SOCIAL SECURITY ADMINISTRATION'S ROLE IN VERIFYING EMPLOYMENT ELIGIBILITY

HEARING

BEFORE THE

SUBCOMMITTEE ON SOCIAL SECURITY

OF THE

COMMITTEE ON WAYS AND MEANS
U.S. HOUSE OF REPRESENTATIVES

ONE HUNDRED TWELFTH CONGRESS

FIRST SESSION

APRIL 14, 2011

Serial No. 112–SS3

Printed for the use of the Committee on Ways and Means

U.S. GOVERNMENT PRINTING OFFICE
72–872 WASHINGTON : 2012

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

COMMITTEE ON WAYS AND MEANS

SUBCOMMITTEE ON SOCIAL SECURITY

SAM JOHNSON, Texas, *Chairman*

KEVIN BRADY, Texas
PAT TIBERI, Ohio
AARON SCHOCK, Illinois
ERIC PAULSEN, Minnesota
RICK BERG, North Dakota
ADRIAN SMITH, Nebraska

XAVIER BECERRA, California
LLOYD DOGGETT, Texas
SHELLEY BERKLEY, Nevada
FORTNEY PETE STARK, California

JON TRAUB, *Staff Director*
JANICE MAYS, *Minority Staff Director*

CONTENTS

Page

Advisory of April 14, 2011, announcing the hearing 2

WITNESSES

Richard M. Stana, Director, Homeland Security and Justice, United States Government Accountability Office 6
Marianna LaCanfora, Assistant Deputy Commissioner, Office of Retirement and Disability Policy, Social Security Administration 21

Tyler Moran, Policy Director, National Immigration Law Center 34
Ana I. Antón, Ph.D., Professor, Department of Computer Science, College of Engineering, North Carolina State University, on behalf of the Association for Computing Machinery 48
Austin T. Fragomen, Jr., Chairman of the Board of Directors of the American Council on International Personnel, on behalf of the HR Initiative for a Legal Workforce 70

SUBMISSIONS FOR THE RECORD

The Honorable Mr. Dreier 94
AARP 96
American Civil Liberties Union 98
American Federation of State County and Municipal Employees 109
American Immigration Lawyers Association 111
American Meat Institute 113
Asian American Center for Advancing Justice 118
Jessica St Pierre 121
Joint Committee on Taxation 123
National Committee to Preserve Social Security and Medicare 132
National Council of Social Security Management Associations 135
National Immigration Law Center 146
Secure ID Coalition 150

MATERIAL SUBMITTED FOR THE RECORD

Questions and Responses for the Record:
Ana I. Antón, Ph.D. 154
Austin T. Fragomen, Jr. 158
Marianna LaCanfora 163
Richard M. Stana 166

SOCIAL SECURITY ADMINISTRATION'S ROLE IN VERIFYING EMPLOYMENT ELIGIBILITY

THURSDAY APRIL 8, 2011

U.S. HOUSE OF REPRESENTATIVES,
COMMITTEE ON WAYS AND MEANS,
SUBCOMMITTEE ON SOCIAL SECURITY,
Washington, DC.

The subcommittee met, pursuant to call, at 2:06 p.m., in Room B–318, Rayburn House Office Building, the Honorable Sam Johnson [chairman of the subcommittee] presiding.

[The advisory of the hearing follows:]

HEARING ADVISORY

Chairman Johnson Announces Hearing on the Social Security Administration's Role in Verifying Employment Eligibility

Thursday, April 07, 2011

Congressman Sam Johnson (R–TX), Chairman, Subcommittee on Social Security of the Committee on Ways and Means, today announced that the Subcommittee will hold a hearing on the Social Security Administration's (SSA's) role in verifying employment eligibility. **The hearing will take place on Thursday, April 14, 2011, in room B–318 Rayburn House Office Building, beginning at 2:00 p.m.**

In view of the limited time available to hear witnesses, oral testimony at this hearing will be from invited witnesses only. However, any individual or organization not scheduled for an oral appearance may submit a written statement for consideration by the Subcommittee and for inclusion in the printed record of the hearing.

BACKGROUND:

The Immigration Reform and Control Act (IRCA) of 1986 made it illegal for employers to knowingly hire immigrants who were not authorized to work in the United States, requiring employers to examine documentation from each newly hired employee to prove his or her identity and eligibility to work. IRCA led to a process based on the Form I–9, *Employment Eligibility Verification,* requiring employees to attest to their work eligibility and employers to certify that the documents presented reasonably appear to be genuine and relate to the individual. The Social Security card is one of a number of documents the employee may use to demonstrate employment eligibility.

The Illegal Immigration Reform and Immigrant Responsibility Act of 1996 required the then Immigration and Naturalization Service, which became part of the U.S. Department of Homeland Security (DHS) in 2003, to conduct three pilot programs, including the Basic Pilot, to determine the best method of verifying an employee's employment eligibility.

Although initially a temporary program, the Basic Pilot's authorization was extended and ultimately expanded to be available to employers nationwide. In the 2010 Department of Homeland Security Appropriations Act (Public Law 111–83), the Basic Pilot was renamed "E–Verify" and the program was extended until September 30, 2012.

E–Verify is an internet-based system administered by the U.S. Citizenship and Immigration Services within DHS in partnership with the SSA. The employer enters information into the E–Verify system from the Form I–9. Verification requests are first transmitted to the SSA, which checks whether the worker's information matches the SSA's records; those involving non-citizens are then routed to DHS. If a worker's information does not match these government databases, a tentative "non-confirmation" notice is sent and the worker then must contact either SSA or DHS to present needed documentation in order to keep their job.

While E–Verify is free, and participation is mostly voluntary, some companies may be required to use E–Verify by State law (including Arizona and Mississippi) or Federal regulation. All Federal agencies are required to use E–Verify for their new hires and certain Federal contractors and subcontractors are required to use E–Verify for new hires and existing employees working directly under the contract.

Since fiscal year 2005, the number of E–Verify requests each year has grown from 980,000 to about 16.5 million in fiscal year 2010. Currently, about 254,000 employers (approximately 4 percent of all employers) are registered to use E–Verify at approximately 867,000 worksites.

In a recent report to the Subcommittee (*Federal Agencies Have Taken Steps to Improve E–Verify, but Challenges Remain,* GAO–11–146), the Government Accountability Office found the E–Verify system had made progress in improving accuracy with immediate confirmations rising to 97.4 percent. However, the study also noted the system was still vulnerable to unauthorized workers and unscrupulous employers presenting stolen or borrowed documents for the purpose of identity fraud.

In announcing the hearing, Chairman Sam Johnson (R–TX) stated, **"A broken federal worksite enforcement policy keeps Americans out of a job, leaves workers vulnerable to identity theft, law-abiding employers with uncertainty and unscrupulous employers able to exploit the system. We can and must do better."**

FOCUS OF THE HEARING:

The hearing will focus on the progress made and challenges created by E–Verify, including the potential burdens on employees, employers and the SSA. The Subcommittee will examine how the current shortcomings of the system could be improved to ease the verification process during this critical time of job creation. Finally, the Subcommittee will also review other proposals to expand employment eligibility verification, including enhancing the Social Security card with tamper-proof, counterfeit-resistant or biometric features and increasing enforcement through the sharing of taxpayer wage information.

DETAILS FOR SUBMISSION OF WRITTEN COMMENTS:

Please Note: Any person(s) and/or organization(s) wishing to submit for the hearing record must follow the appropriate link on the hearing page of the Committee website and complete the informational forms. From the Committee homepage, *http://waysandmeans.house.gov*, select "Hearings." Select the hearing for which you would like to submit, and click on the link entitled, "Click here to provide a submission for the record." Once you have followed the online instructions, submit all requested information. ATTACH your submission as a Word or WordPerfect document, in compliance with the formatting requirements listed below, **by the close of business on Thursday, May 5, 2011**. Finally, please note that due to the change in House mail policy, the U.S. Capitol Police will refuse sealed-package deliveries to all House Office Buildings. For questions, or if you encounter technical problems, please call (202) 225–1721 or (202) 225–3625.

FORMATTING REQUIREMENTS:

The Committee relies on electronic submissions for printing the official hearing record. As always, submissions will be included in the record according to the discretion of the Committee. The Committee will not alter the content of your submission, but we reserve the right to format it according to our guidelines. Any submission provided to the Committee by a witness, any supplementary materials submitted for the printed record, and any written comments in response to a request for written comments must conform to the guidelines listed below. Any submission or supplementary item not in compliance with these guidelines will not be printed, but will be maintained in the Committee files for review and use by the Committee.

1. All submissions and supplementary materials must be provided in Word or WordPerfect format and MUST NOT exceed a total of 10 pages, including attachments. Witnesses and submitters are advised that the Committee relies on electronic submissions for printing the official hearing record.

2. Copies of whole documents submitted as exhibit material will not be accepted for printing. Instead, exhibit material should be referenced and quoted or paraphrased. All exhibit material not meeting these specifications will be maintained in the Committee files for review and use by the Committee.

3. All submissions must include a list of all clients, persons and/or organizations on whose behalf the witness appears. A supplemental sheet must accompany each submission listing the name, company, address, telephone, and fax numbers of each witness.

The Committee seeks to make its facilities accessible to persons with disabilities. If you are in need of special accommodations, please call 202–225–1721 or 202–226–

3411 TTD/TTY in advance of the event (four business days notice is requested). Questions with regard to special accommodation needs in general (including availability of Committee materials in alternative formats) may be directed to the Committee as noted above.

Note: All Committee advisories and news releases are available on the World Wide Web at *http://www.waysandmeans.house.gov/*.

Chairman JOHNSON. The subcommittee will come to order. Welcome, everyone.

Employers are on the front lines of ensuring a legal workforce, and it is a battle for these employers. Consider for a moment that due to our broken immigration enforcement system, the Pew Hispanic Center estimates there are over 8 million illegal workers in this country. With unemployment around 9 percent, these illegal workers often compete with lawful citizens for much-needed jobs.

Today's hearing will examine the employment verification systems available for employers' use, including E–Verify, the largely voluntary system jointly administered by Social Security and Homeland Security. Since our last hearing on this subject nearly 3 years ago, the use of E–Verify has expanded. Today there are over 250,000 employers. That is about 4 percent is all of all U.S. employers registered to use the system. In addition, the use of E–Verify has been mandated in three States, and for the Federal Government, and certain Federal contractors and subcontractors.

Social Security is an integral partner in E–Verify because it has the only database that can confirm citizenship. I want to make clear, however, I am very uncomfortable that Homeland Security is checking on U.S. citizens. That said, Social Security and Homeland Security have, to their credit, worked together to make E–Verify more workable and more accurate. However, as we shall hear shortly from the Government Accountability Office, E–Verify remains vulnerable to identity theft and to employer fraud.

As my Texas colleague and chairman of the Judiciary Committee, Lamar Smith, has said, perhaps the most valid criticism of E–Verify is the identity theft loophole. And I couldn't agree more. If an employee presents a stolen Social Security number and fraudulent photo ID, E–Verify will erroneously indicate that the individual is authorized to work. The employer has been duped, and an innocent American may face years of financial and legal woe because his identity has been stolen.

To build on the successes of E–Verify while making needed adjustments to ensure successful implementation, last Congress I introduced H.R. 5515, the New Employee Verification Act, or NEVA. NEVA would achieve three important goals: One, ensure a legal workforce, safeguard workers' identities, and protect Social Security.

It is true that Congress gave the American people an employment verification system that works while protecting Social Security's ability to serve the public. I would hope that this is one immigration-related issue where both sides could find common ground. As we move forward, we must carefully consider the potential burdens to Social Security and, most importantly, to workers and em-

ployers struggling in these trying times to get Americans working again.

I appreciate all of you all being here. I think that we are going to have a good panel today, and I thank you for joining us. So I look forward to hearing our expert testimony from all of you.

Chairman JOHNSON. And I now recognize my friend and the ranking member, Xavier Becerra, for his opening remarks.

Mr. BECERRA. Mr. Chairman, thank you for calling today's hearing to examine the impact of electronic employment verification eligibility verification systems and the impact it has on the Social Security Administration (SSA) and on our workers in the United States.

The Social Security Administration has played a critical role in the verification of our workforce since 1997, when the basic pilot program began, which is now, of course, known as E–Verify. Today the majority of employees who are checked through E–Verify are cleared fairly quickly; however, some workers are not. Our witnesses today will describe what happens to a worker when they receive a tentative nonconfirmation that the information submitted by their employer does not match information contained on government databases.

A recent Government Accountability Office (GAO) report concluded that individuals often face significant difficulties in resolving nonconfirmations. This is not a trivial matter because the inability to resolve an erroneous nonconfirmation can lead to loss of a job.

In addition, I am deeply troubled to learn that many employers do not comply with E–Verify program rules designed to prevent discrimination or abuse of the system. In this downturned economy, one job loss due to mechanical or technical error or employer noncompliance with E–Verify requirements is one job lost too many.

Mr. Chairman, at this time, I would like to submit into the record the stories of Americans who have suffered greatly from problems with E–Verify. These illustrate the kinds of challenges U.S. citizens and legally authorized workers face in keeping their jobs.

Chairman JOHNSON. Without objection.

Mr. BECERRA. Thank you.

Mr. BECERRA. Many would like to expand the E–Verify system, but we should not do so unless we first address the kinds of problems with the existing system that is identified in today's hearing. In addition, to be able to meet the needs of this growing program, more research has to be dedicated to it.

While some have proposed making E–Verify a permanent, mandatory program, the Congressional Budget Office has estimated that this would cost the taxpayers nearly $18 billion over the next 10 years.

As we work forward and make progress in trying to improve this program, the ultimate solution to what we are trying to address through E–Verify is to reform our broken immigration system. In places like Arizona, where E–Verify is mandatory, some employers have resorted to paying their employees under the table or have simply just stopped complying with the program. The State has

also seen a loss of income tax revenue, confirming predictions that mandatory E–Verify in the absence of immigration reform simply drives employees into the underground economy.

Chairman Johnson, I look forward to working together to jointly improve our electronic employment verification system, and I thank you for calling today's hearing.

Chairman JOHNSON. Thank you, sir.

Today we are joined by five witnesses. Our first witness will be Richard Stana, Director of Homeland Security and Justice, United States Government Accountability Office. Next is Marianna LaCanfora, Assistant Deputy Commissioner, Office of Retirement and Disability Policies, Social Security Administration. Next is Tyler Moran, Policy Director, National Immigration Law Center. Next is Ana Antón, Ph.D. professor, Department of Computer Science, College of Engineering, North Carolina State University, on behalf of the Association for Computing Machinery. And finally, Austin Fragomen, Chairman of the Board of Directors of the American Council on International Personnel, on behalf of the HR Initiative for a Legal Workforce.

I welcome all of you, and we look forward to hearing your testimony. Each witness will have 5 minutes, and your written statements will be made part of the record in the event that you run over a little. So I thank you, and I welcome you.

And thank you, Mr. Stana. You are recognized for 5 minutes.

STATEMENT OF RICHARD M. STANA, DIRECTOR, HOMELAND SECURITY AND JUSTICE, UNITED STATES GOVERNMENT ACCOUNTABILITY OFFICE

Mr. STANA. Thank you, Mr. Chairman. Thank you, Mr. Becerra and Members of the Subcommittee. I am pleased to be here today to discuss the results of our work on E–Verify, which is a voluntary program that can be used to verify the work authorization of newly hired employees.

I would like to discuss three points from our report, and then later I would like to briefly discuss some issues that may be of interest to the subcommittee on how it would affect the Social Security Administration.

First let us discuss the TNCs, the tentative nonconfirmations. The USCIS has substantially reduced the number of TNCs from about 8 percent of all queries just a few years ago to 2.6 percent in fiscal year 2009, which was the subject of our study, down to 1.7 percent last year. So that is moving in the right direction. This was done by expanding the number of databases that are queried. They now look at naturalization databases, and they look at passport data. USCIS also screens for common data entry errors like transpositions or a European date format that can be easily fixed. But erroneous TNCs continue to occur when employee names are misspelled, or they are transposed, or people with multiple surnames use different surnames in one document than they use in another document, and thus it triggers a TNC.

Erroneous final nonconfirmations can occur when SSA field office staff do not update the EV–STAR system, which is an information system on workers who receive SSA TNCs, but SSA is addressing this issue, so we hope that this will be resolved soon.

Mr. BECERRA. Mr. Stana, we ask that you, instead of using the acronyms, mention the names of these programs, because a lot of folks who might be watching may not understand what a TNC and all those other things are.

Mr. STANA. Okay. Thank you.

An FNC is a final nonconfirmation, which is the final notice that you are not confirmed. It is not redressable. In other words, there is no appeal mechanism for that, which may get to the issue you both were talking about with Americans who are work-authorized but get a bad shake out of the system.

So improving government data sets, increasing employee awareness, and making sure employees have a sufficient amount of time to redress the TNC notices is really what is needed here.

Now, I would like to turn briefly to the issue of identity theft that both of you have mentioned. This is a very important issue, and it is one that the system has not been able to address. Identity theft can occur if I were not work-authorized and would use another person's identity to say that my Social Security number is this, and my driver's license number is this, and the E–Verify system says I am work-authorized when I am really not.

Westat did a study on E–Verify a couple of years ago. They found that about 3 percent of the confirmed work-authorized people really aren't. In other words, it creates a false positive. And sometimes this is done by individual workers getting an identity that works. Sometimes it is done with the complicity of the employer; the employer says these documents are valid, let us enter these into the E–Verify system, and we will put you on our payroll.

USCIS has taken a number of steps to try to address this, like a photo-matching tool for 3 of the 26 documents you can use to validate your authorization to work in the United States. But again, this whole system hinges on the integrity of the employer. The employer looks at the photo on the screen, looks at the photo that you present, or looks at the person who is before them and either says it is or it is not a match. So that is an issue that they have to work on a little bit more, finding a key to unlocking the identity theft issue.

Turning to some of the discrimination issues, there is concern that people who have hyphenated names may get a bad shake out of the system, or people who have hyphenated names may encounter certain challenges that those of us who don't do not. They may order their names in a certain sequence differently on different documents. It is not against the law to do that, but it is going to trigger a tentative nonconfirmation.

USCIS has a monitoring and compliance unit that they use to try to identify discriminatory behaviors among employees, such as seeing if a person is not given work assignments or reduced pay until a final confirmation comes through. This is against the law. But again, with about 80 people across the country in this unitand no on-site inspection—I take that back. There was one at the Social Security Administration—it is difficult to determine whether discriminating behavior exists.

