in increased incentives for small employers not to use the system. There are successful private-sector biometric firms that go either to the client workplace with mobile biometric-capture hardware or have the workers come to them. However, the history of subcontractor arrangements in immigration employment practices as a way around employer accountability requirements would argue for careful design of such relationships and services.
- Biometric technology has become very sophisticated and accurate but it is not perfect, and the system would produce false nonconfirmations.[52] False nonconfirmations would likely disproportionately affect manual workers, who sometimes cannot provide useable fingerprints because of damaged fingertips.
- The construction of a biometric database for an enhanced E-Verify would raise additional privacy risks and technology challenges beyond those associated with existing databases or an enhanced E-Verify database without biometric identifiers because of the system's larger storage requirements and because of the security protections needed to prevent theft of biometric data or algorithms.[53] If biometric data is compromised, it is much more difficult for individuals to reclaim identity than is the case with current ID fraud.

[51] The retail cost of fingerprint scanners ranges from as little as $35 (low-resolution, single-print scanner) to as high as several thousand dollars (high-resolution ten-print scanners).

[52] The technology is challenging but not overwhelmingly so because the system would not be asked to look for a one-to-many match, as in the case of many criminal investigations, but rather a one-to-one match against a specific record. Even so, existing biometric systems have false rejection rates ranging from 0.1 to 20 percent; see Ann Cavoukian and Alex Stoianov, *Biometric Encryption: A Positive-Sum Technology that Achieves Strong Authentication, Security AND Privacy*, (Ontario, Canada: Information and Privacy Commissioner of Ontario, 2007), p.8, http://www.ipc.on.ca/images/Resources/bio-encryp.pdf .

[53] Ibid., p. 7-10. As Cavoukian and Stoianov explain, biometric encryption, in which biometric data are linked to an encrypted PIN number, rather than stored directly in the database, may mitigate these security risks.

However, the greatest concerns about a biometric scanning system can be expected to be political and philosophical. Many Americans — perhaps most — will object to providing the government with their fingerprints or other biometrics beyond a photo, much less providing employers with fingerprints when they take a new job. Such procedures are widely associated with criminal justice system practices, and seem antithetical to measures appropriate for law-abiding US citizens. Should such a system be established without broad public support, its effectiveness and use could be seriously undermined by high rates of nonparticipation.

Phasing in and Pilot Testing Next-Generation Alternatives

Enrollment processes to issue secure documents — existing or new — or to develop a PIN pre-verification or biometric system could take place in phases over time. Assuming new E-Verify mandates are a product of comprehensive immigration reform legislation, three significant categories of individuals are already likely to be in contact with USCIS or E-Verify administrators. They are: persons entering the United States with temporary or permanent visas who are authorized to work and could be required or permitted to enroll in the system as part of visa-issuance processes; unauthorized immigrants eligible for legalization pursuant to immigration reform; and legal residents and authorized noncitizen workers and US citizens who get TNCs from E-Verify and correct their records.

Were enrollment opportunities available, other workers who are seeking employment might choose to enroll to protect themselves against identity theft or a future TNC. This would require a large-scale public education campaign. Finally, assuming a work authorization card or other requirements would extend only to those seeking new jobs, enrollment would occur over time as a part of job searches by those seeking new employment. Thus, workers in stable employment situations who do not change jobs might never need to enroll and obtain a new card or PIN number.

At the same time, an employer-neutral E-Verify with either a new or existing secure card or with PIN/biometric technologies would represent a dramatic policy shift for the United States and a major operational challenge for government agencies, employers, and workers, especially US citizens.

Any mandate for an enhanced E-Verify database — including a mandate for a new work authorization document or secure Social Security card — should be preceded by a surge in enrollment capacity with temporary field offices to handle millions of workers. The surge in enrollment capacity could coincide with, and should be linked to, the large number of registrations needed to accommodate a legalization program in the context of comprehensive immigration reform, either on a national level or (initially) in states or labor market sectors with a high number of unauthorized immigrants or states with E-Verify mandates. As soon as workers in a region or industry have been given adequate time to enroll in an enhanced database, verification rules could be changed to limit the number of documents workers may present for identity authentication and to permit the use of next-generation E-Verify systems.