My last point from our report involves resources. Like the I–9 system, unless the E–Verify system is properly resourced, it is not likely to work well. This is because you have to have someone on

site to make sure that the system is properly used and, to the extent possible, to make sure that identity theft is minimized or eliminated. USCIS has to rely on ICE for investigating, sanctioning and seeking prosecution of noncompliant employers, but given its priorities, ICE is not likely to devote many resources to this area. So policy decisions are going to have to be made on how many resources the Congress wishes ICE to put into worksite enforcement.

Lastly, I'd like to discuss E–Verify's impacts on SSA. First, to the extent that SSA staff needs to resolve tentative nonconfirmations, it does take time away from other duties. When the TNC rate goes down from 8 to 1.7 percent, that is helpful. If we go to a mandatory system, we may need more resources so it does not adversely impact the SSA workload.

The other thing that could impact the SSA workload is the self-check system, where an employee or potential employee like you or me could query a system to see if the system would identify us as work-authorized. It is new. It is being piloted. While the pilot is ongoing, it doesn't now seem to be stressing the SSA workload too much. If it becomes mandatory, or if the pilot is expanded nationwide, it could have an effect. But I will let the Social Security Administration discuss ant adverse impact.

That concludes my statement. I will be happy to answer any questions.

Chairman JOHNSON. Thank you, sir.

[The prepared statement of Mr. Stana follows:]

United States Government Accountability Office

GAO

Testimony

Before the Subcommittee on Social Security, Committee on Ways and Means, House of Representatives

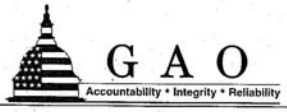
For Release on Delivery
Expected at 2 p.m. EDT
Thursday, April 14, 2011

EMPLOYMENT VERIFICATION

Agencies Have Improved E-Verify, but Significant Challenges Remain

Statement of Richard M. Stana, Director
Homeland Security and Justice

This testimony is embargoed until April 14th at 2:00 p.m.



GAO-11-522T

Chairman Johnson, Ranking Member Becerra, and Members of the Subcommittee:

I am pleased to be here to discuss the E-Verify program, which provides employers a tool for verifying an employee's authorization to work in the United States. The opportunity for employment is one of the most powerful magnets attracting immigrants to the United States. According to the Pew Hispanic Center, as of March 2010, approximately 11.2 million unauthorized immigrants were living in the country, and an estimated 8 million of them, or about 70 percent, were in the labor force. Congress, the administration, and some states have taken various actions to better ensure that those who work here have appropriate work authorization and to safeguard jobs for authorized employees. Nonetheless, opportunities remain for unauthorized workers to fraudulently obtain employment by using borrowed or stolen documents and for unscrupulous employers to hire unauthorized workers. Immigration experts have noted that deterring illegal immigration requires, among other things, a more reliable employment eligibility verification process and a more robust worksite enforcement capacity.

E-Verify is a free, largely voluntary, Internet-based system operated by the Verification Division of the Department of Homeland Security's U.S. Citizenship and Immigration Services (USCIS) and the Social Security Administration (SSA). The goals of E-Verify are to (1) reduce the employment of individuals unauthorized to work, (2) reduce discrimination, (3) protect employee civil liberties and privacy, and (4) prevent undue burden on employers. Pursuant to a 2007 Office of Management Budget directive, all federal agencies are required to use E-Verify on their new hires and, as of September 2009, certain federal contractors and subcontractors are required to use E-Verify for newly hired employees working in the United States as well as existing employees working directly under the contract. A number of states have also mandated that some or all employers within the state use E-Verify on new hires. From October 1, 2010, through April 5, 2011, E-Verify processed approximately 7.8 million queries from nearly 258,000 employers.

In an August 2005 report and June 2008 testimony on E-Verify, we noted that USCIS faced challenges in detecting identity fraud and ensuring

employer compliance with the program's rules.[1] We highlighted some of the challenges USCIS and SSA faced in reducing instances of erroneous tentative nonconfirmations (TNC), or situations in which work-authorized employees are not automatically confirmed by E-Verify.[2] We also noted that mandatory implementation of E-Verify would place increased demands on USCIS's and SSA's resources. My comments today are based primarily on a report we issued in December 2010 and provide updates to the challenges we noted in our 2005 report and 2008 testimony.[3] My statement, as requested, highlights findings from that report and discusses the extent to which (1) USCIS has reduced the incidence of TNCs and E-Verify's vulnerability to fraud, (2) USCIS has provided safeguards for employees' personal information, and (3) USCIS and SSA have taken steps to prepare for mandatory E-Verify implementation. Our December 2010 report also includes a discussion of the extent to which USCIS has improved its ability to monitor and ensure employer compliance with E-Verify program policies and procedures.

For our report, we analyzed data on the results of E-Verify cases for fiscal year 2009 and interviewed senior E-Verify program officials about their procedures for ensuring quality in the E-Verify transaction database. We determined that the data were sufficiently reliable for the purposes of our report. We reviewed documentation explaining how to resolve TNCs and assist employees with name and citizenship changes. We reviewed USCIS's privacy policy for E-Verify and conducted interviews with privacy officials at USCIS to determine what, if any, challenges exist in resolving TNCs. We assessed USCIS's and SSA's life-cycle cost estimates and SSA's workload estimates, and compared them to characteristics of a reliable cost estimate as defined in GAO's Cost Estimating and Assessment Guide.[4] We selected

[1] GAO, *Immigration Enforcement: Weaknesses Hinder Employment Verification and Worksite Enforcement Efforts*, GAO-05-813 (Washington, D.C.: Aug. 31, 2005) and GAO, *Employment Verification: Challenges Exist in Implementing a Mandatory Electronic Employment Verification System*, GAO-08-895T (Washington, D.C.: June 10, 2008).

[2] We collectively refer to these situations—as well as those in which (1) employers inadvertently make errors in data entry when making E-Verify queries, (2) employees provide inconsistent personal information to government agencies, and (3) government databases contain errors unrelated to an employer's or employee's action—as erroneous TNCs.

[3] GAO, *Employment Verification: Federal Agencies Have Taken Steps to Improve E-Verify, but Significant Challenges Remain*, GAO-11-146 (Washington, D.C.: Dec. 17, 2010).

[4] GAO, *GAO Cost Estimating and Assessment Guide: Best Practices for Developing and Managing Capital Program Costs*, GAO-09-3SP (Washington, D.C.: March 2009), 8-13.

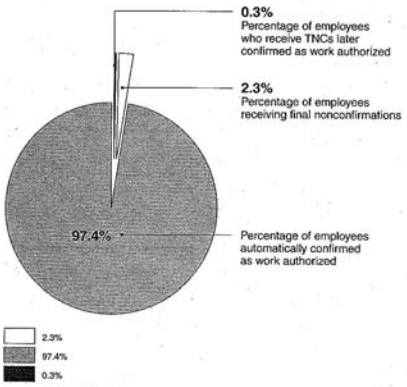
three states for site visits—Colorado, North Carolina, and Arizona—based on, among other reasons, the length of time each state's E-Verify law had been in effect. While the views provided are not generalizable, they provided us with additional perspectives on the benefits and challenges associated with the E-Verify program. More detailed information on our scope and methodology is contained in our December 2010 report. We conducted this work in accordance with generally accepted government auditing standards.

USCIS and SSA Have Reduced TNCs, but the Accuracy of E-Verify Continues to Be Limited by Both Inconsistent Recording of Employees' Names and Fraud

USCIS has reduced TNCs from about 8 percent for the period June 2004 through March 2007 to about 2.6 percent in fiscal year 2009.[5] As shown in figure 1, in fiscal year 2009, about 2.6 percent or over 211,000 of newly hired employees received either a SSA or USCIS TNC, including about 0.3 percent who were determined to be work eligible after they contested a TNC and resolved errors or inaccuracies in their records, and about 2.3 percent, or about 189,000, who received a final nonconfirmation because their employment eligibility status remained unresolved. For the approximately 2.3 percent who received a final nonconfirmation, USCIS was unable to determine how many of these employees (1) were authorized employees who did not take action to resolve a TNC because they were not informed by their employers of their right to contest the TNC, (2) independently decided not to contest the TNC, or (3) were not eligible to work.

[5] Since our December 2010 report, USCIS reported that it has further reduced the TNC rate from about 2.6 percent in fiscal year 2009 to about 1.7 percent in fiscal year 2010.

Figure 1: E-Verify Results for Fiscal Year 2009



Source: GAO analysis of DHS data.

USCIS has reduced TNCs and increased E-Verify accuracy by, among other things, expanding the number of databases that E-Verify can query and instituting quality control procedures to screen for data entry errors. However, erroneous TNCs continue to occur, in part, because of inaccuracies and inconsistencies in how personal information is recorded on employee documents, in government databases, or both. Some actions have been taken to address name-related TNCs, but more could be done. Specifically, USCIS could better position employees to avoid an erroneous TNC by disseminating information to employees on the importance of providing consistent name information and how to record their names consistently. In our December 2010 report, we recommended that USCIS disseminate information to employees on the potential for name mismatches to result in erroneous TNCs and how to record their names consistently. USCIS concurred with our recommendation and outlined

actions to address it. For example, USCIS commented that in November 2010 it began to distribute the U.S. Citizenship Welcome Packet at all naturalization ceremonies to advise new citizens to update their records with SSA. USCIS also commented that it has commissioned a study, to be completed in the third quarter of fiscal year 2011, to determine how to enhance its name-matching algorithms. USCIS's actions for reducing the likelihood of name-related erroneous TNCs are useful steps, but they do not fully address the intent of the recommendation because they do not provide specific information to employees on how to prevent a name-related TNC. See our December 2010 report for more details.

In addition, identity fraud remains a challenge because employers may not be able to determine if employees are presenting genuine identity and employment eligibility documents that are borrowed or stolen.[6] E-Verify also cannot detect cases in which an unscrupulous employer assists unauthorized employees. USCIS has taken actions to address fraud, most notably with the fiscal year 2007 implementation of the photo matching tool for permanent residency cards and employment authorization documents and the September 2010 addition to the matching tool of passport photographs. Although the photo tool has some limitations, it can help reduce some fraud associated with the use of genuine documents in which the original photograph is substituted for another.[7] To help combat identity fraud, USCIS is also seeking to obtain driver's license data from states and planning to develop a program that would allow victims of identity theft to "lock" their Social Security numbers within E-Verify until they need them to obtain employment authorization.[8] Combating identity fraud through the use of biometrics, such as through fingerprint or facial

[6] GAO has previously reported on the risks associated with the use of fraudulent documents and agencies' actions to address them. See GAO, *Border Security: Better Usage of Electronic Passport Security Features Could Improve Fraud Detection*, GAO-10-96 (Washington, D.C.: Jan. 22, 2010), and *State Department: Undercover Tests Show Passport Issuance Process Remains Vulnerable to Fraud*, GAO-10-922T (Washington, D.C.: July 29, 2010).

[7] According to USCIS, from October 2009 to August 2010, there were 393,574 cases that initiated E-Verify's photo matching tool. Of these cases, employers indicated that 1,569 employees' photos did not match, with one case resulting in a contested TNC. USCIS told us that it is unable to determine what percentage of the remaining 1,568 cases involved identity fraud because they do not have additional information on those cases.

[8] According to USCIS, a locked Social Security number would halt any attempt by participating E-Verify employers to verify an employee's Social Security number through E-Verify if the employee notifies USCIS that his or her identity has been stolen and can provide supporting documentation to USCIS.

recognition, has been included in proposed legislation before Congress as an element of comprehensive immigration reform, but implementing a biometric system has its own set of challenges, including those associated with cost and civil liberties. Resolving these issues will be important if this technology is to be effectively implemented in combating identity fraud in the employment verification process.

An effective employment authorization system requires a credible worksite enforcement program to ensure employer compliance with applicable immigration laws; however, USCIS is challenged in ensuring employer compliance with E-Verify requirements for several reasons. For example, USCIS cannot monitor the extent to which employers follow program rules because USCIS does not have a presence in employers' workplaces.[9] USCIS is further limited by its existing technology infrastructure, which provides limited ability to analyze patterns and trends in the data that could be indicative of employer misuse of E-Verify. USCIS has minimal avenue for recourse if employers do not respond or remedy noncompliant behavior after a contact from USCIS compliance staff because it has limited authority to investigate employer misuse and no authority to impose penalties against such employers, other than terminating those who knowingly use the voluntary system for an unauthorized purpose. For enforcement action for violations of immigration laws, USCIS relies on U.S. Immigration and Customs Enforcement (ICE) to investigate, sanction, and prosecute employers. However, ICE has reported that it has limited resources to investigate and sanction employers that knowingly hire unauthorized workers or those that knowingly violate E-Verify program rules.[10] Instead, according to senior ICE officials, ICE agents seek to maximize limited resources by applying risk assessment principles to worksite enforcement cases and focusing on detecting and removing unauthorized workers from critical infrastructure sites.

[9] Senior E-Verify program officials said they expect improved technology enabling automated analysis of E-Verify data to be implemented by fiscal year 2012.

[10] In fiscal year, 2010 ICE spent about 600,000 agent-reported workload hours on worksite enforcement, issued 237 fines as the result of worksite audits, and made 196 criminal and 1,224 administrative worksite enforcement arrests. For the first two quarters of fiscal year 2011, ICE reported that the agency spent about 333,000 agent-reported workload hours on worksite enforcement, issued 171 fines as the result of worksite audits, and made 105 criminal and 745 administrative worksite enforcement arrests.

DHS Has Instituted Employee Privacy Protections for E-Verify, but Resolving Erroneous TNCs Can Be Challenging

USCIS has taken actions to institute safeguards for the privacy of personal information for employees who are processed through E-Verify, but has not established mechanisms for employees to identify and access personal information maintained by DHS that may lead to an erroneous TNC, or for E-Verify staff to correct such information. To safeguard the privacy of personal information for employees who are processed through E-Verify, USCIS has addressed the Fair Information Practice Principles, which are the basis for DHS's privacy policy.[11] For example, USCIS published privacy notices in 2009 and 2010 that defined parameters, including setting limits on DHS's collection and use of personal information for the E-Verify program.

Notwithstanding the efforts made by USCIS to address privacy concerns, employees are limited in their ability to identify and access personal information maintained by DHS that may lead to an erroneous TNC.[12] In our December 2010 report, we recommended that USCIS develop procedures to enable employees to access personal information and correct inaccuracies or inconsistencies in such information within DHS databases. USCIS concurred and identified steps that it is taking to address this issue, such as developing a pilot program to assist employees receiving TNCs to request a records update and referring individuals who receive a TNC to local USCIS or U.S. Customs and Border Protection offices and ports of entry to correct records when inconsistent or inaccurate information is identified. In part to address this recommendation, in March 2011, USCIS began implementing a Self-Check program to allow individuals to check their own work authorization status

[11] The Fair Information Practice Principles adopted by DHS are a revision of principles, called the Fair Information Practices, first proposed by a U.S. government advisory committee. See Department of Health, Education, and Welfare, *Records, Computers and the Rights of Citizens: Report of the Secretary's Advisory Committee on Automated Personal Data Systems* (July 1973). These principles include Transparency, Individual Participation, Purpose Specification, Data Minimization, Use Limitation, Data Quality and Integrity, Security, and Accountability and Auditing.

[12] If an employee chooses to contest a TNC, the employer is required to provide the employee a referral letter that identifies which agency an employee needs to visit or call to resolve the TNC and close the case.

against SSA and DHS databases prior to applying for a job.[13] We recognize that these efforts may be a step in the right direction, but they do not fully respond to our recommendation. This is because, among other things, USCIS does not have operating procedures in place for USCIS staff to explain to employees what personal information produced the TNC or what specific steps they should take to correct the information. We encourage USCIS to continue its efforts to develop procedures enabling employees to access and correct inaccurate and inconsistent personal information in DHS databases.

USCIS and SSA Have Taken Actions to Prepare for Mandatory Implementation of E-Verify, but Face Challenges in Estimating Costs

USCIS and SSA have taken actions to prepare for possible mandatory implementation of E-Verify for all employers nationwide by addressing key practices for effectively managing E-Verify system capacity and availability and coordinating with each other in operating E-Verify. However, USCIS and SSA face challenges in accurately estimating E-Verify costs. Our analysis showed that USCIS's E-Verify estimates partially met three of four characteristics of a reliable cost estimate and minimally met one characteristic.[14] As a result, we found that USCIS is at increased risk of not making informed investment decisions, understanding system affordability, and developing justifiable budget requests for future E-Verify use and potential mandatory implementation of it. To ensure that USCIS has a sound basis for making decisions about resource investments for E-Verify and securing sufficient resources, in our December 2010 report, we recommended that the Director of USCIS ensure that a life-cycle cost estimate for E-Verify is developed in a manner that reflects the four characteristics of a reliable estimate consistent with best practices. USCIS concurred and senior program officials told us that USCIS, among other things, has contracted with a federally funded research and development

[13]The Self-Check program allows users to check their work authorization status by entering information into an online portal. The Self-Check program checks users' information against relevant SSA and DHS databases and returns information on users' employment eligibility status. USCIS is releasing the E-Verify Self-Check service in phases, and plans to expand Self-Check's availability nationwide within 12 months. Self-Check service is currently offered to users that maintain an address in Arizona, Colorado, the District of Columbia, Idaho, Mississippi, or Virginia. We have not assessed the privacy implications associated with the Self-Check program.

[14] Our research has determined that a reliable cost estimate should include four characteristics. Specifically, the estimate should be comprehensive, well-documented, accurate, and credible. GAO, *GAO Cost Estimating and Assessment Guide: Best Practices for Developing and Managing Capital Program Costs*, GAO-09-3SP (Washington, D.C.: March 2009), 8-13.

center to develop an independent cost estimate of the life-cycle costs of E-Verify to better comply with our cost-estimating guidance.

Our analysis showed that SSA's E-Verify estimates substantially met three of four characteristics of a reliable cost estimate. However, we found that SSA's cost estimates are partially credible because SSA may not be able to provide assurance to USCIS that it can provide the required level of support for E-Verify operations if it experiences cost overruns within any one fiscal year.[15] In our December 2010 report, we recommended that the Commissioner of SSA assess the risk around SSA's E-Verify workload estimate, in accordance with best practices, to ensure that SSA can accurately project costs associated with its E-Verify workload and provide the required level of support to USCIS and E-Verify operations. SSA did not concur, and stated that it assesses the risk around its workload cost estimates and, if E-Verify were to become mandatory, SSA would adapt its budget models and recalculate estimated costs based on the new projected E-Verify workload volume. As discussed in our December 2010 report, however, SSA does not conduct a risk and uncertainty analysis that uses statistical models to quantitatively determine the extent of variability around its cost estimate or identify the limitations associated with the assumptions used to create the estimate. Thus, we continue to believe that SSA should adopt this best practice for estimating risks to help it reduce the potential for experiencing cost overruns for E-Verify.

Chairman Johnson, Ranking Member Becerra, and Members of the Subcommittee, this concludes my prepared statement. I will be pleased to respond to any questions you may have.

GAO Contacts and Staff Acknowledgments

For further information regarding this testimony, please contact Richard M. Stana at (202) 512-8777 or stanar@gao.gov. In addition, contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this statement. Individuals who made key contributions

[15] Pursuant to a reimbursable agreement, at the beginning of each fiscal year, USCIS pays SSA the costs for maintaining its system operations, as well as the projected costs for assisting employees with resolving TNCs. At the end of each fiscal year, SSA and USCIS reconcile any differences between actual costs and estimates, and SSA is to return any unspent funds to USCIS. USCIS provides SSA estimates of anticipated transaction volumes to help SSA estimate its future costs for operating E-Verify. In fiscal year 2010, USCIS reimbursed SSA approximately $7.8 million for operating E-Verify.

to this testimony are Evi Rezmovic, Assistant Director; Sara Margraf; and Michelle Woods. Additionally, key contributors to our December 2010 report include Blake Ainsworth, David Alexander, Tonia Brown, Frances Cook, Marisol Cruz, John de Ferrari, Julian King, Danielle Pakdaman, David Plocher, Karen Richey, Robert Robinson, Douglas Sloane, Stacey Steele, Desiree Cunningham, Vanessa Taylor, Teresa Tucker, and Ashley Vaughan.

Chairman JOHNSON. Ms. LaCanfora, you are recognized for 5 minutes.

STATEMENT OF MARIANNA LACANFORA, ASSISTANT DEPUTY COMMISSIONER, OFFICE OF RETIREMENT AND DISABILITY POLICY, SOCIAL SECURITY ADMINISTRATION

Ms. LACANFORA. Thank you. Chairman Johnson, Ranking Member Becerra and Members of the Subcommittee, thank you for the opportunity to discuss SSA's supporting role in E–Verify, DHS's electronic employment eligibility verification system. I would like to

start by briefly describing the purpose of our Social Security numbers, or SSNs.

Assigning SSNs is key to administering Social Security programs. We establish the SSN as a way for employers to report an employee's earnings accurately. We use the SSN to credit wages to the earnings record that we maintain for each worker. The earnings record is the basis for determining eligibility for, and the amount of, Social Security benefits.

The SSN also plays a key role in E–Verify. By law, all employers are required to verify the identity and employment eligibility of new employees. E–Verify is a voluntary, electronic tool that employers can use to comply with the law. When an employer submits information about a new hire, DHS sends this information to us electronically to verify the SSN, the name and the date of birth in our records. For new hires alleging U.S. citizenship, we also confirm citizenship based on the information that we have in our records. For any naturalized citizen whose U.S. citizenship we cannot confirm using our records, DHS verifies naturalization and thus the authorization to work. For noncitizens, if there is a match with our records, DHS will then determine the current work authorization status. DHS notifies the employer of the results of these verifications.

So far this fiscal year, we have handled about 7.5 million queries. In fiscal year 2010, E–Verify handled over 16.5 million queries and automatically confirmed work authorization in about 98 percent of these queries instantly or within 24 hours. The remaining 2 percent received an initial systems mismatch. We call that a tentative nonconfirmation. Of that 2 percent, just under half contacted us at Social Security to resolve the mismatch.

When an individual comes into one of our offices with a tentative nonconfirmation, we work to resolve the discrepancy. For example, the person may need to change their name in our records due to a marriage or a divorce that they had not previously reported to us.

It is important to note that we need to verify the identity of any individual whose record we update. That is why we must process almost all of these updates during face-to-face interviews in our local offices. In some cases we may be unable to resolve the discrepancy the same day because the individual may need to obtain evidence, such as a marriage certificate.

We use EV–STAR, which is a Web-based portal, to update the E–Verify system with the status of a pending case. Once we resolve the discrepancy by updating our records, or by determining that our records should not be changed, we again update EV–STAR to show the outcome of the case. The employer can check E–Verify for the status of the case and see the final confirmation or nonconfirmation.

We have worked with the DHS over the last few years to improve the E–Verify system. For example, in 2009, we completed a significant improvement to our computer systems that support E–Verify. This improved system ensures that there is no interference between our mission-critical workloads and DHS's E–Verify program. At the request of DHS, we designed the system to handle up to 60 million queries per year. With additional hardware and fund-

ing, we could increase our capacity if the need arises. Even with this and other improvements we remain focused on further reducing the need for workers to visit our local offices.

Each year DHS provides funds to cover our E–Verify-related costs. Our costs include systems maintenance costs and the cost of assisting individuals to resolve the tentative nonconfirmations. Receiving timely and adequate reimbursement from DHS for E–Verify is critical.

In conclusion, I thank you for giving me this opportunity to discuss our role in assisting DHS to administer the E–Verify system. I would be happy to answer any questions you may have.

Chairman JOHNSON. Thank you, ma'am.

[The prepared statement of Ms. LaCanfora follows:]

HEARING BEFORE
COMMITTEE ON WAYS AND MEANS
SUBCOMMITTEE ON SOCIAL SECURITY
UNITED STATES HOUSE OF REPRESENTATIVES

SOCIAL SECURITY ADMINISTRATION'S ROLE IN VERIFYING EMPLOYMENT ELIGIBILITY

APRIL 14, 2011

STATEMENT OF
MARIANNA LACANFORA
ASSISTANT DEPUTY COMMISSIONER
OFFICE OF RETIREMENT AND DISABILITY POLICY

Mr. Chairman and Members of the Subcommittee:

Thank you for inviting me to participate in these important oversight hearings concerning Social Security. Yesterday we told you about issues that relate to enumeration and identity theft. Today I will discuss our role in helping the Department of Homeland Security (DHS) administer its E-Verify system, which supports the employer community in the 21st century.

Our Mission and Ensuring the Accuracy of Our Records

For over 75 years, America has depended on Social Security. Our programs benefit workers, their dependents, and survivors at critical junctures in their lives: when they retire, when they become disabled, and after losing a loved one. Each month, we send about $60 billion in benefits to approximately 60 million beneficiaries.

Assigning Social Security numbers (SSNs) and issuing Social Security cards has always been one of our core workloads. We have assigned about 465 million SSNs since the inception of the program.

The SSN is a record-keeping tool that allows employers to uniquely identify and accurately report a worker's earnings. Names alone cannot ensure accurate reporting, but the combination of a name and an SSN provides a system for accurately reporting and recording wage information.

While the SSN has a very limited purpose, the role of the card is even narrower. It is simply a record of the number assigned to the worker so that he or she can provide the correct number to an employer, as well as potentially to show if the individual is permitted to work. The card was never intended, and should not serve, as a personal identification document.

Relationship Between the SSN and Determinations of Work Authorization

The primary purpose of the SSN is to allow us to properly credit a worker's earnings, which we use to determine potential eligibility for and the amount of benefit payments. However, the Social Security card in conjunction with an identity document may be used to determine whether a person is authorized to work. The Immigration Reform and Control Act of 1986 (IRCA) made it illegal for an employer to knowingly hire anyone not legally permitted to work in the United States. Under IRCA, all employers are required to verify the identity and employment eligibility of all new employees regardless of citizenship or national origin. IRCA and DHS regulations specify a number of documents that

may be used for this purpose. Some documents, such as a United States passport, establish both employment eligibility and identity. Others, such as a Social Security card may establish employment eligibility, but the Social Security card does not establish identity. If the employee provides a document that establishes employment eligibility only, he or she must also provide an identification document, such as a State driver's license.

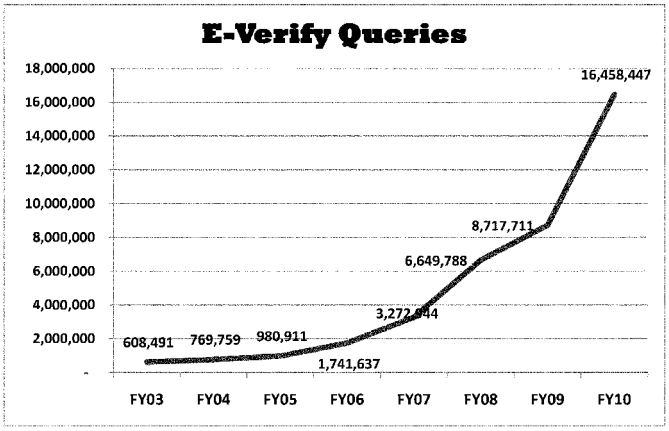
History of the Current Employment Eligibility Verification System

E-Verify is a fast, free, Internet-based system that allows employers to electronically verify the employment eligibility of new hires. E-Verify is also required for certain Federal contractors and subcontractors. The support we provide to DHS for E-Verify is not related to the benefit programs we administer; therefore, DHS reimburses us for all costs we incur in support of its program.

In 1996, Congress enacted the Illegal Immigration Reform and Immigrant Responsibility Act (IIRIRA), which required the former Immigration and Naturalization Service (INS) and SSA to test a method of providing an effective, nondiscriminatory employment eligibility confirmation process. Consistent with the law, INS and SSA implemented E-Verify (originally known as the Basic Pilot) in five of the seven States with the highest estimated population of noncitizens who were not lawfully present in the United States: California, Florida, Illinois, New York, and Texas.

In March 1999, INS added Nebraska to assist employers in the meat packing industry. Employers in these six states were also allowed to use the system to verify the employment eligibility of new hires at their work sites located in other States. In 2001, Congress extended authorization for the program for an additional 2 years. In 2003, Congress extended the program for another 5 years and expanded its availability to employers in all 50 States. Congress has since extended E-Verify through September 2012.

Employer use of E-Verify has grown in recent years because DHS has increased outreach and education efforts and two States mandate employer use of the program. Before the nationwide expansion, less than 3,000 employers participated. Currently, DHS has about 256,000 employers registered to use E-Verify at approximately 870,000 worksites. As the number of participating employers has grown, so has the number of queries we handle as shown in the chart below. For the first 6 months of this fiscal year, we have handled about 7.5 million queries.



The E-Verify Process

Participating employers register with DHS to use the E-Verify system to verify a newly hired employee's SSN and work authorization status. The employer inputs information from the new hire's Form I-9, the Employment Eligibility Verification Form, into the web-based system. DHS then electronically sends us this information to verify that the newly hired employee's SSN, name, and date of birth match the information in our records. For employees alleging United States citizenship, we also confirm citizenship status as recorded in our records, thereby allowing DHS to confirm work authorization. For any naturalized citizen whose United States citizenship we cannot confirm, DHS will verify naturalization and, thus, authorization to work. For all noncitizens, if there is a match with our records, DHS determines current work authorization status.

Once DHS makes a determination, DHS notifies employers whether the new hire is authorized to work. E-Verify confirms work authorization for approximately 98 percent of these initial verification requests within 24 hours, often within seconds. For the minority of cases when the SSA record does not match the data submitted by the employer, E-Verify notifies the employer that the new hire has received an SSA tentative nonconfirmation—that is, that the new hire must take additional steps to be verified to work under the system.

The employer must then notify the employee of the tentative non-confirmation and provide an opportunity for the employee to contest the finding. If the employee receives an SSA tentative nonconfirmation, the employee has 8 Federal workdays to visit one of our local offices to present required documentation to update or correct our records (for example, proof of age or citizenship/noncitizen status). In some situations, we must verify the documentation with the issuing agency before we can update the new hire's record.

It is important to note that, as part of the process to correct our records, we need to verify the identity of the individual whose records we are updating. That is why we process almost all of these updates during a face-to-face interview in our field offices.

Once we update our records, we input the status of the case to the E-Verify SSA Tentative Non-confirmation Automated Response system (EV-STAR), a web-based portal our employees access directly which, in turn, updates the E-Verify system. The employer can then check E-Verify to determine the status of the case and, once the case has been resolved, see the final confirmation or non-confirmation.

E-Verify Enhancements

Since the inception of E-Verify, we have worked collaboratively with DHS to make the system more efficient and easier to use. I would like to highlight a few of the most significant improvements.

In 2007 and 2008, we worked with DHS to make several changes that reduced the number of new hires receiving a tentative non-confirmation. In September 2007, DHS modified the front-end of the E-Verify system to do a "pre-tentative non-confirmation check." This pre-check verifies the data entered into the system, and if any information does not match, asks employers to double check the data. The pre-check acts as a fail-safe against employer keying errors or misreading of the information on the DHS Form I-9.

In May 2008, DHS updated the E-Verify system to include naturalization data. Experience with E-Verify had shown that many naturalized citizens had not reported their citizenship changes to us and therefore were more likely to receive a tentative non-confirmation. By including DHS naturalization data in the initial electronic verification process, naturalized citizens are now likely to be automatically confirmed through E-Verify.

At the same time, DHS also changed the process for contesting tentative non-confirmations based on citizenship mismatches. Under this process, naturalized citizens who receive a tentative non-confirmation can call DHS directly to resolve the issue. While new hires still have the option of resolving the mismatch in person at one of our field offices, this new process provides better, more convenient service to the public and helps reduce the number of visitors coming to our field offices to change their records.

In 2009, we completed a major improvement to our systems that support E-Verify. We isolated E-Verify workloads from our mission critical workloads. No other workloads run in this isolated E-Verify environment; therefore, use of the E-Verify system does not affect our mission critical workloads, and increases in our mission critical workloads do not affect the operation of E-Verify.

The more robust design of this system increases our capacity to handle E-Verify queries. At DHS' request, we designed the system to accommodate 60 million queries a year because United States employers hire about 60 million workers each year. In time, we may need additional capacity, but we expect our systems will be able to handle potential expansions, provided we receive necessary resources and lead times. This systems environment will help us provide prompt, efficient, and accurate service to those seeking employment.

We continue to make improvements to support the E-Verify program. This month, we are adding enhancements to our computer systems to help us identify individuals who are visiting our field offices due to an E-Verify tentative non-confirmation. This new functionality will help us better serve the public by ensuring that our employees update EV-STAR, and thus E-Verify, with the most current case information. These enhancements demonstrate our continued commitment to help DHS improve E-Verify.

DHS recently launched its E-Verify Self Check tool. This Self Check tool allows a worker to check his or her own employment authorization status and resolve discrepancies before seeking employment. As of March 21, 2011, E-Verify Self Check is available to users who maintain an address and are physically located in Arizona, Idaho, Colorado, Mississippi, Virginia, or the District of Columbia. We worked collaboratively with DHS during its development and implementation of the E-Verify Self Check service, and we expect that DHS will reimburse us for any work that our field offices must handle because of this new service. We will continue to work with DHS as it expands availability of the tool nationwide.

SSA E-Verify Workloads

Over the last 10 years, E-Verify evolved from a small pilot program to a program available to employers nationwide, and its usage has dramatically increased. We respond to every query run through the system, and we are the primary point of contact for new hires contesting a tentative non-confirmation.

In almost every situation, we must conduct a face-to-face interview to verify that new hires contesting tentative non-confirmations are who they say they are. During the interview, the new hire must present documentation to support his or her request for an update or correction to our master file of SSNs, or Numident. It takes about 20 minutes to complete each face-to-face interview and to update the EV-STAR system and the Numident when a person requests a change to his or her record.

Sometimes the new hire may not have the documentation required to support a change in our records, and he or she must request the document from the custodian of record or issuing agency. These record requests can add weeks to the process. For example, a new hire may not have an original or a certified copy of his or her marriage certificate and may need to obtain the original. In other cases, a new hire has the document, but we must verify its authenticity with the custodian of the record. Thus, in complex cases, changing a Numident record may require multiple visits to one of our field offices.

This process is critical to the integrity of our records and of E-Verify, hut can be inconvenient for new hires who are trying to change their records and create additional work for our field offices. For example, in FY 2007, for every 100 E-Verify queries, we handled about 2.6 contacts. In FY 2008, that number went down to about 1.5 contacts per 100 queries. Currently, we estimate that we will handle about 0.8 contacts for every 100 queries.

We will continue to work with DHS to assess our policies and procedures to identify ways to better serve the public and reduce the number of new hires who visit our field offices to resolve tentative non-confirmations.

Funding For E-Verify

DHS reimburses SSA for all operating costs related to the E-Verify system, including our systems maintenance costs and the costs of assisting new hires who visit our field offices and call our teleservice centers to contest a tentative non-confirmation.

We understand that there are several proposals to extend and expand the E-Verify program. However, we will be able to successfully support an expansion of the program only if we are fully reimbursed for our E-Verify costs. SSA would need sufficient resources, time, and a multi-year phased-in approach to prepare for any additional work caused by expansion of the program. While our systems environment can handle substantially increased volumes of queries if necessary, we may need to add additional capacity should the program be mandatory for all current employees as well as new hires.

Importance of Relationship with the Employer Community

Let me turn now to other ways that we support the employer community in its effort to accurately report wages. One of our most important responsibilities is maintaining the accuracy of earnings for all workers who have paid Federal Insurance Contributions Act, or FICA, taxes. As I noted above, properly crediting earnings to the correct SSN ensures that we can determine eligibility for retirement, survivors, and disability benefits and pay the correct benefit amount. Our relationship with over 6 million employers across the United States is vital to the success of this responsibility.

One of the most important ways in which we support the employer community is through our SSN verification services. We have successfully provided SSN verification services to the employer community for many years. Employers can verify SSNs for their employees electronically, by telephone, or by submitting paper listings. In the beginning, we processed most SSN verifications in our field offices. Because this process was highly labor intensive, we have since automated much of this work.

Business Services Online

Our Business Services Online (BSO) initiative enables authorized organizations and individuals to conduct business with us. Once registered through BSO, users may request, activate, and access various services and functions, including our Social Security Number Verification Service (SSNVS), our Telephone Number Employer Verification (TNEV) service, our consent-based SSN verification system (CBSV), and electronic wage reporting.

SSNVS

Today we do most of our employer SSN verifications electronically through the SSNVS program. Under SSNVS, we verify SSNs and names solely to ensure that the records of current or former employees are correct for wage reporting purposes. In FY 2010, we processed about 104 million SSN verifications using SSNVS.

SSNVS is a voluntary, free, and secure Internet service that provides employers with an immediate response for a limited number of SSN verification requests or a next business day response for high volume SSN verification requests.

Employers must use SSNVS consistently. For example:

- If they use it for newly hired workers, they should verify information on all newly hired workers.
- If they use it to verify information on other workers, they should verify the information for all other workers.

We strictly limit third-party use of SSNVS to organizations that contract with employers to either handle the wage reporting responsibilities or perform an administrative function directly related to annual wage reporting responsibilities of hired employees.