VI. Recommendations for E-Verify Improvements: What Reforms Are Needed?

DHS and Congress should continue to build, improve, and invest in E-Verify. Three sets of reforms are urgently needed to strengthen the effectiveness, performance, and stakeholder support for the current system now; they merit high-priority attention and action.

Redress for Unresolved System Errors

E-Verify wrongly nonconfirms some US citizens and other legal workers because employers fail to inform workers of TNCs or workers are unable to correct TNC errors. These mistakes will persist. A degree of error is inherent in a large information system. The TNC process determines whether nonconfirmations are the result of database or user errors, or the result of unauthorized worker employment. However, the TNC process presumes that workers are unauthorized unless they can prove otherwise.

Recommendation: Strengthen due-process protections and compensate workers when system errors result in the wrongful termination of US citizens and other legal workers:

- Establish a right to review and correct one's record outside the burdensome process of a Freedom of Information Act request.[54] USCIS should establish a simple and inexpensive procedure to allow individuals to authenticate their data and confirm their work-authorization status in SSA and DHS databases prior to employer screening. This should include establishment of a "worker portal" that would allow workers to access the E-Verify system independently. USCIS is exploring this concept. It should be a top priority.
- Permit workers to appeal a final nonconfirmation and be compensated by the government for lost wages and other expenses in the case of system error that led to a job loss. No such mechanism now exists, in part because USCIS cannot confirm that such errors have occurred. Appeals would be unusual, given other due-process and employer compliance reforms; and fraudulent appeals are unlikely since unauthorized workers would be reluctant to engage in this process.
- Legislation should clarify that workers must be treated as work-authorized with the right to remain employed without adverse employment consequences pending the resolution of a contested TNC and possible appeals of a final nonconfirmation. A stay of nonconfirmation should be issued pending resolution of any appeals process.

[54] The Privacy Act of 1974 establishes that individuals have the right to review and correct records in government databases, 5 U.S.C. §§ 552, et seq.; see testimony of Timothy Sparapani, Senior Legislative Counsel, American Civil Liberties Union, before the US House of Representatives Committee on the Judiciary Subcommittee on Immigration, Citizenship, Refugees, Border Security, and International Law, June 10, 2008, http://www.aclu.org/images/asset_upload_file944_35580.pdf.

Employer Training and Worker Protections

E-Verify contains numerous steps and guesswork for employers that are likely to increase with mandatory electronic verification. To mitigate the potential for employer mistakes or misuse of the system, additional penalties and protections must be an explicit element of E-Verify.

Recommendation: Strengthen enforcement of worker protections and employer penalties, training, and oversight.

- Impose penalties on noncompliant employers by adding E-Verify worker protections to the list of unfair immigration-related employment practices prohibited by §274B of the Immigration and Nationality Act (INA). Currently, the only penalty against employers for prescreening workers, selective screening, suspending a worker pending the resolution of a TNC, or otherwise violating E-Verify's worker protections is removal from the program; and even this punishment has been exceedingly rarely, if ever, invoked. Congress should enumerate prohibited E-Verify employment practices, and provide for meaningful civil penalties as well as a right of private action when government investigators fail to pursue a worker's properly filed complaint.[55]
- Congress should provide additional funding to strengthen the Justice Department's Office of Special Counsel for Immigration-Related Unfair Employment Practices to ensure rigorous investigation and prosecution of illegal E-Verify employment practices, and to hire additional Administrative Law Judges to swiftly hear complaints filed by OSC and employees.[56] Congress also should strengthen the DHS Office for Civil Rights and Civil Liberties to ensure proper monitoring of E-Verify abuses from within DHS.
- Continue and expand efforts by the E-Verify Monitoring and Compliance branch to ensure that employers understand their obligations to new hires under E-Verify, especially the opportunity to correct a TNC and remain employed without adverse consequences while a TNC resolution is pending. Training and oversight should also have a clear focus on prohibitions against prescreening. All E-Verify users must take an online tutorial and pass a test afterward on proper procedures, but these procedures are not always remembered or followed. Additional educational materials should be provided through mass media, employer associations, direct communication from USCIS, and other appropriate outreach. USCIS and the DHS Office of Civil Liberties have already initiated important projects along these lines, which should be continued and expanded.
- Organize broad worker education initiatives to ensure that workers understand their rights under E-Verify, especially the right to correct a TNC without facing adverse employment consequences. Worker education should also make use of multiple media and outreach strategies. USCIS and the DHS Office of Civil Liberties have already initiated important projects along these lines, which should be continued and expanded. Funding should be made available for nonprofit, faith-based, and other organizations to help educate the public.

[55] Current penalties for unfair immigration-related employment practices range from $100 to $2,000 for a first offense, and up to $10,000 for repeat offenders; see INA §274B(g).

[56] The Office of Legal Counsel is already responsible for the investigation of charges and issuance of complaints related to other unfair immigration-related employment practices, such as discrimination on the basis of national origin or (in the case of legal aliens) citizenship status; see INA §§274B(a)-(c).

Data Analysis, Audits, and Workplace Enforcement

E-Verify's greatest weaknesses are vulnerability to identity fraud and off-the-books employment. A well-designed system will make it easy for employers to verify their workers' legal status; but even a perfect one cannot prevent employers from evading the system if they are determined to do so. In the absence of a fundamentally different system, identity fraud and off-the-books employment can only be combated by systematic oversight and skillful worksite enforcement.

Recommendation: Monitor E-Verify compliance and strengthen auditing to identify patterns of misuse, selective screening, identity fraud, and off-the-books employment. An effective, up-and-running monitoring and compliance unit must be a top DHS priority.

- DHS should continue and expand a recent initiative to develop algorithms to match patterns of E-Verify use and nonuse with likely cases of employer misuse. Such analyses should include identifying firms that verify too few workers relative to industry standards (possibly indicating off-the-books employment), firms with many nonconfirmations but too few TNC corrections (possibly indicating pre-screening or other misuse of the system), and identity data which is verified suspiciously often, possibly indicating identity fraud.[57] This type of auditing strengthens E-Verify's role in immigration enforcement and its protections for lawful workers.
- Auditors should also analyze samples of confirmed and nonconfirmed workers to estimate the actual rate of false confirmations and nonconfirmations — a labor-intensive undertaking, particularly in the case of final nonconfirmations. These error rates should be tracked over time in order to evaluate E-Verify's accuracy and test system improvements. Lawmakers should establish a dedicated office within USCIS or elsewhere to participate in these audits for database accuracy.

Recommendation: Increase workplace enforcement staffing and protocols to include credible threats of enforcement and meaningful penalties where employers are noncompliant with verification requirements. In addition to the existing USCIS-US Immigration and Customs Enforcement (ICE) memorandum, such compliance enforcement should include developing protocols for referring cases to the Department of Labor (including joint ICE-DOL taskforces), the Equal Employment Opportunity Commission, and the Office of Special Counsel for Immigration-Related Unfair Employment Practices to investigate possible violations of immigration and labor laws.

Recommendation: Enact legislation to permit limited data sharing with the Internal Revenue Service (IRS) and SSA with strict privacy protections.

- Data sharing between DHS, the Internal Revenue Service (IRS), and SSA would strengthen enforcement-based pattern analysis, but DHS' access to these sources should be limited to suspicious cases meeting established suspicion criteria, rather than granted universally, and subject to limited use, limited retention times, and oversight..
- DHS access to IRS and SSA data must be managed carefully to ensure that pattern analysis does not expose good-faith employers to new privacy threats and to prevent use of shared data for purposes beyond verification enforcement.

[57] USCIS has begun to explore data mining in these ways.

- As usage of E-Verify becomes widespread, DHS may be able to conduct pattern analysis against its own records, in which case its access to other federal data sources could be sunset after three to five years.

Ultimately, what are acceptable error and compliance rates and program costs — measured in dollars, and also in the societal impact of electronic verification — are political questions. However, assuming that electronic verification will become mandatory and that the current E-Verify will continue to grow and serve as the initial platform for a mandatory system, it is essential that the necessary program infrastructure also be built so it can properly carry out its immigration policy mission.