There are penalties for SSNVS misuse. Anyone who knowingly and willfully uses SSNVS to request or obtain information from us under false pretenses violates Federal law and may be punished by a fine, imprisonment, or both.

If the name and SSN do not match our records, we tell the employer that the mismatch response does not imply that the employee intentionally provided incorrect information. We also note that the response does not make any statement about the employee's immigration status, and is not a basis, in and of itself, to take any adverse action against the employee.

TNEV

TNEV is an automated telephone service that allows registered employers and third-parties to verify up to 10 employee names and SSNs at one time without speaking to an SSA employee. Like SSNVS, registered users can use TNEV only after an employee has been hired and only for wage reporting purposes. In FY 2010, TNEV handled over 500 calls.

CBSV

CBSV is a fee- and consent-based SSN verification service available to enrolled private companies and Federal, State, and local government agencies. It provides instant, automated verification. Using CBSV, participating companies can verify the SSNs of their customers and clients. Entities must have an Employer Identification Number (EIN) to enroll.

CBSV verifies whether a name and SSN combination match the data in our records. The submitted information is matched against our Numident file. The matching elements include SSN, name, and date of birth. Each SSN and name combination submitted to CBSV will be returned with a "yes" or "no" verification code indicating that the submission either matches or does not match our records. If applicable, we will report a death indicator when our records reflect that the SSN holder is deceased. Results obtained from CBSV do not confirm or authenticate "proof of identity."

CBSV requires the written consent of the SSN holder and the verification results may be used only for the reason that the number holder specifies.

CBSV is fee-based. To use CBSV, entities must pay a one-time non-refundable enrollment fee of $5,000 and then pay a transaction fee per SSN verification request. The transaction fee is presently $5.00 and must be paid in advance.

Periodically, we will recalculate our costs to provide the CBSV service and adjust the transaction fee charged as appropriate. We notify subscribers in writing of any change in the transaction fee. We may close enrollment to CBSV at our discretion.

In FY 2010, we responded to about 1.2 million requests for SSN verification through CBSV.

Wage Reporting

Once an employee is hired, employers must provide us with annual reports of his or her wages. Our role in the wage reporting process is to ensure that all workers receive credit for the work for which they and their employers paid Social Security taxes.

Currently, employers report wages to us annually on Forms W-2 (Wage and Tax Statement). We process the W-2 data for tax purposes for the Internal Revenue Service (IRS). In addition, self-employed individuals report information on self-employment income to IRS on Schedule SE. IRS then sends this self-

employment information to us. We use the individual's name and SSN to record his or her earnings. Use of and disclosure of tax return information is governed by section 6103 of the Internal Revenue Code, and we only use this information for the purpose of administering our programs.

Each year, we process about 240 million W-2s from 6.3 million employers. Employers send these reports either electronically or on paper. We encourage electronic wage reporting, and we work with the employer community to educate them on its advantages. More and more employers submit their wage reports electronically; in fact, employers filed about 84 percent of W-2s electronically in FY 2010 -- up from less than 10 percent in 1999. We believe continued increases in electronic filing will reduce errors over time.

The Earnings Suspense File

The Earnings Suspense File (ESF), or "suspense file," is an electronic holding file for wage items reported on W-2s that we cannot match to the earnings records of an individual worker. If we later resolve the mismatch, we can remove the item from the suspense file and credit the earnings to that person's record.

Since the beginning of the program in 1937 through Tax Year (TY) 2008, the most recent year for which earnings data are available, the suspense file contained about 305 million wage items. While the suspense file represents an accounting of unassociated wage items, the taxes on these wages have been paid into the Trust Funds. For TY 2008, the Trust Funds received credit for $10.7 billion in payroll taxes based on wage items placed in the suspense file.

In order to credit wages to the correct worker, the worker's name and SSN on the W-2 must match the name and SSN in our records. About 10 percent of the W-2s that we receive have invalid name and SSN combinations when we receive them. In our initial processing, our computer system uses more than twenty automated routines to identify commonly occurring errors that, when corrected, enable us to properly post the W-2 information to the correct record.

Using these computer routines, we posted more than half of all W-2s that contained invalid name/SSN combinations to the correct SSN for TY 2008. The balance, about four percent of all W-2s we received for TY 2008, went to the suspense file.

Removing W-2 Items from the Suspense File

We remove wage items from the suspense file on an ongoing basis and post them to the correct worker's record. These reinstatements typically occur when a worker provides evidence of missing wages after reviewing his or her Social Security Statement, or when an employer submits a corrected W-2. Over time, the percentage of W-2s for a given year or period of years that remain in the suspense file declines as a result of this subsequent processing.

We are dedicated to reducing the suspense file's rate of growth and reducing its current size. We want to make sure that workers receive full credit for their earnings and that we pay the correct benefit amount.

Conclusion

I want to thank you again for inviting me to be here today. On behalf of all of my SSA colleagues, we look forward to your continued support of Social Security and for our mission.

I will be glad to answer any questions that you may have.

Chairman JOHNSON. Ms. Moran, welcome. You are recognized for 5 minutes.

STATEMENT OF TYLER MORAN, POLICY DIRECTOR, NATIONAL IMMIGRATION LAW CENTER

Ms. MORAN. Thank you. Good afternoon, Chairman Johnson, Ranking Member Becerra and Members of the Committee. Thank you for the opportunity to testify on E–Verify. The National Immigration Law Center has worked on E–Verify since it was implemented in 1997, and I have personally advocated for improvements in this program for almost a decade.

E–Verify faces a number of challenges despite the progress that it has made, and these challenges would be greatly exacerbated if this program is made mandatory. That is why it is particularly troubling that there may be a bill in the House this year to make this program mandatory, because it almost certainly would pass. According to the Congressional Budget Office, a mandatory E–Verify bill would result in over $17 billion in tax losses because undocumented workers would not leave the country. They and their employers who are currently paying taxes would simply go underground to get around the system.

SSA also testified in 2007 that over 3 million workers would have to go to SSA to stand in line and correct database errors or lose their jobs. And this is a system, as Mr. Stana has testified, that doesn't detect half of undocumented workers.

Additionally, if a mandatory system is put on line without legalizing the 8 million undocumented workers in our economy, it is going to set the system up for failure, not to mention to decimate industries like agriculture.

I want to start by addressing the error rate. The 98 percent confirmation rate sounds very impressive, and there have been a lot of improvements to the programs. But I think it is more helpful to talk about the number of workers affected versus the percentage. Using Westat's conservative estimates, in the mandatory system, 1.2 million people would have to stand in line at SSA to correct their records or lose their jobs, and 770,000 people would likely lose their jobs. This is an underestimate because every employer that has audited, their own data comes up with higher error rates. For example, when Los Angeles County audited its use of E–Verify, it found on the low end that 2 percent of SSA TNCs were erroneous. To make this really concrete, a 2 percent error rate in Texas would mean 244,000 people going to SSA or losing their jobs. And in California that would mean 362,000 people—78,000 alone in L.A. going to only 7 SSA offices.

So these are future projections, but using Westat's statistics in fiscal year 2010 alone, 80,000 U.S. citizens and lawful immigrants lost their jobs. Jessica, a native-born U.S. citizen from southern Florida, is one of those people who called our office. She got a job offer that she accepted at a good-paying telecommunications company. They told her she got a TNC. She went to SSA. She provided the documentation. They said, you are all set, and provided her with paperwork that her name and SSN matched. She went back to her employer, who at first said okay. Three days later they said, I am sorry, you got a final nonconfirmation, we are going to have to fire you. She went back to SSA, waited in line and said, I thought it was okay. They said it is okay. She went back to the employer and the employer said, I am sorry. She was very frustrated. She called USCIS, DHS, and finally called us. She was out of work for 3 months, including over the Christmas holiday. And she now has a lower-paying job.

The worst part about this is that there is no due process in the system, and there is nothing we can do for Jessica to get back her wages or to get back her job. So it is important to note that Jessica is not the only one that faces these challenges at SSA. People have

to take off time from work. It takes costs them money and often they have to go back multiple times.

I want to highlight Arizona because I think it is a good window into what a mandatory system could look like without legalizing undocumented workers. Arizona is the first State to make E–Verify mandatory, and there is three main takeaways. One, undocumented workers didn't leave the State, they didn't leave the country; they went into the underground economy, or they are now popping up as independent contractors. Number two, employers are coaching workers how to get around the system. And number three, despite penalties and mandates, half of employers aren't even using it. So you might think this is all worth it if the system works. But again, 54 percent of undocumented workers aren't detected by the system.

So what are the solutions? As I said in my opening statement, E–Verify has made a number of improvements, but it is just not ready for prime time. If and when Congress decides to make this program mandatory, there are a number of policies that have to accompany it, and they are in my written testimony, but I want to highlight three.

Number one, it has to be paired with a path to legal status for the 8 million undocumented workers. People aren't going to pack their bags because of E–Verify. They are going to stay here, and there are going to be major repercussions for the economy.

Number two, we have to create due process so people have a way to challenge these errors, and that they get back pay if they lose their jobs. We have 9 percent unemployment. We can't have 1 million workers losing their jobs.

And number three, you should phase in E–Verify with performance evaluations along the way for database accuracy, privacy, and employer compliance to make sure the system works for workers and businesses alike.

So in a year when Congress is all about cutting budgets and high-performance programs, mandatory E–Verify just doesn't make sense. When this bill goes to the House floor, you are going to hear a lot about protecting jobs and undocumented immigrants, but I think the members of this committee can play a really key role in highlighting the impact on SSA and impact on U.S. citizens who are the people that are most affected by this program.

Thank you.

Chairman JOHNSON. Thank you, ma'am.

[The prepared statement of Ms. Moran follows:]

This testimony is embargoed until April 14th at 2:00 p.m.

Statement of Tyler Moran
Policy Director, National Immigration Law Center
House Committee on Ways and Means
Subcommittee on Social Security
Hearing on the Social Security Administration's Role in Verifying Employment Eligibility
April 14, 2011

Members of the Committee, thank you for the opportunity to address the critical issue of the progress made and challenges created by E-Verify. My name is Tyler Moran, and I am the Policy Director at the National Immigration Law Center (NILC). NILC is a nonpartisan national legal advocacy organization that works to advance and promote the rights of low-income immigrants and their family members. Since its inception in 1979, NILC has earned a national reputation as a leading expert on the intersection of immigration law and the employment rights of low-income immigrants. NILC's extensive knowledge of the complex interplay between immigrants' legal status and their rights under U.S. employment laws is an important resource for immigrant rights coalitions and community groups, as well as policymakers, attorneys, workers' rights advocates, labor unions, government agencies, and the media. NILC has analyzed and advocated for improvements of E-Verify since it was first implemented in 1997 as the Basic Pilot program, and has extensive experience assisting advocates and attorneys in responding to problems with the program as it affects workers—immigrants and U.S.-born alike.

Overview

Since E-Verify was implemented in 1997, it has narrowly been framed as a tool to prevent the employment of undocumented workers. The biggest impact of the program, however, is on U.S. workers, businesses, and the Social Security Administration (SSA). If made mandatory, 6 million employers and their 154 million employees would have to receive permission from the government before continuing the employment relationship. E-Verify has made progress since it was first implemented, but the fact remains that the system simply is not ready for mandatory use: it would cause a minimum of $22 billion in lost tax revenue at a time when policymakers are trying to slash budgets; would cause anywhere from 1.2 million to 3 million workers to stand in line at SSA or lose their jobs at a time of 9 percent unemployment; and is unable to detect 54 percent of unauthorized workers who are run through the system.

Mandatory E-Verify has been part of every immigration reform bill since 2005, and NILC has worked on a bi-partisan basis to craft proposals that ensure due process and privacy protections for all workers. The key starting point to any mandatory E-Verify proposal, however, is a path to legal status for undocumented immigrants in our country. Mandatory E-Verify without creating a legal labor force will set the program up for failure and exacerbate our current economic challenges. Eight million undocumented workers are not going to leave the country because of E-Verify; they and their employers will simply move into the underground economy, resulting in a significant loss of federal, state, and local tax revenues, including a drastic reduction in contributions to the Social Security trust fund.

My testimony today will focus on: (1) the impact of E-Verify on U.S. citizens and lawful immigrants; (2) the costs of implementing E-Verify without a legal workforce; (3) the impact of a mandatory system on SSA; and (4) what it would take to make E-Verify successful.

E-Verify error rates will cause American workers to lose their jobs

While E-Verify error rates have improved since the program was implemented in 1997, there is still significant cause for concern. Currently, 97.4 percent of workers run through E-Verify are immediately

confirmed as work authorized.[1] As a statistic, this may sound successful, but these numbers represent real people— your constituents—and the actual number of workers affected is concerning. Using a statistical model developed by the Westat Corporation for the Department of Homeland Security (DHS), approximately 0.8 percent of tentative nonconfirmations (TNCs)—or 22 percent of all persons run through E-Verify—are issued in error.[2] Of the 16 million E-Verify queries by employers in fiscal year 2010, 128,000 workers had to go to SSA or call DHS to fix a database error or lose their jobs.[3] Of the 0.8 percent of workers who received a TNC in error, 0.3 percent[4] were able to correct the issue and keep their jobs—meaning 0.5 percent of all U.S. citizen and work-authorized immigrant workers receive a *final* nonconfirmation (FNC) in error. A final nonconfirmation obligates the employer to fire the worker or risk being liable for immigration violations.[5] This means that in fiscal year 2010 approximately 80,000 workers likely received erroneous findings from the system and may have lost their jobs as a result.[6]

For example[7] –

- *A U.S. citizen born in Florida was hired for a good-paying telecommunications position in October 2010. After hire, she was run through E-Verify and received a TNC. Her employer did not sit down with her to explain to her what a TNC means, nor to explain any of her rights. The worker went to her local SSA office twice to try and resolve the situation, but despite SSA telling her that her information had been updated, the employer told her that she was still not confirmed. She ultimately received an FNC and was fired. After her termination, she has gone to great lengths to try and correct this error, but has been unable to do so. She was unemployed for over 3 months, including over the Christmas holiday, but recently accepted a new lower-paid position.*[8]

---

[1] Richard M. Stana, *Report to the Subcommittee on Social Security, Committee on Ways and Means, U.S. House of Representatives: Employment Verification, Federal Agencies Have Taken Steps to Improve E-Verify, but Significant Challenges Remain* (Government Accountability Office, Dec. 2010, GAO-11-146), www.gao.gov/new.items/d11146.pdf,.

[2] Employers receive a "tentative nonconfirmation" notice-or TNC-from either SSA or DHS when the agencies are unable to automatically confirm a worker's employment eligibility. A "tentative nonconfirmation" notice is not an indication of an immigration violation, and workers have the right to contest the finding with the appropriate agency. For erroneous TNC rate, *see Findings of the Web-Based E-Verify Program Evaluation* (Westat, Dec. 2009), www.uscis.gov/USCIS/E-Verify/E-Verify/Final%20E-Verify%20Report%2012-16-09_2.pdf, p. 117.

[3] There were approximately 16 million E-Verify queries in fiscal year 2010. See *E-Verify Gets High Marks from Employers in Customer Satisfaction Survey* (U.S. Citizenship and Immigration Services, Jan. 18, 2011), www.uscis.gov/portal/site/uscis/menuitem.5af9bb95919f35e66f614176543f6d1a/?vgnextoid=a6adb46adba9d210VgnVCM100000082ca60aRCRD&vgnextchannel=a2dd6d26d17df110VgnVCM1000004718190aRCRD. Approximately 0.8 percent of work-authorized individuals receive a TNC in error. See Westat, *supra* note 2. The 128,000 figure was arrived at by multiplying these two numbers.

[4] *Statistics and Reports* (U.S. Citizenship and Immigration Services, Feb. 4, 2011), http://www.uscis.gov/portal/site/uscis/menuitem.eb1d4c2a3e5b9ac89243c6a7543f6d1a/?vgnextoid=7c579589cdb76210VgnVCM100000b92ca60aRCRD&vgnextchannel=7c579589cdb76210VgnVCM100000b92ca60aRCRD.

[5] 8 USC §1324a note.

[6] There were approximately 16 million E-Verify queries in fiscal year 2010. See U.S. Citizenship and Immigration Services *supra* note 4. Approximately 0.5 percent of work-authorized individuals receive a final nonconfirmation in error. (0.8 percent receive an *erroneous* TNC, and 0.3 percent are able to correct their TNC. This results in 0.5 percent of individuals receiving an erroneous TNC that could not be corrected and therefore became an erroneous final nonconfirmation.) The 80,000 figure was arrived at by multiplying these two numbers.

[7] For more examples of U.S. citizens and lawful immigrants affected by E-Verify, see *How Errors in E-Verify Databases Impact U.S. Citizens and Lawfully Present Immigrants* (NILC, March 2010), www.nilc.org/immsemplymnt/ircaempverif/e-verify-errors-and-USCs-2010-03-03.pdf.

[8] Jessica St. Fleur, *Written Statement for the House Committee on the Judiciary, Subcommittee on Immigration Policy and Enforcement: Hearing on E-Verify – Preserving Jobs for American Workers*, Feb. 10, 2011.