VII. Conclusion

USCIS has made impressive progress in reducing E-Verify error rates and rapidly expanding the numbers of employers who have voluntarily enrolled in the system. However, the system continues to produce an unknown number of false confirmations — primarily as a result of the inadequacies of the I-9 identity authentication process and the vulnerability of the system to identity fraud — and false nonconfirmations — primarily a result of database and user errors. Further substantial database improvements may be difficult to accomplish in the near term.

E-Verify is employer-centric, relying exclusively on employers to manage the confirmation process. Error rates and employer mistakes or misuse may increase as new E-Verify mandates under the current system are implemented, raising a real risk that the program's costs and unintended consequences could undermine its benefits as a tool of immigration control. New E-Verify mandates would be especially ill-fated in the absence of comprehensive immigration reform.

The core weakness of E-Verify is that it is not designed for, or capable of, authenticating identity that would prevent false confirmations based on stolen identities. Because identity verification is one of the two key attributes of an effective verification system, E-Verify as it is currently designed can only be partially effective in achieving reliable electronic employment verification.

There is a public policy imperative in growing E-Verify, but a risk that requiring participation in an employer-centric system — as presently designed — will not achieve the vital immigration policy goal of effective compliance in hiring lawful workers that is essential to achieving effective immigration controls. To resolve this dilemma, we recommend that as part of comprehensive immigration reform, Congress provide a statutory framework for mandatory electronic verification that a) provides for up to three new pilot projects as the basis for building more employer-neutral, next-generation E-Verify approaches that address the problem of authenticating identity; and b) strengthens the current E-Verify system.

Getting E-Verify right will be at the heart of successful comprehensive immigration reform, and rushing to expand a flawed system could lead to a repeat of the mistakes of the 1980s**,** thereby threatening the success of current and future reforms.

Works Cited

American Council on International Personnel. 2008. Comments on Proposed Rule Published at 73 Fed. Reg. 33374 (June 12, 2008). August 11, 2008.

Arizona's Employer Sanctions Law. Washington, DC: American Friends Service Committee. http://www.afsc.org/tucson/ht/a/GetDocumentAction/i/74700.

Asian American Legal Defense and Education Fund. 2009. Asian American Access to Democracy in the 2008 Elections. New York: Asian American Legal Defense and Education Fund. http://aaldef.org/docs/AALDEF_Election_2008_Report.pdf.

Bansak, Cynthia and Steven Raphael. 2001. Immigration Reform and the Earnings of Latino Workers: Do Employer Sanctions Cause Discrimination? *Industrial and Labor Relations Review*, 54 (2).

Barnhart, Jo Anne B. 2006. Statement of the Commissioner of the Social Security Administration before the House Committee on Ways and Means. 109th Cong., 2nd sess., July 26, 2006. http://www.ssa.gov/legislation/testimony_072606.html.

Boomer, Christina. 2008. Some Valley workers Having Trouble with E-Verify. *ABC 15 TV*, March 24, 2008. http://www.abc15.com/news/local/story/Some-Valley-workers-having-trouble-with-E-Verify/VdTlB1vZu0--Qy0e5zGJcg.cspx.

Brennan Center for Justice. 2006. Citizens without Proof: A Survey of Americans' Possession of Documentary Proof of Citizenship and Photo Identification. New York: Brennan Center for Justice at New York University. http://www.brennancenter.org/page/-/d/download_file_39242.pdf.

Cavoukian, Ann and Alex Stoianov. 2007. *Biometric Encryption: A Positive-Sum Technology that Achieves Strong Authentication, Security AND Privacy*. Ontario, Canada: Information and Privacy Commissioner of Ontario. http://www.ipc.on.ca/images/Resources/bio-encryp.pdf.

Durand, Jorge, Douglas S. Massey, and Emilio A. Parrado. 1999. The New Era of Mexican Migration to the United States. *Journal of American History* 86 (2).

Federal Acquisition Regulation Case 2007-013. R*egulatory Impact Analysis, Employment Eligibility Verification*. October 2008.

Fiscal Policy Institute. 2007. *The Underground Economy in the New York City Affordable Housing Construction Industry*. Albany, NY: Fiscal Policy Institute. http://www.fiscalpolicy.org/publications2007/FPI_AffordableHousingApril2007.pdf.

Fix, Michael, Doris Meissner, Randy Capps, Elizabeth Dennison, and Roberto Suro. *Mandatory Verification in the States: A Policy Research Agenda*. Washington, DC: Migration Policy Institute. December 2008.
http://www.uscis.gov/files/nativedocuments/e-verify-mandatory-impl-evaluation.pdf.

González, Daniel. 2008. Illegal workers manage to skirt Arizona employer-sanctions law. Borrowed identities, cash pay fuel an underground economy. *Arizona Republic*, November 30, 2008.
http://www.azcentral.com/news/articles/2008/11/30/20081130underground1127.html.

González, Daniel. 2008. Illegal workers manage to skirt Arizona employer-sanctions law – Borrowed identities, cash pay fuel an underground economy. *Arizona Republic*, November 30, 2008.
http://www.azcentral.com/news/articles/2008/11/30/20081130underground1127.html.

Hansen, Ronald. 2008. Economy Serves Up Unhappy Meal: Worst Lull in 2 Decades is Hurting Valley Restaurateurs. *Arizona Republic*, March 3, 2008.
http://www.azcentral.com/arizonarepublic/news/articles/0303biz-econ-restaurants0303.html.

Harper, Jim. Identity Crisis: How Identification is Overused and Misunderstood. Washington, DC: Cato Institute 2006.

Illegal Immigration Reform and Immigrant Responsibility Act (IIRIRA) of 1996. Public Law No. 104-208. September 30, 1996.
http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=104_cong_public_laws&docid=f:publ208.104.pdf.

Immigration and Nationality Act of 1952. Public Law No. 82-414. December 24, 1952. Amended and updated as of March 20, 2009.
http://www.uscis.gov/propub/ProPubVAP.jsp?dockey=c9fef57852dc066cfe16a4cb816838a4.

Intel Corporation. 2008. Comments on Proposed Employment Eligibility Regulations Implementing Executive Order 12989. August 8, 2008.

Isaacs, Caroline. 2009. *Sanctioning Arizona: The Hidden Impacts of Arizona's Employer Sanctions Law*. Washington, DC: American Friends Service Committee.
http://www.afsc.org/tucson/ht/a/GetDocumentAction/i/74700.

Javelin Strategy and Research. 2009. *2009 Identity Fraud Survey Report*. Pleasanton, CA: Javelin Strategy and Research.
http://www.javelinstrategy.com/products/A87547/127/delivery.pdf.

Kerwin, Donald. 2009. The Efficacy of Labor Standards Enforcement as an Immigration Enforcement Tool. Washington, DC: Migration Policy Institute. Forthcoming 2009.

Kossoudji, Sherrie A., and Deborah A. Cobb-Clark. 2002. Coming out of the Shadows: Learning about Legal Status and Wages from the Legalized Population. *Journal of Labor Economics* 20 (3): 598-628.

McNulty, Michael and Charles Rangel. 2008. The Facts on Employment Verification: Current Proposals are Unworkable for SSA, Threaten Progress in Reducing Disability Claims Backlog. Letter to House Democratic colleagues, Washington, DC. March 27, 2008. http://www.nationalwatermelonassociation.com/docs/Electronic%20Employment%20Verification%20is%20Unworkable%20for%20SSA%20and%20threatens%20progress.pdf.

Neumann, Peter G. 2007. Testimony of the Principal Scientist, Computer Science Lab SRI International, on behalf of the US Public Policy Committee of the Association for Computing Machinery before the House Committee on Ways and Means Subcommittee on Social Security. 110th Cong., 1st sess., June 7, 2007. http://usacm.acm.org/usacm/PDF/EEVS_Testimony_Peter_Neumann_USACM.pdf.

Pallack, Becky. 2008. Small Businesses Bump into E-Verify Obstacles. *Arizona Daily Star*, April 8, 2008. http://regulus2.azstarnet.com/blogs/clockingin/8616/small-businesses-bump-into-e-verify-obstacles.

Peter Orszag. 2008. Letter to the Honorable John Conyers, Jr. Washington, DC: Congressional Budget Office. http://www.cbo.gov/ftpdocs/91xx/doc9100/hr4088ltr.pdf.

Phillips, Julie A., and Douglas S. Massey. 1999. The New Labor Market: Immigrants and Wages after IRCA. *Demography* 36 (2): 233-246.