- *A U.S. citizen and former captain in the U.S. Navy with 34 years of service and a history of having maintained high security clearance was flagged by E-Verify as not eligible for employment. It took him and his wife, an attorney, two months to resolve the discrepancy.*[9]

- *A U.S. citizen applied for a position with a temporary agency in California, only to be turned away because E-Verify was unable to confirm her work authorization. The employer did not advise her of her right to contest the finding and violated the law by asking her to show additional documents. She was unemployed for over four months without health insurance and was diagnosed with a serious illness during that time.*[10]

If use of E-Verify were to become mandatory, using Westat's statistical model, about 1.2 million U.S. citizen and work-authorized immigrants would have to contact SSA or DHS or risk losing their jobs[11] and about 770,000 workers would likely lose their jobs.[12] These numbers, however, are likely underestimates as employers who audit their own E-Verify data report higher error rates than federal government estimates. For example, when Los Angeles County audited its use of E-Verify for county workers, it found that 2.0 to 2.7 percent of its TNCs from SSA were erroneous in 2008-09.[13]

Mandatory E-Verify for all workers: estimated error rates

Source of estimate	Erroneous TNC rate	# of workers required to contact SSA or DHS or lose their jobs
Westat report	0.8%	1.2 million
LA County	2.0%-2.7%	3 million – 4.1 million
Intel corporation[14]	12%	18.5 million

The error rates affect all workers, but Westat found that they have a discriminatory impact on lawful foreign-born workers. Westat's 2009 report found the erroneous TNC rate for foreign-born workers was 20 times higher than that of U.S.-born workers.[15]

The challenges U.S. workers face in correcting E-Verify errors

Receipt of an erroneous TNC puts an enormous burden on workers and can result in loss of wages to challenge the error, adverse action by employers, and loss of employment. In fact, GAO called the process of challenging an E-Verify error "formidable."[16]

---

[9] Account related at a Jan. 24, 2009, town hall meeting in Ashtabula, OH, sponsored by Building Unity in the Community and billed as "Why We Need Comprehensive Immigration Reform."
[10] Summary of charge filed with the Dept. of Justice Office of Special Counsel for Immigration-Related Unfair Employment Practices in 2008.
[11] About 0.8 percent of workers receive an *erroneous* tentative nonconfirmation, or "TNC." Westat, *supra* note 2, p. 117. There are currently about 154,287,000 million workers in the U.S. The 1.2 million figure was arrived at by multiplying these two numbers.
[12] Approximately 0.5 percent of work-authorized individuals receive a final nonconfirmation in error. See note 7, *supra*. There are currently 154,287,000 million workers in the U.S. The 771,435 figure was arrived at by multiplying 154,287,000 million by the 0.5 erroneous final nonconfirmation rate.
[13] Marc Rosenblum, *E-Verify: Strengths, Weaknesses, and Proposals for Reform* (Migration Policy Institute, Feb. 2011), http://www.migrationpolicy.org/pubs/E-Verify-Insight.pdf.
[14] Intel Corporation, "Comments on Proposed Employment Eligibility Regulations Implementing Executive Order 12989 (as amended)," Aug. 8, 2008.
[15] Westat *supra* note 2, p. xxxv.
[16] Stana, *supra* note 1, p. 34.

When workers receive a TNC notice, they often have to take unpaid time off from work to follow up with SSA, which may take more than one trip. In fiscal year 2009, 22 percent of workers spent more than $50 to correct database errors and 13 percent spent more than $100.[17] In 2009, the waiting times for SSA office visits were 61 percent longer than they were in 2002. During the period March 1, 2009 through April 30, 2010, about 3.1 million visitors waited more than 1 hour for service, and of those visitors, over 330,000 waited more than 2 hours. Further, in fiscal year 2009, about 3.3 million visitors left a field office without receiving service.[18] American Council on International Personnel members report that corrections at SSA usually take in excess of 90 days, and that employees must wait four or more hours per trip, with repeated trips to SSA frequently required to get their records corrected.[19] Though waiting times at SSA offices have improved in the last year, the Commissioner recently testified that a reduction in funding would reverse the progress SSA has made.[20]

Workers aren't always given the opportunity to correct these errors. Although required by law to do so, employers do not always notify workers of a TNC. Workers who do not contest database errors lose their jobs. In fiscal year 2009, 42 percent of workers report that they were not informed by their employer of a TNC.[21] A survey of 376 immigrant workers in Arizona also found that 33.5 percent had been fired, apparently after receiving an E-Verify TNC, but that *none* had been notified by employers that they had received a TNC or given information to appeal the finding.[22]

Employer noncompliance with the program's rules is extremely high, with over 66 percent of employers taking adverse actions against workers receiving a TNC.[23] Actions include prohibiting workers for whom they had received a TNC from working; restricting such workers' work assignments; and delaying job training for such workers.[24] And, at least 57 percent of employers using E-Verify violate the program's rules by using it to prescreen workers.[25] When workers are prescreened and not offered a job, it takes them at least three weeks to find other employment.[26]

Noncompliance with program rules would almost certainly increase if all employers were required to use the system. Current E-Verify users are disproportionately large businesses and federal contractors, and most users that have enrolled in the system have chosen to do so on a voluntary basis — all factors that make them *more likely* than a "typical" U.S. employer to approve of the system and use it successfully. In Arizona, the first state to make E-Verify mandatory, employers are less compliant with E-Verify

---

[17] Westat *supra* note 2, pp. 203-204

[18] *Customer Waiting Times in the Social Security Administration's Field Offices* (Social Security Administration Office of the Inspector General, Oct. 2010), http://www.socialsecurity.gov/oig/ADOBEPDF/A-04-10-11034.pdf, p. 3.

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

[20] Michael J. Astrue, *Testimony before the U.S. Senate Committee on Appropriations, Subcommittee on Labor, Health and Human Services, Education and Related Agencies* (Social Security Administration, March 9, 2011), http://www.socialsecurity.gov/legislation/SSA%20BudgetTestimony030911.pdf, p. 18.

[21] Westat *supra* note 2 pp. 154, 199

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

[23] Westat *supra* note 2, p. 157. Thirty-seven percent of employers self-reported that they took adverse actions against workers receiving a TNC, and workers reported that an additional 29 percent of employers took adverse action against them, with a total of over 66 percent of employers take adverse action.

[24] Westat, *supra* note 2, pp. 157, 204.

[25] *Id.* at 149

[26] *Id.* at 140

procedures than other E-Verify employers.[27] The likely reason is that, unlike most E-Verify users, most Arizona employers did not volunteer to use the program.

Mandatory E-Verify will result in billions of dollars of lost tax revenue, while only detecting half of all undocumented workers.

Undocumented workers are not going to leave the country simply because Congress makes it harder for them to work here. It is clear that undocumented immigrants fill a niche in our economy and are here to stay, despite imposition of a verification system. And because these workers are a central part of our economy, employers will use any means necessary to keep them, including moving into the underground economy, misclassifying workers as independent contractors, and simply not participating in any employment verification system.[28] The implications of undocumented workers moving into the underground economy are grave. In analyzing a 2008 bill that would have made E-Verify mandatory (without also providing a way for unauthorized workers to become work-authorized) the Congressional Budget Office (CBO) found that it would decrease federal revenue by more than $22 billion over ten years—because it would increase the number of employers and workers who resort to the black market, outside of the tax system.[29]

Eight million undocumented workers moving off the books will also threaten the solvency of the Social Security trust fund. Over the next 20 years, the number of senior citizens relative to the number of working-age Americans will increase by 67 percent, which means that they will "transition from being net taxpayers to net recipients" and they will be "supported by a smaller workforce that is struggling to meet its own needs."[30] It is estimated that two-thirds of undocumented immigrants currently pay payroll taxes, which generated $12 billion into the Social Security Trust fund in 2007.[31] In fact, the trust fund had received a net benefit of somewhere between $120 billion and $240 billion from unauthorized immigrants by 2007, which represents 5.4 percent to 10.7 percent of the trust fund's total assets. The chief actuary of SSA has stated that without undocumented immigrants' contributions to the trust fund, there would have been a "shortfall of tax revenue to cover [payouts] starting [in] 2009, or six years earlier than estimated under the 2010 Trustees Report."[32]

Arizona, the first state to make E-Verify mandatory for all employers in 2008, provides a window into the economic consequences of implementing the program with undocumented workers in the labor force. In 2008, the first year the law was in effect, income tax collection dropped 13 percent from the year before. Sales taxes, however, only dropped by 2.5 percent for food and 6.8 percent for clothing. The conclusion was that workers weren't paying income taxes, but were still earning money to spend—meaning that the

---

[27] Westat, *supra* note 2, p. 237.
[28] *See* Jim McTague, "The Underground Economy: Illegal Immigrants and Others Working Off the Books Cost the U.S. Hundreds of Billions of Dollars in Unpaid Taxes," *The Wall Street Journal Classroom Edition*, April 2005, http://wsjclassroom.com/archive/05apr/econ_underground.htm; Lora Jo Foo, *The Vulnerable and Exploitable Immigrant Workforce and the Need for Strengthening Worker Protective Legislation* (Yale Law Journal, 103 Yale L.J. 2179, May 1994), www.wiego.org/papers/FooImmigrantWorkers.pdf.
[29] Letter to Rep. John Conyers, Chair, Committee on the Judiciary, U.S. House of Representatives, from Peter Orszag, Director, Congressional Budget Office, Apr. 4, 2008, www.cbo.gov/ftpdocs/91xx/doc9100/hr4088ltr.pdf.
[30] Dowell Myers, *Thinking Ahead About Our Immigrant Future: New Trends and Mutual Benefits in Our Aging Society* (Immigration Policy Center, Jan. 2008), http://www.immigrationpolicy.org/sites/default/files/docs/Thinking%20Ahead%201-08.pdf.
[31] Edward Schumatcher-Matos, "How illegal immigrants are helping Social Security," *The Washington Post*, Sept. 3, 2010, http://www.washingtonpost.com/wp-dyn/content/article/2010/09/02/AR2010090202673.html.
[32] *Id.*

underground economy was growing.[33] This loss in tax revenue was happening at a time when the state was facing a $3 billion budget gap. The Public Policy Institute of California echoed this finding in a recently released study that found that although the law did lead to some undocumented immigrants leaving the state, the unintended consequence of the law was that workers were being pushed into underground employment.[34]

Arizona employers who didn't move their workforce into the underground economy simply didn't use E-Verify or learned how to manipulate the system. Though Arizona employers made 1.3 million new hires in the fiscal year that ended in September 2009 and were required by state law to check all of them via E-Verify, they actually checked only 730,000 of them—or slightly more than half.[35] U.S. Immigration and Customs Enforcement (ICE) officials also report that unscrupulous employers in Arizona have learned that E-Verify's photo-matching tool (which is used to confirm workers' identities through a photo comparison) accepts only two documents, and therefore they ask employees whom they suspect are not work-authorized to provide some other identity document that the photo-matching tool does not accept.[36]

In addition to these enormous costs and limitations, E-Verify has come up short in its role of detecting undocumented workers. Westat researchers found that in 2008, 54 percent of unauthorized workers for whom E-Verify checks were run—or 56,000 workers—were erroneously confirmed as being work-authorized.[37] Migration Policy Institute estimates that 230,000 unauthorized workers were erroneously confirmed in 2009.[38]

The impact of mandatory E-Verify on SSA

While DHS administers E-Verify, SSA plays an integral role in ensuring its functionality. In fact, SSA takes on the bulk of verification responsibilities because it must verify the name, Social Security number (SSN), and date of birth (and citizenship status of U.S. citizens) of *every worker* in the country whose employer participates in E-Verify. If E-Verify were to become mandatory this would mean that SSA would need to process 154 million queries in the initial implementation period and 50-60 million queries each year thereafter. This is at a time when the agency is dealing with "unprecedented workloads combined with declining budgets [that have] damaged [the agency's] service delivery."[39]

Processing queries is just one aspect of SSA's work. Serving customers who must fix database errors puts the greatest demand on SSA resources. A November 2010 SSA Office of the Inspector General report found that in fiscal year 2008, when there were only a total of 7 million E-Verify queries, approximately 88,000 people called the 1-800 number or visited SSA due to E-Verify errors.[40] In a hearing before this subcommittee in 2007, SSA estimated that if E-Verify were made mandatory, 3.6 million citizens and lawful immigrants would either have to go to an SSA office to correct their records or

---

[33] Daniel Gonzalez, "Illegal Workers Manage to Skirt Arizona Employer-Sanctions Law: Borrowed Identities, Cash Pay Fuel an Underground Economy," *The Arizona Republic*, Nov. 30, 2008.
[34] Magnus Lofstrom, Sarah Bohn, and Steven Raphael, *Lessons from the 2007 Legal Arizona Workers Act* (Public Policy Institute of California, March 2011), http://www.ppic.org/content/pubs/report/R_311MLR.pdf.
[35] Jahna Berry, "Most Arizona Employers Aren't Using E-Verify," *The Arizona Republic*, July 28, 2010, www.azcentral.com/arizonarepublic/news/articles/2010/07/28/20100728arizona-employers-ignoring-e-verify.html.
[36] Stana, *supra* note 1, p. 22.
[37] Westat *supra* note 2, p. 118.
[38] Marc Rosenblum, E-Verify: Strengths, Weaknesses, and Proposals for Reform, Senate staff briefing handout (Migration Policy Institute, Feb. 17, 2011).
[39] Astrue, *supra* note 20, p. 2.
[40] *Field Office Workload Related to Nonconfirmation Responses from the Employment Verification Program* (Office of the Inspector General, Social Security Administration, Nov. 2010 A-03-09-19052), http://www.socialsecurity.gov/oig/ADOBEPDF/A-03-09-19052.pdf, Appendix D.

lose their jobs.[41] Additionally, the President of the National Council of Social Security Management Associations, Inc., has testified in the past that if mandatory E-Verify and hardened SSN card are implemented without necessary funding, "it could cripple SSA's service capabilities."[42] This problem is compounded by the fact that the agency has suffered from "years of underfunding."[43] The Commissioner also recently testified that further funding reductions will threaten SSA's ability to keep its "technology environment operating smoothly,"[44] which would include the operation of E-Verify.

Biometric cards and information-sharing do not address E-Verify's limitations, yet create new challenges.

Identity sharing and fraud is a major weakness of E-Verify since the system can only detect if documentation presented by the individual is legitimate—not if the documentation presented matches the individual. Numerous proposals have been introduced to address this limitation, including biometric employment cards and the sharing of taxpayer information with DHS. These proposals, however, only create greater challenges and jeopardize important tax confidentiality law.

Limitations of a biometric employment card

A handful of bills and proposals have been introduced over the last few years that create a biometric employment verification card. The costs, accuracy and mission creep that would result from such a card, however, far outweigh any benefit. As this committee well knows, despite best intentions to keep a card used for one sole purpose, the temptation to use it for other purpose is inevitable. After the SSN card was created in 1936, the first regulation issued by the Social Security Board declared that SSNs were for the exclusive use of the Social Security system.[45] Nevertheless, SSNs have become the universal identifier of choice for government agencies. Like the SSN, a biometric employment card would quickly become the primary identifier used for other purposes, from proving eligibility to vote to establishing identity when buying a gun.

The cost of implementing a biometric system is prohibitively expensive. One existing system that provides insight into what it would cost to implement a national biometric ID, and whether it would be a success, is the Transportation Worker Identification Credential (TWIC), a biometric ID used to access maritime transportation facilities and vessels. DHS estimated that it would need to spend up to $1.9 billion in order to issue biometric IDs to a mere one million workers under TWIC.[46] Applying this cost-per-worker ratio to a national employment eligibility verification system affecting 150 million workers, it is reasonable to assume that the price tag would be $285 billion.

In addition to cost concerns, the accuracy of a biometric, such as a fingerprint, is still inadequate and will likely prevent millions of U.S. citizens from obtaining jobs. The National Maritime Security Advisory Committee (NMSAC) reports that different enrollment sites for the TWIC card have not been able to

---

[41] Transcript from Hearing on Employment Eligibility Verification Systems (Subcommittee on Social Security, Committee on Ways and Means, U.S. House of Representatives, June 7, 2007).
[42] Richard Warsinskey, *Testimony before the U.S. Senate Committee on Finance: Funding Social Security's Administrative Costs: Will the Budget Meet the Mission?* (National Council of Social Security Management Associations, Inc., May 23, 2007), http://finance.senate.gov/hearings/testimony/2007test/052307testrw.pdf.
[43] Astrue, supra note 20, p. 2.
[44] *Id.*, p. 7.
[45] Marc Rotenberg, Executive Director, Electronic Privacy Information Center, Statement at U.S. House Committee on the Judiciary, Subcommittee on Immigration, Border Security, and Claims, May 12, 2005, http://commdocs.house.gov/committees/judiciary/hju21141.000/hju21141_0f.htm.
[46] *Transcript from Hearing on Transportation Worker Identification Programs* (Committee on Commerce, Science & Transportation, U.S. Senate, May 16, 2006).

enroll between 3.7 and 8 percent of workers because of fingerprinting failures.[47] And a U.S. Government Accountability Office (GAO) report revealed that thousands of TWIC enrollees experienced delays in receiving their TWIC card for varying reasons.[48] A different GAO report on the Census Bureau's requirement that all temporary employees be fingerprinted for FBI background checks found that, after Census Bureau staff received hours of training in proper fingerprinting techniques, over 20 percent of the prints they took were unusable.[49] Workers who perform manual or farm labor will face particular challenges because the tips of their fingers can become worn or abraded, and prints made from them are difficult to read.[50]

Information sharing between SSA and DHS and the Internal Revenue Service

A handful of bills have also proposed information-sharing among the Internal Revenue Service, SSA and DHS. Proposals differ, but they generally create exceptions to the confidentiality provisions in the tax code by requiring SSA to disclose taxpayer identity information of employers and employees to DHS when the employer has filed Wage and Tax Statements (Forms W-2) that have a certain number of names that do not match SSA records or employees that write "000-00-0000" on their W-2 instead of an SSN.

Disclosure of employers' taxpayer identity information to DHS is problematic. There are numerous reasons why employees' names and SSNs might not match SSA records, including incorrect data entry, name changes due to marriage or divorce, and misspelled names. No-matches are not a proxy for unauthorized immigration status. Rather, they indicate that workers are not receiving proper credit for their earnings, which will affect the level of retirement or disability benefits they may receive in the future. In fact, SSA estimates that 17.8 million (or 4.1 percent) of its records contain discrepancies, and that 12.7 million (about 70 percent) of those records with errors belong to native-born U.S. citizens.[51]

DHS itself recognizes that SSA's database is ineffective as an immigration enforcement tool. For example, SSA already shares with DHS a list of SSNs associated with the "Nonwork Alien File," a database which contains information on noncitizens who have earnings recorded under nonwork SSNs, which DHS could use to track immigrants who are potentially working in the U.S. unlawfully using a nonwork SSN. DHS has stated, however, that the file is not an effective worksite enforcement tool due to "inaccuracies in the data and the absence of some information that would help the department efficiently target its enforcement."[52] These "inaccuracies," however, derive from the same database that results in no-match's on the W-2.

---

[47] "National Maritime Security Advisory Committee, TWIC Working Group: Discussion Items" (as amended July 30, 2008), www.maritimedelriv.com/Port_Security/TSA/files/NMSAC_TWG_recommendations_amended.pdf, p.1 and 7.

[48] *Transportation Worker Identification Credential: Progress Made in Enrolling Workers and Activating Credentials but Evaluation Plan Needed to Help Inform the Implementation of Card Readers* (U.S. Government Accountability Office, GAO-10-43, Nov. 2009), www.gao.gov/new.items/d1043.pdf.

[49] Robert Goldenkoff, *2010 Census: Census Bureau Continues to Make Progress in Mitigating Risks to a Successful Enumeration, but Still Faces Various Challenges* (U.S. Government Accountability Office, GAO-10-132T, Oct. 7, 2009), www.gao.gov/new.items/d10132t.pdf.

[50] "What Factors Cause Biometric Systems to Fail?" (International Biometrics Group website), www.biometricgroup.com/reports/public/reports/biometric_failure.html.

[51] *Congressional Response Report: Accuracy of the Social Security Administration's Numident File* (Office of the Inspector General, Social Security Administration, December 2006, A-08-06-26100).

[52] Barbara D. Bovbjerg, *Social Security Numbers: Coordinated Approach to SSN Data Could Help Reduce Unauthorized Work* (Washington, DC: Government Accountability Office, February 16, 2006), www.gao.gov/new.items/d06458t.pdf.

Disclosure of employers' taxpayer identity information when SSA records indicate employees used 000-00-0000 instead of an SSN is also problematic, since the existence of such a situation does not necessarily indicate fraud. Employers are instructed by the IRS to put 000-00-0000 on W-2s when their employees have applied for SSNs but have not received them. Advocates of information-sharing between IRS, SSA, and DHS frequently cite the use of 000-00-000 as justification for the breach of tax confidentiality rules, because they argue that using all zeroes on a W-2 is an indication that a person is not work-authorized. However, employers with high numbers of authorized workers who don't yet have their SSNs would be flagged by SSA for simply following the law.

These information-sharing requirements are an incursion into protections for confidentiality of tax information provided by section 6103 of the tax code, which are designed to increase compliance with the tax law by barring tax information from being used for non-tax purposes. These confidentiality protections would be undermined by wholesale information-sharing for non-tax purposes without prior review by an independent arbiter. Additionally, because DHS would be given access to employer tax identity information, it is likely that employers will become fearful that they are in violation of immigration law when their previously confidential tax information is revealed. The result is that employers will be overly cautious and fire these employees. Already, thousands of workers have been fired due to the mistaken assumption that an SSA no-match letter indicates an immigration violation.[53] There is also no indication that DHS makes good use of earnings information it currently has available to it, nor that it has a clear sense of what its future data needs will be and what information will actually be useful for enforcement purposes.[54] Given these gaps, wholesale information sharing with DHS is unwise.

How can the shortcomings of E-Verify be improved?

As stated in my introduction, E-Verify has made progress since it was implemented in 1997, but it simply isn't ready for mandatory use. If and when Congress decides to make the program mandatory, there are a number of key policies that must accompany any expansion in order to set the program up for success. These recommendations are based on NILC's 14 years of experience with the program.

1. **Only consider making E-Verify mandatory if paired with a legalization program**. If implemented without legalizing the 8 million undocumented workers in our economy, employers will simply move them off the books into the underground economy, causing billions of dollars in lost tax revenue.
2. **Apply E-Verify only to new hires.** Reverification of the entire workforce would place a huge administrative burden on workers and businesses alike. A current turnover/separation rate of 40 percent a year (50-60 million employees hired each year) means that most people's employment eligibility will be verified by the new system in a timely manner without forcing employers to go through old records and reverify existing workers.
3. **Phase in E-Verify with performance evaluations**. Phase-in E-Verify incrementally by size of employer or by industry, with vigorous performance evaluations taking place prior to each expansion. Evaluations should address, at minimum, wrongful terminations due to system errors, employer compliance with program rules, and the impact of the system on workers' privacy.

---

[53] C. Mehta, N. Theodore, and M. Hincapié, *Social Security Administration's No-Match Letter Program: Implications for Immigration Enforcement and Workers' Rights* (Center for Urban Economic Development, University of Illinois at Chicago; and National Immigration Law Center, Nov. 2003) at 2, available at www.uic.edu/cuppa/uicued/npublications/recent/SSAnomatchreport.pdf.

[54] *See Immigration Enforcement: Benefits and Limitations to Using Earnings Data to Identify Unauthorized Work, GAO-06-814R* (Government Accountability Office, July 11, 2006) at 4, available at www.gao.gov/new.items/d06814r.pdf.

Minimum performance criteria should be met within each of these areas before subsequent expansions of the system.

4. **Ensure data accuracy**. Establish data accuracy standards that are subject to annual review to ensure that the data accessed by employers is accurate and continuously updated.
5. **Protect workers from misuse of the system**. Prohibit use of E-Verify to selectively verify only certain workers, pre-screen workers before a job offer, take adverse employment actions based on system determinations, and fail to inform workers of their rights under the program. Establish an oversight and penalty structure to ensure employer compliance with program rules.
6. **Ensure due process for workers subject to database errors**. Provide for administrative and judicial review and allow workers to remain employed while they challenge government errors. Provide compensation from the government, costs, and attorney's fees when an error in the databases results in wrongful termination of employment.
7. **Protect the privacy of workers**. Minimize the amount of data collected and stored and create penalties for collecting, maintaining, or distributing data not authorized in the statute. Create penalties to deter the use E-Verify data to commit identity fraud or for any other unauthorized purpose.
8. **Create oversight of the E-Verify**. In order to ensure that employers are complying with program requirements, authorize random audits of the program that include, but are not limited to, a review of employer compliance with E-Verify requirements, a review of the adequacy of E-Verify rules and procedures to protect authorized workers, and a review of whether the program is being managed in a way that appropriately addresses civil rights and civil liberties concerns.
9. **Fund an outreach program**. Following in the footsteps of the process instituted when the I-9 employment eligibility verification form was first introduced in 1986, the Office of Special Counsel for Immigration-Related Unfair Employment Practices (OSC) should be charged with conducting outreach and education to both workers and employers in order to inform them about how the system works, rights and responsibilities under the new system, and avenues for redress in the case of error or unfair employment practices.
10. **Create a term-limited employment verification advisory panel**. The advisory panel would advise SSA and DHS on implementation of E-Verify, including standards of database accuracy, privacy, and compliance, in addition to outreach to workers and employers. The panel would include representatives from appropriate federal agencies, organizations with technological and operational expertise in database accuracy, and other stakeholders that represent the interests of persons and entities affected by database inaccuracies, including business, labor unions, privacy advocates, and immigration organizations.
11. **Clarify that states are preempted from requiring businesses to use E-Verify**. Clarifying the statute's language with respect to this issue would ensure that the federal government controls uniform expansion of the program.
12. **Test new ideas through pilot projects**. DHS's E-Verify program is not the only possible platform for electronic eligibility verification, and alternative verification systems have been proposed. Any new idea should not be implemented on a large scale, however, before being rigorously tested. Pilot programs should measure the effectiveness, accuracy, and usability of new systems, and assess how they compare to E-Verify.

In the meantime, there are a number of steps that can be taken to improve the integrity of the program in its voluntary nature.

1. **Create due process for workers who lose their jobs.** Currently, there is no redress procedure for workers who receive an E-Verify final non-confirmation (FNC) in error. Employers who receive an FNC risk being held liable for immigration violations if they do not terminate the worker's employment, yet the worker has no means to either fix the error or get his or her job

back. As noted in my testimony, at least 80,000 workers lost their jobs in FY10. Workers should also be able to stay on the job while they challenge the erroneous FNC.

2. **Improve employer compliance with E-Verify rules.** Employer noncompliance with the E-Verify Memorandum of Understanding (MOU) has increased since the program was implemented, likely because the number of employers who are required to use the program has increased. There is currently no penalty for an employer who violates the MOU—even though it could result in the loss of employment for the worker. A number of steps can be taken including:
   - Revising the MOU to include penalties for misuse or noncompliance that employers must agree to be subject to as a condition of using E-Verify.
   - Increasing staff charged with ensuring compliance with the MOU (versus compliance with immigration law).
   - Requiring the DHS Office for Civil Rights and Civil Liberties to conduct annual civil liberties impact assessments of the program that include, but are not limited to, a review of employer compliance with E-Verify system requirements; a review of the adequacy of E-Verify rules and procedures to protect authorized workers; a review of whether the program is being managed in a manner that appropriately addresses and anticipates civil rights and civil liberties concerns; and recommendations for additional actions needed to address civil rights and civil liberties concerns.

3. **Establish a complaint and redress process for violations of the E-Verify MOU.** Create a community liaison department within the E-Verify monitoring and compliance unit to assist workers who suffer adverse action because of misuse of the E-Verify program and develop protocols for responding to worker complaints. As noted in my testimony, 66 percent of workers face adverse action from their employer when they receive a TNC.

4. **Increase appropriations for the Department of Justice Office of Special Counsel for Unfair Immigration Related Employment Practices (OSC).** OSC is the agency tasked with working with workers and employers to enforce the anti-discrimination provisions in the Immigration and Nationality Act, including the employment verification process. OSC currently receives the bulk of phone calls from E-Verify users who either have questions about the program or who want to report employer misuse.

5. **Halt further expansion of E-Verify.** Rather than supporting mandates for the rapid growth of the existing program, further expansion should be halted until there is a comprehensive analysis of current and potential problems, and consider a number of modifications to ensure that the program accomplishes its goals.

Conclusion

Making E-Verify mandatory outside of broader reform of our immigration system undermines American jobs and will ultimately impose new burdens on our economy, workers, businesses and SSA. E-Verify has made a number of improvements, but still suffers from significant shortcomings that must be addressed before further expansion. Because so much of the focus of E-Verify is on DHS, it will be important for this committee to continue to play a leadership role in highlighting the impact of the program on SSA and U.S. workers. It would be a major step in our country to require all workers to seek confirmation from the government to keep their job and we need to get it right.

Chairman JOHNSON. It sounds like you don't like the program. We have got to do something to stop the illegal workers.

Ms. MORAN. If we pair it with legalization, then we can talk.

Chairman JOHNSON. Dr. Antón, you are recognized for 5 minutes. Thank you.

STATEMENT OF ANA I. ANTÓN, Ph.D., PROFESSOR, DEPARTMENT OF COMPUTER SCIENCE, COLLEGE OF ENGINEERING, NORTH CAROLINA STATE UNIVERSITY, ON BEHALF OF THE ASSOCIATION FOR COMPUTING MACHINERY

Ms. ANTÓN. Good afternoon, Chairman Johnson, Ranking Member Becerra and Members of the Subcommittee. Thank you for the opportunity to testify. This statement represents my own professional position, as well as that of the Association of Computing Machinery's U.S. Public Policy Council.

By way of introduction, I am a professor of software engineering at North Carolina State University and the director of an academic privacy research center. In addition, I serve on several industry and government technical boards and advisors, including the DHS Data Privacy and Integrity Advisory Committee.

The E–Verify pilot system is intended to ensure that only authorized citizens and legal residents can be employed in the United States, a laudable objective, especially in a time of notable unemployment. Unfortunately the intent has not matched the realization. Complex systems such as E–Verify are fallible and often misused and subject to mission creep. One large-scale evaluation of E–Verify reported that the majority of illegal immigrants checked through the system were incorrectly deemed eligible to work primarily as a result of identity fraud. Thus E–Verify remains vulnerable to and incentivizes the use of identity fraud.

Among the issues noted in my written testimony are three that are especially critical to consider from a systems engineering perspective. First, E–Verify must be able to accurately identify the individuals and employers authorized to use the system in a trustworthy manner before it is widely deployed. Second, proof of success with a pilot must be required before extensively expanding it. Third, complex systems such as E–Verify are often misused and repurposed in ways that violate sound principles of security and good software engineering. This should be considered in the design of the system and in supporting legislation.

Given the identification-authentication concerns in E–Verify, it is important to distinguish between an identifier and an authenticator. Both have very special technical meanings and are often confused. In my written testimony I described the differences between identification and authentication. In brief, an identifier is a label associated with a person. An authenticator provides a basis to believe that some identifier accurately labels the person.

Within the context of E–Verify, the self-check pilot system, which we heard of a few minutes ago, it authenticates individuals by requesting information that can easily be obtained via the white pages and public tax records by individuals other than the holder of the Social Security number. The requested information is not sufficient for proper authentication. The pilot allows unauthorized individuals and fraudsters to access the system, allowing them to check stolen information to determine if it can be used to craft a new fraudulent identity to obtain employment. As currently configured, mandated use of E–Verify would encourage an increase in computer fraud, abuse and identity theft.

Additionally, to protect the innocent, employers who take action on nonconfirmation returns without informing applicants and pro-

viding them an opportunity to appeal and correct mistaken records must face strong penalties. Exceptions for cases of natural disaster or emergency should also be built in. Under such circumstances, requirements should be waived or suspended when seeking new employment.

In the time remaining, I will highlight a few recommendations from my written testimony, again from a systems engineering perspective. First, it is critical to eliminate the weaknesses in E–Verify and objectively audit the pilot before it is scaled up or extended to individuals for anything other than employment. Lack of proper system validation and verification will almost certainly lead to cost and schedule overruns, system breakdowns, intrusions and perhaps obsolescence.

Second, it is imperative that vulnerabilities be examined and risks addressed to protect the system as well as the identity of the individual whose information is contained within it.

Third, adopting biometric technologies as a solution to the E–Verify authentication problem would be premature and is unlikely to solve some of the fundamental problems with the current system.

In conclusion, we are encouraged by your attention to these issues, and the computing professionals that I represent stand ready to help you in your efforts.

Thank you for your attention.

Chairman JOHNSON. Thank you, ma'am. I appreciate your comments.

[The prepared statement of Ms. Antón follows:]

This testimony is embargoed until April 14th at 2:00 p.m.

Testimony before the House Committee on Ways and Means Subcommittee on Social Security:
Social Security Administration's Role in Verifying Employment Eligibility

14 April 2011

Statement of
Ana I. Antón, Ph.D.

Professor
North Carolina State University

Director
CSC Policy and Compliance Initiative &
ThePrivacyPlace.Org

Vice Chair, USACM

Introduction

Thank you Chairman Johnson and Ranking Member Becerra for the opportunity to testify.

I am a professor at North Carolina State University in the Department of Computer Science in the College of Engineering. In addition, I serve as Director of ThePrivacyPlace.Org, a privacy research center collaboration between NC State University and Purdue University. I also serve on several industry and government boards of technical advisors, including the Department of Homeland Security's Data Privacy and Integrity Advisory Committee. A brief biography is in Appendix A.

This statement represents my own position as well as that of the Association for Computing Machinery's (ACM) U.S. Public Policy Council (USACM), of which I serve as vice-chair. With over 100,000 members, the Association for Computing Machinery (ACM) is the world's largest educational and scientific computing society, uniting computing educators, researchers and professionals to inspire dialogue, share resources and address the field's challenges. USACM serves as the focal point for ACM's interaction with U.S. government organizations, the computing community, and the U.S. public in all matters of U.S. public policy related to information technology.

The stakes are high for E-verify. This largely automated system—currently in pilot operation—may ultimately serve as the single most important factor in determining whether a person may be gainfully employed in the United States. As such, it must take into account complex issues around identity management, security, accuracy, and scalability, among others. These are not solely technology issues. Computing technologies are powerful and can play a role in employment verification, but even the most modern technologies have limits. Congress, the Executive Branch, and possibly the Judicial Branch must make decisions on risks and tradeoffs on complex policy issues. Should the E-Verify pilot system continue to be expanded, careful, balanced and informed consideration should guide both the technical architecture and policy decisions. This statement is intended to inform the committee on the computing community's perspective on these challenges. In particular, I wish to make three points on the key technology and policy issues:

1. E-Verify must accurately identify and authenticate the individuals and employers authorized to use the system in a layered, trustworthy manner before it is widely deployed. Although no authentication technology is perfect (including biometrics), effective approaches to identity management are layered and do not rely on one point of identification. Unauthorized accesses to the E-Verify databases would compromise the identities of anyone whose information it manages, including American citizens and permanent residents. The current pilot does not provide this level of accuracy.

2. Proof of success with a pilot is required before extensively scaling any software system. The E-Verify system should not be scaled up until certain weaknesses are eliminated and the pilot is objectively audited against established metrics for success. E-verify should not be

extended to verify individuals' status for anything other than employment until after the system has been fully deployed and the impact and implications of any such extensions have been carefully considered.

3. Complex systems (such as E-Verify) are fallible and often misused or repurposed in ways that violate sound principles of security and good software engineering. Adequate, appropriate alternative mechanisms are crucial for handling unforeseen challenges and errors after the system is deployed. Even with initial pilot system success, scaling complex software systems may result in cost and schedule overruns, system breakdowns, intrusions and even obsolescence. Moreover, mission creep adds to the complexity of software systems, increasing the risk of the problems mentioned above. It also undermines the principle of data minimization as recommended in the USACM Privacy Recommendations (see Appendix C).

My testimony covers software engineering and security best practices that are relevant given our examination of the proposed expansions of the E-verify system. In this testimony, I describe several challenges for developing a system that securely verifies employment eligibility. Specifically, I discuss:

- alternative approaches to managing identity and authentication;
- plausible technical solutions for validating system pilots before proceeding to make it a permanent system; and
- objective, technical recommendations for this committee to consider as it moves forward with its efforts to verify employment eligibility in the United States.

E-Verify Background

The E-Verify pilot system is designed to allow employers to determine whether an employee is eligible to work in the United States, using information reported in an employee's Form I-9 (Employment Eligibility Verification). Before the widespread use of digital technologies, the documents used to verify employment eligibility represented little threat of being a source of large-scale identity theft or fraud. However, now such documents are digitally scanned and incorporated into massive databases. If not properly managed the databases underlying E-verify could facilitate identity fraud and introduce significant risks.

Administered the by the Department of Homeland Security and the Social Security Administration, E-Verify is being used by over 238,000 employers, yielding 16 million queries[1] during 2010 the Fiscal Year. E-Verify is mandatory for some employers with federal contracts or subcontracts that contain the Federal Acquisition Regulation (FAR) E-Verify clause and employers in certain states.

[1] DHS E-Verify Web Page: http://www.dhs.gov/files/programs/gc_1185221678150.shtm

From a technical standpoint, difficulties in a pilot system's implementation provide reasons for concerns that would apply even more strongly if the pilot system's scale is widely expanded. These should be addressed before any further expansion of the pilot. Moreover, the significance of failures experienced with the pilot cannot be dismissed as acceptable and simply imposing additional mandatory training does not comprehensively address the problems. For example, a January 2010 audit report by the Inspector General[2] showed that the Social Security Administration itself failed to comply with the E-Verify Memorandum of Understanding (MoU) requirements. Specifically, the SSA: verified the employment eligibility of 26 existing employees because they had applied for new positions within the agency; erroneously verified the eligibility of 31 volunteers who were not employees; and verified the eligibility of at least 18 job applicants who were never hired—a clearly prohibited use. Moreover, 49% of SSA hires were not verified during the required 3 days prior to hire time period. Finally, the eligibility of 19% of the new SSA hires was never verified.

In December 2009, the Westat Corporation conducted an evaluation of the E-Verify system for the Department of Homeland Security[3]. Westat reported that 54 percent of the illegal immigrants checked through E-Verify were incorrectly deemed eligible to work because they are using stolen or borrowed identities[4]. This finding shows that the E-Verify pilot system is not able to detect identity theft and/or employer fraud.