Pierce, Elizabeth. 1997. Modeling Database Error Rates. *Data Quality,* 3 (1).

Rivera-Batiz, Francisco L. 1999. Undocumented Workers in the Labor Market: An Analysis of the Earnings of Legal and Illegal Mexican Immigrants in the United States. *Journal of Population Economics* 12 (1): 91-116.

Rosenblum, Marc. 2009. The Basics of E-Verify, the US Employer Verification System. *Migration Information Source*. April 2009. http://www.migrationinformation.org/Feature/display.cfm?ID=726.

Schumer, Charles. 2009. Schumer Announces Principles for Comprehensive Immigration Reform Bill in Works in Senate. Remarks delivered at the 6th Annual Immigration Law and Policy Conference, Migration Policy Institute. June 24, 2009, http://schumer.senate.gov/new_website/record.cfm?id=314990.

Select Commission on Immigration and Refugee Policy. 1981. *U.S. Immigration Policy and the National Interest.* Washington, DC: Government Printing Office.

Sparapani, Timothy. 2008. Opposing the Creation of a "No-Work" List through Mandated Employment Eligibility Verification Prescreening. Testimony of the Senior Legislative Counsel for the American Civil Liberties Union before the House Committee on the Judiciary Subcommittee on Immigration, Citizenship, Refugees, Border Security, and International Law. 110th Cong., 2d sess., June 10, 2008. http://www.aclu.org/images/asset_upload_file944_35580.pdf.

Stana, Richard M. 2008. Employment Verification: Challenges Exist in Implementing a Mandatory Electronic Employment Verification System. Statement for the record by the Government Accountability Office Director of Homeland Security and Justice Issues before the House Committee on the Judiciary Subcommittee on Immigration, Citizenship, Refugees, Border Security, and International Law. 110th Cong., 2d sess., June 10, 2008. http://www.gao.gov/new.items/d08895t.pdf.

Symantec. 2009. *Symantec Internet Global Security Threat Report – Trends for 2008*. Cupertino, CA: Symantec. http://eval.symantec.com/mktginfo/enterprise/white_papers/b-whitepaper_internet_security_threat_report_xiv_04-2009.en-us.pdf.

US Citizenship and Immigration Services. The E-Verify Program for Employment Verification Memorandum of Understanding. Washington, DC: Department of Homeland Security. Accessed October 29, 2008. http://www.uscis.gov/files/nativedocuments/MOU.pdf.

_____. 2009. E-Verify User Manual. Washington, DC: Department of Homeland Security. March 2009: 34-35. http://www.uscis.gov/files/nativedocuments/E-Verify_Manual.pdf.

US Citizenship and Immigration Services Ombudsman. 2008. Observations on the E-Verify Experience in Arizona and Recommended Customer Service Enhancements. Washington, DC: US Department of Homeland Security Office of the Citizenship and Immigration Services Ombudsman. http://www.dhs.gov/xlibrary/assets/cisomb_everify_recommendation_2008-12-22.pdf.

US Commission on Immigration Reform. 1994. *US Immigration Policy: Restoring Credibility*. Washington, DC: Government Printing Office. http://www.utexas.edu/lbj/uscir/reports.html.

US Department of Transportation Federal Highway Administration. 2008. *Licensed Drivers by Sex and Ratio to Population – 2007*. Washington, DC: Department of Transportation Federal Highway Administration. http://www.fhwa.dot.gov/policyinformation/statistics/2007/dl1c.cfm.

US Government Accountability Office. 1990. *Immigration Reform: Employer Sanctions and the Question of Discrimination*. GGD-90-62. Washington, DC: Government Accountability Office. http://archive.gao.gov/d24t8/140974.pdf.

_____. 1999. *Illegal Aliens: Fraudulent Documents Undermining the Effectiveness of the Employment Verification System*. GAOT-GGD/HEHS-99-1 75. Washington, DC: Government Accountability Office. http://archive.gao.gov/f0902b/162489.pdf.

_____. 2005. *Weaknesses Hinder Employment Verification and Worksite Enforcement Efforts*. GAO-05-813. Washington, DC: Government Accountability Office. http://www.gao.gov/new.items/d05813.pdf.