The E-Verify pilot results from the SSA Inspector General and the Westat evaluation do not instill a sense of confidence that the pilot is ready to be promoted to a permanent larger-scaled system. Before scaling up, software engineering best practice requires a successful small-scale pilot and only when such success is achieved should one proceed to a larger-scale permanent system.

Scientific validation—evidence that a software system successfully meets pre-specified criteria with metrics—is critical before proceeding. The E-Verify pilot system includes policies and processes required for it to operate and perform as intended. However, flaws in business processes and factors external to the system can undermine an otherwise effective technology. As currently designed, there is no way for E-Verify to prevent any of the problems mentioned in the Inspector General audit report—improving, scaling and expanding the underlying technology will not solve the problems associated with erroneous verifications as system development continues.

A sense of urgency in our nation's efforts to protect its citizens can sometimes lead to taking shortcuts without proper validation and testing. Just last week, the Transportation Security Administration's (TSA) failure to scientifically validate their SPOT (Screening of Passengers by Observational Techniques) program before deployment was the subject of a hearing held by the

[2] The Social Security Administration's Implementation of the E-Verify Program for New Hires, Audit Report, The Office of the Inspector General, January 2010. http://www.ssa.gov/oig/ADOBEPDF/A-03-09-29154.pdf
[3] Westat Corporation, Findings of the E-Verify Program Evaluation (Rockville, MD), December 2009.
[4] Tim O'Coin, Study: E-Verify failure rate over 50%, WPRI.com Eyewitness News, February 25, 2010. http://www.wpri.com/dpp/news/local_news/providence-study-finds-everify-database-fails-to-catch-illegal-workers-over-50-percent-of-the-time.

House Science and Technology Committee's Subcommittee on Investigations and Oversight[5]. Validation and testing is especially important in high-value systems such as E-Verify. Compromises to these systems would likely result in massive identity fraud, which would be more damaging given the planned and proposed expansions to the E-Verify pilot system. Rushing deployment without fully addressing problems would also likely result in costly mistakes and overruns in implementation, which are not desirable at any time and especially not at a time of significant Federal budget deficits.

Several enhancements have been made to E-Verify since it was first introduced[6]. Since May of 2008, the Integrated Border Inspection System has provided real-time arrival and departure information for non-citizens. In February of 2009, DHS began sharing passport data and photographs with the Department of State (based on DoS records) as governed by a memorandum of understanding[7]. Both of these enhancements sought to reduce the number of mismatches in E-Verify. Such enhancements[8] are useful in that they are targeted and purposeful, serving to improve the system's ability to accurately verify individuals.

The new E-Verify self-check pilot allows workers to use the system to check their status without notifying employers or potential employers. Ensuring the system continues to only provides a simple "yes" or "no" response without revealing anything further is a step a step toward preserving the security of the system. However, we observe that there may be a potential for abusing self-check protection. For example, E-Verify could offer an unintended service to fraudsters, allowing them to validate identity data before attempting identity theft. The self-check pilot is available in six states (Arizona, Idaho, Colorado, Mississippi, Virginia, and the District of Columbia).

USACM reviewed the self-check pilot system[9] and noted that the system requested information that can easily be obtained via public records (e.g. county tax records) by individuals other than the holder of a given SSN[10]. Attention should be paid to whether the "what you know" questions for the E-Verify self-check pilot" are well-designed, meaning usable to the individual wishing to check their records, but unusable to outsiders. Our concern here is about the information that is being requested because it is not sufficient for proper authentication. The current selection of questions about the year in which you purchased your home, how much it cost and the age range

[5] Subcommittee Examines Behavioral Science Used by TSA to Screen Potential Security Risks, April 6, 2011. http://science.house.gov/press-release/subcommittee-examines-behavioral-science-used-tsa-screen-potential-security-risks

[6] "Priorities Enforcing Immigration Law," http://www.uscis.gov/portal/site/ uscis/ menuitem.5af9bb95919f35e66f614176543f6d1a/?vgnextoid=d3ace7c336c60210VgnVCM1000004718190aRCRD&vgnextchannel=8a2791daff2df110VgnVCM1000004718190aRCRD

[7] This memorandum of understanding was signed in December of 2008.

[8] Additional planned enhancements to E-Verify include: incorporation of Student and Exchange Visitors Information System (SEVIS) data, integration of DMV photographs (to date, no state has agreed to add its driver's license data to E-Verify), and allowing citizens to lock/unlock their SSNs for E-Verify purposes.

[9] Given that non-property owners are given a different set of questions, our tests can only be considered illustrative rather than comprehensive.

[10] In our experience, the self-check system requires an individual to submit his or her name, address, SSN and date of birth to access the system—information that is easily available to individuals wishing to verify someone else's employment eligibility. The secret questions cannot truly be considered "secret" given that the answers to these questions are available via public records: home addresses are available via whitepages.com; age range is available via whitepages.com; county or city in which one resides is available via Google maps; price paid for a home is available via local county tax records websites.

of the head of household, does not instill much confidence in this regard nor does the use of a "uscis.gov" URL for the "non-DHS, independent assurance service that uses non-governmental information to generate questions." Ultimately, we want citizens to be able to do their own self-checks; however, we must consider whether there are risks associated with granting unauthorized individuals access to the system or with allowing fraudsters to check the information they've stolen in an attempt to determine if they can use the information to craft a new, fraudulent identity.

Mission Creep

Mission creep—also called repurposing or piggybacking—in software engineering refers to efforts to expand a system beyond its original goals after initial success. Mission creep introduces substantial risks associated with cost and schedule overruns[11], system breakdowns, and intrusions as new applications are developed and "linked" to existing systems without proper validation or architecting, resulting in (for example) brittle and vulnerable databases. The ACM U.S. Public Policy Council has been unable to obtain E-Verify pilot's pre-defined metrics for success. If criteria for success with specified metrics and thresholds for success have not been defined, then software engineering best practice suggests that the system should not continue to be extended, enhanced, or authorized to become a permanent system. As of December 2010, USCIS and SSA had not yet "established a written service-level agreement that describes acceptable and unacceptable SSA service levels required to support the E-Verify program"[12]. Defining these requirements is critical for establishing success criteria for the E-Verify program before scaling the system up.

Given the currently planned enhancements to E-Verify as well as the proposed legislation to expand the usage of E-Verify[13], one can envision years of continual pressure to expand its mission. Linkages to other databases and applications, whether for authorizing home loans or for denying certain services to deadbeat parents, will place tremendous pressure on a system designed for one specific purpose. In his 2007 testimony to this same subcommittee[14], Peter Neumann referred to this practice as "piggybacking," noting that each time a system or database is piggybacked it increases the system's exposure as well as the danger that the data integrity will be compromised and/or data will be leaked. Moreover, when data integrity has already been compromised, i.e. there are errors in the original database, those errors will then be propagated to the piggybacking systems. Thus, the potential impact of errors on individuals is progressively increased.

---

[11] F.D. Davis and V. Venkatesh. "Toward pre-prototype user acceptance testing of new information systems: implications for software project management," *IEEE Transactions on Engineering Management*, 51(1), pp. 31 - 46, February 2004.
[12] Federal Agencies Have Taken Steps to Improve E-Verify, but Significant Challenges Remain, GAO Report #GAO-11-146, December 17, 2010.
[13] There are three specific bills that seek to expand E-Verify: (1) H.R.693: The E-Verify Modernization Act of 2011, (2) H.R.695: Legal Eligibility for Granting A Loan Act of 2011, and (3) H.R.282: To require Federal contractors to participate in the E-Verify Program for employment eligibility verification.
[14] Testimony of Peter G. Neumann on the Security and Privacy in the Employment Eligibility Verification System (EEVS) and Related Systems, House of Representatives Committee on Ways and Means Subcommittee on Social Security Thursday, June 7, 2007.

We will note that past experience with large systems IT procurement and engineering has shown that adding new missions to existing systems results in delays, errors, and cost overruns. This has been the experience with procurements for systems in the Department of Defense, IRS, FBI, FAA, and many other Federal agencies. This also can introduce new vulnerabilities. Thus, we recommend extreme caution in any expansion of the E- Verify system beyond its original design.

Authentication and Access Control

In addition to mission creep, one must consider the risks associated with authentication and access control.

An *identifier* is a name or other label that can be used to uniquely select a particular person within a specific group or context. For example, my SSN identifies me within the group of U.S. Social Security participants. But someone who knows my SSN is not necessarily me. Many other people in many contexts have valid access to my SSN.

Authentication is the process of verifying that an identifier is valid and associated with a particular identity. There are three traditional categories of authenticators: knowledge-based ("what you know," e.g., a password), object-based ("what you have," e.g., an RFID token or a driver's license), and ID-based ("what you are," e.g., a biometric such as a fingerprint).[15] There are strengths and weaknesses in each form of authenticator; these are discussed in more detail in USACM's short tutorial on authentication, attached as Appendix B.

Government systems that rely on the SSN as an identifier and authenticator are risky. Knowledge of a SSN (or any other universal identifier) is not sufficient to reliably authenticate any party in this transaction, but this use is commonplace. Authentication needs to be performed in a way that someone eavesdropping on a transaction cannot then masquerade as either the individual or the government service system for any operation. Moreover, the authentication should not center on questions whose answers are easily obtained by a fraudster via public records that are available online (e.g. property tax records). In this regard, the E-Verify self check implementation is troubling.

One form of identity management and access control that is being proposed is the use of biometric solutions. Given currently available technology, the idea of a tamper-proof identity card is a myth. No identification is completely tamper-proof or secure because perfect security is simply not possible. For example, an attacker could steal or counterfeit the ID, etc. Ultimately, security is about risk analysis. Thus, it is important to focus on risk-based approaches to improving identification, such as counterfeit-resistance.

[15] O'Gorman, L. Comparing Passwords, Tokens, and Biometrics for User Authentication. *Proceedings of the IEEE*, Volume 91, pp. 2021-2040, 2003.

Biometrics

Biometric technologies have been proposed by some vendors as a method to more accurately identify individuals in a manner that cannot be forged. These technologies offer several benefits. In particular, physical attributes are extremely difficult to forge or fake; using numerous attributes provide a high likelihood of uniquely identifying an individual, and biometrics are difficult to forget or leave at home when a token, card or fob is not required. However, there are several distinct disadvantages: biometric readers are expensive and some have significant failure rates, biometrics are irreplaceable—once collected, the information can never be recovered without trusting the collector, biometrics protecting high value objects or systems pose a threat to the owner (a thief may be willing to cut off a thumb, for example), and physical attributes change over time (a hand print taken with a particular ring may not work on a day when the owner forgot to wear the ring, and fingerprints become less distinct as one ages or due to years of manual labor).

Generally, there are two approaches to biometric identification technologies: a distributed token approach and a centralized database approach.

Distributed Token Approach[16]. In this approach, subjects are given a card or a token similar to a key fob that has a biometric reader on it. The reader is provisioned by imprinting the subject's biometric into it in a secure fashion. Once imprinted, the token can be activated by the subject by re-scanning their biometric. At that point the biometric sends its identification code to a reader. There are several advantages to this approach: there is no central repository containing biometric data, tokens can be programmed to use a new identification code if the old one becomes invalid (thereby avoiding the 'irreplaceable biometric' problem), different biometrics can be used in the same system depending on the readers (e.g. one person can use her thumb, another can use his index finger, another could use a vein/artery pattern in her hand). Finally, this approach is inherently secure because it is built as a two-factor authentication system—you have to use something you are (your biometric) as well as something you have (your token/reader device). This is an expensive approach, however, because everyone must be given a token upon provisioning. Although this approach still requires a central database, the database stores identification codes rather than biometrics. Within the context of E-Verify, an advantage for the government is that it would not require a database of biometric identifiers to be maintained. In fact, even if the biometric card, token or fob is lost or stolen, no biometric data is recoverable because its contents are encrypted. This is a huge benefit to security and privacy. However, a disadvantage of this kind of biometric technology is that it would require all E-Verify enrolled employers to purchase a biometric reader or scanner, introducing its own risks such as hardware failure.

[16] In a Distributed Token Approach a new biometric ID is first provisioned by identifying and authenticating and individual—the individual then receives a biometric token such as a card or key fob, which is imprinted with the individual's biometric. The token captures and encrypts biometric markers (e.g. a thumb print) in much the same way as a password is automatically hashed upon entry. This is important because if the token is lost, then no biometric data is compromised. Once a biometric token is imprinted, it is tested against a standard identification/authentication/authorization process to ensure accuracy. If the biometric marker is a hand print or thumb print, then the token owner would swipe their hand or thumb across a reader and the scan is automatically captured, encrypted, and compared with the biometric stored on the device. If it matches, then the token identifies itself through a secured channel to a device reader.

Centralized Database Approach. In this approach, biometric information is stored by an organization or the government in a remotely accessible database that is used to perform verifications. Within the context of E-Verify, one might envision a database that contains a "white list" of individuals who are authorized to work. The US-VISIT system employs such a database-only approach, but it compares biometrics against a "black list" of terrorists and other bad actors[17]. This black list approach would be less intrusive from a privacy standpoint, but its feasibility would be questionable given the number of individuals who wish to work in the U.S. but are ineligible to do so. It is easy to envision pressure to design E-Verify so that it would be capable of the same sort of comparison. Our USACM privacy principles emphasize that the least privacy-invasive alternative should always be sought in the design of any system.

A centralized database approach is less expensive than the distributed token approach because biometric readers can be stationed at access points and it does not require giving the subject a card or token. However, this approach requires the government to be trusted to protect irreplaceable biometric data and to not misuse biometrics for purposes other than the one for which it was collected. In addition, biometric databases are high-value assets and targets for criminals seeking to construct an ID. Moreover, this is a single factor authentication approach and, thus, it is a single point of failure.

Maintaining Complex Systems

Given that mistakes can have serious human impact, any laws or rules should be carefully crafted so as not to hurt innocent individuals—especially those who may be victims of identity theft. In addition, E-Verify will continue to be an attractive target for mission creep because it offers an attractive way for some groups to suggest as a mechanism to identify individuals—for now as eligible to legally work (and, if Congress allows it, to verify individuals as eligible for an increasing number of services, including home loans).

The GAO has noted that USCIS and SSA currently lack the ability to accurately estimate costs for E-Verify, thus there exists a significant risk of making poorly informed decisions and not securing necessary resources, leading to cost and schedule overruns and performance shortfalls[18]. Numerous complex software systems developed for large government programs have exceeded their budgets while producing sub-standard software. The FBI's Virtual Case File system was abandoned in early 2005 after over 700,000 lines of code were produced and $170 million dollars were spent because the system failed to meet fundamental requirements outlined years earlier by the FBI[19]. It was replaced with another software development project, called Sentinel, which was deemed by the Department of Justice to be two years behind schedule and $100

[17] Black lists in technology are intended to be complete, but it is impracticable to identify every person not eligible to work in the United States. However, an incomplete black list could still prevent known bad actors from repeatedly attempting to bypass the system.
[18] Federal Agencies Have Taken Steps to Improve E-Verify, but Significant Challenges Remain, GAO Report #GAO-11-146, December 17, 2010.
[19] http://www.justice.gov/oig/testimony/0502/final.pdf

million dollars over budget[20]. The Department of Justice is also concerned that the original requirements for Sentinel are now six years old and are likely to be outdated by advances in technology. Similar schedule and budgeting problems affected the modernization of software systems at the IRS[21] and the FAA[22]. We have no technical assurance that a software system as complex as E-Verify would be developed without similar budgeting and scheduling problems. Moreover, the December 2010 GAO Report on E-Verify notes that the pilot system remains vulnerable to identity theft and employer fraud.

Even large, highly technical, security-conscious companies that depend on their security practices for their very existence experience security violations. In January 2010, Google announced that it had several systems compromised by a cyber attack known as "Operation Aurora[23]." In addition, Adobe, Yahoo!, Symantec, and Morgan Stanley were also attacked. Last month, RSA, Inc.—the firm that invented the first public key encryption algorithm for both signing and encryption—had sensitive information related to their popular two-factor authentication product called SecurID stolen. These incidents demonstrate the kind of attacks that target significantly important system or high-value asset (such as the E-Verify database) and which will be inevitable over the course of time.

Recommendations

Here, I present two sets of recommendations. The first set of recommendations are technical in nature and address best practices in moving forward with the E-Verify pilot system. The second addresses broader public policy considerations based on experience with large, public-facing software systems.

Technical Recommendations on Best Practices for the E-Verify Pilot System

- The E-Verify pilot system should not be scaled up or extended to verify individuals for anything other than employment until weaknesses, such as those identified in the SSA Inspector General audit and the Westat Corporation evaluation, are eliminated and the pilot is objectively audited to verify pilot success. Moving forward without proper system validation and verification will inevitably lead to cost and schedule overruns, system breakdowns, intrusions and perhaps obsolescence.

- It is imperative that vulnerabilities be examined and risks addressed to protect the system as well as the identities of the individuals whose information is managed within it. E-Verify remains vulnerable to identity theft, employer fraud and may serve as a valuable tool for identity fraudsters.

[20] http://www.justice.gov/oig/reports/FBI/a1101.pdf
[21] http://news.cnet.com/IRS-trudges-on-with-aging-computers/2100-1028_3-6175657.html
[22] http://www.gao.gov/new.items/d09271.pdf
[23] http://www.mcafee.com/us/threat-center/operation-aurora.aspx

- Although it is tempting to resort to use of biometric technologies as a solution to the authentication problem posed by a system such as E-verify, it would be premature at this time. Until further testing and consideration is performed, the use of biometric methods should not be considered for the following reasons:
  - No single biometric technology is applicable to the entire population: not everyone has all their fingers, or irises, or other body parts that might be measured uniquely. DNA is present across all living humans, but is the same in identical twins and triplets, and is expensive and slow to analyze.
  - Most biometric measures may change with time. Even fingerprints may wear away from age, medication, or labor (e.g., bricklayers and some chemical workers).
  - No large-scale studies have been performed on populations as large as the U.S. to determine the rates of collision and accuracy of biometric identifiers, or of the accuracy of biometric measurement devices.
  - In the event of some future compromise of any large biometric database of U.S. citizens there would be no way to "reset" the biometrics to start over if a way was found to forge their use.
  - Biometric collection technologies are susceptible to privacy abuses[24].
  - Many people are uncomfortable with biometric information being collected or used, and perceive it as an invasion of privacy.