_____. 2006. *Immigration Benefits: Additional Efforts Needed to Help Ensure Alien Files Are Located When Needed.* GAO 07-85. Washington, DC: Government Accountability Office. http://www.gao.gov/new.items/d0785.pdf.

_____. 2006. *Social Security Administration: Improved Agency Coordination Needed for Social Security Card Enhancement Efforts.* GAO-06-303. Washington, DC: Government Accountability Office. http://www.gao.gov/new.items/d06303.pdf.

_____. 2007. *Border Security: Security of New Passports and Visas Enhanced, but More Needs to Be Done to Prevent Their Fraudulent Use.* GAO-07-1006. Washington, DC: Government Accountability Office. http://www.gao.gov/new.items/d071006.pdf.

_____. 2009. *Department of State: Undercover Tests Reveal Significant Vulnerabilities in State's Passport Issuance Process.* GAO-09-447. Washington, DC: Government Accountability Office. http://www.gao.gov/new.items/d09447.pdf.

US Immigration and Customs Enforcement. 2007. 53 former employees at Swift & Company meat processing plant in Cactus, Texas, charged in federal indictments. News release, January 10, 2007. http://www.ice.gov/pi/news/newsreleases/articles/070110amarillo.htm.

US Social Security Administration. 2006. *Accuracy of the Social Security Administration's Numident File.* A-08-06-26100. Washington, DC: Social Security Administration. http://www.ssa.gov/oig/ADOBEPDF/A-08-06-26100.pdf.

Westat. 2007. *Findings of the Web-Based Basic Pilot Evaluation.* Rockville, MD: Westat. http://www.uscis.gov/files/article/WebBasicPilotRprtSept2007.pdf.

About the Authors

Doris Meissner

Doris Meissner, former Commissioner of the US Immigration and Naturalization Service (INS), is a Senior Fellow at the Migration Policy Institute (MPI) where she directs MPI's work on US immigration policy. She also contributes to the Institute's work on immigration and national security, the politics of immigration, administering immigration systems and government agencies, and cooperation with other countries.

Ms. Meissner has authored and co-authored numerous reports, articles, and op-eds and is frequently quoted in the media. She served as director of MPI's Independent Task Force on Immigration and America's Future, a bipartisan group of distinguished leaders. The group's 2006 report and recommendations address how to harness the advantages of immigration for a 21st century economy and society.

From 1993 to 2000, she served in the Clinton administration as Commissioner of the INS, then part of the US Department of Justice. She first joined the Department of Justice in 1973 as a White House Fellow and Special Assistant to the Attorney General. She served in various senior policy posts at Justice until 1981, when she became Acting Commissioner of INS and then Executive Associate Commissioner, the third-ranking post in the agency.

In 1986, she joined the Carnegie Endowment for International Peace as a senior associate. Ms. Meissner created the Endowment's Immigration Policy Project, which became MPI in 2001.

A graduate of the University of Wisconsin-Madison, where she earned BA and MA degrees, she began her professional career there as assistant director of student financial aids. She was also the first executive director of the National Women's Political Caucus (NWPC).

Marc R. Rosenblum

Marc R. Rosenblum is a Senior Policy Analyst at MPI, where he works on the Labor Markets Initiative, US immigration policy, and Mexico-US migration issues.

Dr. Rosenblum is the author of The Transnational Politics of US Immigration Policy (University of California, San Diego Center for Comparative Immigration Studies, 2004) and has also published over 20 academic journal articles, book chapters, and policy briefs on immigration, immigration policy, and US-Latin American relations. His book Defining Migration: America's Great Debate and the History of US Immigration Policy analyzes US immigration policy since the Civil War, with a focus on

the post-IRCA and post-9/11 periods (forthcoming, 2010); and he is the coeditor (with Daniel Tichenor) of The Oxford Handbook of International Migration (Oxford University Press, forthcoming).

Dr. Rosenblum earned his B.A. from Columbia University and his Ph.D. from the University of California, San Diego, and is an Associate Professor of Political Science and the Robert Dupuy Professor of Pan-American Studies at the University of New Orleans. He was a Council on Foreign Relations Fellow detailed to the office of US Sen. Edward Kennedy during the 2006 Senate immigration debate, and was involved in crafting the legislation.