Additional Recommendations Based on Experience with Large Public-Facing Systems

- Careful consideration is critical before mandating use of E-verify because mandatory use would basically also mandate an increase in computer fraud, abuse, and identity theft. If E-verify were to be made mandatory for every employer, it would be a burden on small employers and/or a major security problem. It would require small employers to install Internet connectivity that they might not have, including Internet ISP subscriptions from some rural and remote areas where such service would be expensive. Furthermore, most small businesses do not have either the expertise or the resources to properly secure those systems against viruses, botnets, and intrusions. Thus, their systems would be at risk, and the information they would enter about prospective employees would be at risk of exposure for identity theft.

- There should be strong penalties for employers taking action on non-confirmation returns without informing applicants, providing them an opportunity to appeal and correct mistaken information in the records. Otherwise, the system may be used as an excuse for employment discrimination. Because the E-Verify system is certain to have errors, failures, and be subject to problems verifying some special cases (e.g., victims of identity theft), it is all too

[24] Shimon Modi and Eugene H. Spafford; Future Biometric Systems and Privacy; chapter in Privacy in America: Interdisciplinary Perspectives; edited by William Aspray and Philip Doty; Scarecrow Press, Inc.; 2011.

easy for it to be used as an excuse that "the computer said you aren't eligible" to deny someone's application or status without investigating complaints of error.

- Exceptions for cases of natural disaster or emergency should be built in if E-Verify is mandated. For example, if there is another Hurricane Katrina where all personal records and identification is lost on a wide scale, or if an individual family loses all their possessions in a fire or tornado, presenting appropriate ID may be impossible. Requirements should be waived or suspended when seeking new employment under such circumstances.

Acknowledgments

I am particularly grateful to Aaron K. Massey, Cameron Wilson (ACM Director of Public Policy), David Bruggeman (ACM Public Policy Analyst), Eugene H. Spafford (USACM Chairman, and Professor at Purdue University), Stuart Shapiro, Jeremy Epstein, Jessica Young, Ramya Gopolan, Peter Swire, Daniel Dean, Lane Surreat, Alan Sheridan, Vincha V Bhat, Prachi Nandgaonkar, and many other members of ACM and USACM for their generous help in my preparing this testimony.

About USACM

USACM is the U.S. Public Policy Council of the Association for Computing Machinery (ACM). USACM members include leading computer scientists, engineers, and other professionals from industry, academia, and government. (http://www.acm.org/usacm)

About ACM

ACM, the Association for Computing Machinery www.acm.org, is the world's largest educational and scientific computing society, uniting computing educators, researchers and professionals to inspire dialogue, share resources and address the field's challenges. ACM strengthens the computing profession's collective voice through strong leadership, promotion of the highest standards, and recognition of technical excellence. ACM supports the professional growth of its members by providing opportunities for life-long learning, career development, and professional networking.

Appendix A – Biographical Information

Dr. Annie I. Anton is a Professor of Computer Science in the College of Engineering at the North Carolina State University and Director of the Computer Science Policy and Compliance Initiative. She received her Ph.D. in Computer Science in June of 1997, with a minor in Management and Public Policy, from the College of Computing at the Georgia Institute of Technology in Atlanta. She received a BS in Information and Computer Science with a minor in Technical and Business Communication in 1990 and an MS in Information and Computer Science in 1992 (also from Georgia Tech). After one year at the University of South Florida, Dr. Anton joined the computer science department at NC State. From 2005-2006 she was a visiting faculty (sabbatical) scholar at Purdue University's CERIAS. In 2008 she chaired the NC State Public Policy Task Force and she is currently chairing the NC State University Reappointment, Promotion and Tenure Committee.

She was awarded an NSF CAREER Award in 2000, named a CRA Digital Government Fellow in 2002, nominated and selected for the 2004-2005 IDA/DARPA Defense Science Study Group, and received the CSO (Chief Security Officer) Magazine "Woman of Influence in the Public Sector" award at the 2005 Executive Women's Forum. In 2006, she was honored with an award for "Most Influential Paper of ICRE 1996" at RE'06 for her 1996 paper entitled "Goal-Based Requirements Analysis". Her 1994 IEEE Software paper with co-authors Colin Potts and Kenji Takahashi was ranked the #10 most highly cited IEEE Software paper in its 25th Anniversary issue. She is a former associate editor of *IEEE Transactions on Software Engineering*, and former cognitive issues area editor for the *Requirements Engineering Journal*, and a member of the International Board of Referees for *Computers & Security*. She is a member of the International Association of Privacy Professionals, a member of Omicron Delta Kappa (OΔK) National Leadership Honor Society, a senior member of the IEEE as well as Vice Chair of the ACM U.S. Public Policy Council.

Anton currently serves on various boards: the U.S. DHS Data Privacy and Integrity Advisory Committee, the CRA Board of Directors, an Intel Advisory Board, the Future of Privacy Forum Advisory Board, the DARPA ISAT Study Group, and is corporate secretary for Trekking For Kids, Inc. She is a former member of the Microsoft Research University Relations Faculty Advisory Board, the CRA-W, the NSF Computer & Information Science & Engineering Directorate Advisory Council, the Distinguished External Advisory Board for the TRUST Research Center at U.C. Berkeley, the Advisory Board for the Electronic Privacy Information Center in Washington, DC, the Georgia Tech Advisory Board (GTAB), and Georgia Tech Alumni Association Board of Trustees. Dr. Anton is director of ThePrivacyPlace.Org (http://theprivacyplace.org). Her URL is: http://www.csc.ncsu.edu/ faculty/anton.

Appendix B – Understanding Identity and Identification

Professionals who work with issues of security and control use some terms to precisely describe access to resources and naming. These same terms have usage in general language, but the words frequently are used imprecisely and even misleadingly. When describing how security in information systems operate, and when formulating regulations or laws, it is important that these terms are understood and used precisely.

The purpose of this short document is to describe these important terms for readers who are not familiar with the more formal definitions. These related terms are *identification*, *authentication*, and *authorization*. Related concepts include *uniqueness* and *biometrics*.

Terms

Identification is associating a distinguishing label (*identifier*) with something within a specific group or context. You can identify someone by getting both their label and the context of that label. An ID card can provide both the name (e.g. "John Smith") and the context (e.g., "licensed driver"). Identification can also occur by providing only the context or group name, such as identifying oneself as a police officer, a student, a graduate of West Point, or a member of Congress by wearing an appropriate badge, uniform, or class ring. The reliability of an identification depends on the confidence that the distinguishing label and context actually apply to the individual in question.

Note that even when identification is reliable – and it often is not – it does not imply anything beyond being able to distinguish among items or people. Identification can be used to determine if someone is a member of a group or not, or among members of the group. If someone were to identify herself as "Snow White," that is an identification if she uses it consistently. In the context of a Halloween party or an Internet chat room, that may be a logical label to adopt.

A key concept is that identification does not need to be a standard name. It can be a nickname, a login, or a simple description, such as "I am the tallest one here" or "I am the one with red hair." Those are means to distinguish one person from another in a particular group context.

People are most often identified in social situations by their names. In the United States, these names are usually composed of a first (given) name, one or more middle names (usually), and a last (family) name. In other countries, names may be a single word, or everyone may have a common family or middle name.

Uniqueness is when multiple items do not have the same identifier. Human names are seldom unique across a large enough population. For instance, there are many, many people named "John Smith" in the USA. If we also consider ancestors, then there may be even more individuals who have been associated with the same identifier (name).

We can further qualify an identifier to make it more specific and less likely to be a duplicate of another identifier. For instance, someone could be "John Smith who was born April 1, 1952 in Boise and whose mother was named Matilda." However, we cannot always be certain this is unique, and it is unwieldy to use in formal documents. Thus, we commonly use an artificial identifier that is generated and assigned in a manner that ensures that it is unique within context. For instance, Social Security numbers are supposed to be assigned without reuse, making them theoretically unique. Other identifiers (e.g., driver's license numbers) are similarly generated to provide uniqueness.

Authentication is the process of verifying – to some desired level of confidence – that a claimed identifier is valid and actually associated with a particular item or person. Often, this validation is performed by one or more persons inspecting the identification and authenticator(s). The authenticators can also be examined by some technical means, such as a login program or a badge reader connected to a computer.

Authenticators of people are typically some combination of "something known," "something possessed," and "something about (structural)" the person. These items have been previously registered with the persons or organizations performing the authentication. Additional factors can also be used, such as physical location, recognition by human or canine guards, and so on.

- *Something known* is a secret or a fact that is unlikely to be known to an impostor. Passwords, when properly chosen and protected, are this form of authenticator. In many old combat movies, the spy is exposed because he doesn't know which team won the World Series the previous year – this is another form of "something known" as a group authenticator. Many companies use items such as "mother's maiden name," "birth date" or "social security number" as authenticators, but this is bad practice as those items are often easily discovered facts: Many of these items are public information as a matter of law or custom.

- *Something possessed* is a distinguishable token or a key that matches a counterpart. A license issued by a government agency is a form of token. Another example from an old movie is the dollar bill or playing card that is ripped raggedly in half – the two halves are kept and joined together to *mutually authenticate* two parties.

- *Something about* (structure) the object or person being authenticated. We can examine something physical about the person we wish to identify, such as a fingerprint, or the pattern of blood vessels inside the eye. If the comparison of a person's distinguished characteristic is automated, then it is known as a *biometric*. A current location may also be used for authentication, such as GPS coordinates, telephone caller-id or computer network address.

Using a combination of authenticators is known as *multi-factor authentication*.

Authorization is the granting of rights (verb) or the grant itself (noun). Generally, one authorizes an authenticated party. *Permission* is used by some people as a synonym for authorization.

An example

Consider a scenario involving a person who wishes to enter a guarded building. When the person approaches the building to enter, a guard stops him to verify that he can enter. The person produces an *identification* card (something possessed) issued by a trusted authority (the context). The guard compares the picture on the ID with the face of the person, and causes him to put his fingers on a scanner (a biometric). These checks confirm that the person is the one identified by the card. She has been instructed that anyone with a valid blue card is allowed to enter, but without a cell phone, so she allows the person to pass after determining that he does not have a cell phone.

Note that this is use of multi-factor authentication, and the identification is based on group membership ("people with a valid blue badge") – no specific name or ID number is required. Permission to enter is the authorization involved. A further element of access control that is not based on identity or authentication is also involved: there is no authorization to carry a cell phone in.

There are many potential weaknesses in this system as described. The system can be redesigned to prevent the weaknesses, but defensive measures may be too expensive or cumbersome to be worth the effort given both the likelihood of the threats occurring and the value of what is behind the door. Examples of weaknesses include:

- The picture on the card may be old and the guard makes a false negative authentication: she refuses to allow the authorized person to pass.
- The guard may be overpowered or bribed so that unauthorized people enter.
- The card has been altered from a valid card — the color has been changed, or the original holder's photograph and fingerprints have been replaced by this impostor.
- The cards are made to published standards without adequate safeguards: this is a forged card made by a well-informed and sophisticated attacker.
- The attacker has stolen the card, disguised himself as the cardholder, and donned fingerprint caps that fool the scanning machinery.
- The guard is unable to recognize a disguised cell phone.

- Someone pretending to be a law enforcement officer, in uniform, orders the guard to let him pass or he will arrest her for obstructing justice. She complies.
- If too many people arrive in a short time, the guard may not be able to process them in a timely fashion, and someone is either denied access incorrectly or slips in unnoticed.
- The guard may fall ill and leave her post, leaving the door locked or unlocked for subsequent visitors.
- A first-time visitor has no way of knowing that this is really a legitimate guard and the right door.

Additional Notes

1. As illustrated by the last point in the previous example, the problem of authentication is bidirectional — all parties in the transaction need some level of assurance that they know the identities of the other parties. This is one reason why *phishing* succeeds: the customers enter their authenticating information, but the other party (the purported merchant) is not strongly authenticated to the customer.
2. It is possible to have authentication and authorization without specific identification. For instance, producing an *authentic* $20 bill provides authorization to make a purchase for something up to $20 in cost. It is not a requirement to *identify* the purchaser beyond being a member of the group who has cash.
3. Knowing precise, authentic identity **does not disclose intent.** Knowing the name of everyone who enters a building or boards a plane does not mean that they will be well-behaved. Mohamed Atta's Florida driver's license and picture were legitimate and examined when he passed through airport security on 9/11/2001. Most identification checks instituted in the wake of 9/11 perform at most a weak security function because there is poor (or no) authentication, and even when the identity is known it does not prove anything about intent.
4. Social security numbers are not supposed to be reused. However, numerous recorded cases of SSN duplication make the use of these numbers as unique IDs problematic.
5. Most biometrics have been developed and tested for authentication of a claimed identity, not for performing the identification itself; fingerprints are a notable exception. Insufficient experience has been gained with both physical features and biometrics to know error rates over large populations. By example, given the data that John Smith is 6'1" tall, has brown hair and green eyes, we can determine with some confidence whether a person in the room claiming to be John is actually John. However, given that same information and a crowd of people in a football stadium, we cannot be certain that

we can uniquely identify John if he is present. Almost certainly, we will also make many false positive identifications. The same problems may exist with automated biometrics such as measuring facial features or hand geometry.

6. We know that every potential biometric has deficiencies. Not everyone has valid fingerprints over their entire lives, twins and triplets have the same DNA, and so on. People with special interests in some technologies have made unsupported claims about the performance of certain biometrics.

7. Most organizations use weak authenticators. In part, this is because most people are poor at remembering items such as long passwords and multiple ID numbers. As noted, use of authenticators such as mother's maiden name, social security number, or other such items is poor practice because those items can be easily found for many people.

8. Every instance where identifiers and authenticators are to be used should be carefully analyzed to determine strengths and weaknesses. This includes the value of what is being protected, and the consequences of false positives (authenticating an incorrect identity) and false negatives (failing to authenticate a valid identity).

9. As noted, identification and authentication mechanisms depend on context. Any security protocol is only as strong as the weakest element.

Appendix C – Privacy Policy Recommendations

USACM Policy Recommendations on Privacy

BACKGROUND

Current computing technologies enable the collection, exchange, analysis, and use of personal information on a scale unprecedented in the history of civilization. These technologies, which are widely used by many types of organizations, allow for massive storage, aggregation, analysis, and dissemination of data. Advanced capabilities for surveillance and data matching/mining are being applied to everything from product marketing to national security.

Despite the intended benefits of using these technologies, there are also significant concerns about their potential for negative impact on personal privacy. Well-publicized instances of personal data exposures and misuse have demonstrated some of the challenges in the adequate protection of privacy. Personal data — including copies of video, audio, and other surveillance — needs to be collected, stored, and managed appropriately throughout every stage of its use by all involved parties. Protecting privacy, however, requires more than simply ensuring effective information security.

The U.S. Public Policy Council of the Association for Computing Machinery (USACM) advocates a proactive approach to privacy policy by both government and private sector organizations. We urge public and private policy makers to embrace the following recommendations when developing systems that make use of personal information. These recommendations should also be central to any development of any legislation, regulations, international agreements, and internal policies that govern how personal information is stored and managed. Striking a balance between individual privacy rights and valid government and commercial needs is a complex task for technologists and policy makers, but one of vital importance. For this reason, USACM has developed the following recommendations on this important issue.

RECOMMENDATIONS

MINIMIZATION

1. Collect and use only the personal information that is strictly required for the purposes stated in the privacy policy.
2. Store information for only as long as it is needed for the stated purposes.
3. If the information is collected for statistical purposes, delete the personal information after the statistics have been calculated and verified.
4. Implement systematic mechanisms to evaluate, reduce, and destroy unneeded and stale personal information on a regular basis, rather than retaining it indefinitely.

5. Before deployment of new activities and technologies that might impact personal privacy, carefully evaluate them for their necessity, effectiveness, and proportionality: the least privacy-invasive alternatives should always be sought.

CONSENT

6. Unless legally exempt, require each individual's explicit, informed consent to collect or share his or her personal information (*opt-in*); or clearly provide a readily-accessible mechanism for individuals to cause prompt cessation of the sharing of their personal information, including when appropriate, the deletion of that information (*opt-out*). (NB: The advantages and disadvantages of these two approaches will depend on the particular application and relevant regulations.)
7. Whether opt-in or opt-out, require informed consent by the individual before using personal information for any purposes not stated in the privacy policy that was in force at the time of collection of that information.

OPENNESS

8. Whenever any personal information is collected, explicitly state the precise purpose for the collection and all the ways that the information might be used, including any plans to share it with other parties.
9. Be explicit about the default usage of information: whether it will only be used by explicit request (opt-in), or if it will be used until a request is made to discontinue that use (opt-out).
10. Explicitly state how long this information will be stored and used, consistent with the "Minimization" principle.
11. Make these privacy policy statements clear, concise, and conspicuous to those responsible for deciding whether and how to provide the data.
12. Avoid arbitrary, frequent, or undisclosed modification of these policy statements.
13. Communicate these policies to individuals whose data is being collected, unless legally exempted from doing so.

ACCESS

14. Establish and support an individual's right to inspect and make corrections to her or his stored personal information, unless legally exempted from doing so.
15. Provide mechanisms to allow individuals to determine with which parties their information has been shared, and for what purposes, unless legally exempted from doing so.
16. Provide clear, accessible details about how to contact someone appropriate to obtain additional information or to resolve problems relating to stored personal information.

ACCURACY

17. Ensure that personal information is sufficiently accurate and up-to-date for the intended purposes.
18. Ensure that all corrections are propagated in a timely manner to all parties that have received or supplied the inaccurate data.

SECURITY

19. Use appropriate physical, administrative, and technical measures to maintain all personal information securely and protect it against unauthorized and inappropriate access or modification.
20. Apply security measures to all potential storage and transmission of the data, including all electronic (portable storage, laptops, backup media), and physical (printouts, microfiche) copies.

ACCOUNTABILITY

21. Promote accountability for how personal information is collected, maintained, and shared.
22. Enforce adherence to privacy policies through such methods as audit logs, internal reviews, independent audits, and sanctions for policy violations.
23. Maintain *provenance* — information regarding the sources and history of personal data — for at least as long as the data itself is stored.
24. Ensure that the parties most able to mitigate potential privacy risks and privacy violation incidents are trained, authorized, equipped, and motivated to do so.

USACM does not accept the view that individual privacy must typically be sacrificed to achieve effective implementation of systems, nor do we accept that cost reduction is always a sufficient reason to reduce privacy protections. Computing options are available today for meeting many private sector and government needs while fully embracing the recommendations described above. These include the use of de-identified data, aggregated data, limited datasets, and narrowly defined and fully audited queries and searches. New technologies are being investigated and developed that can further protect privacy. USACM can assist policy-makers in identifying experts and applicable technologies.

21

Chairman JOHNSON. Mr. Fragomen, welcome. You are recognized for 5 minutes.

STATEMENT OF AUSTIN T. FRAGOMEN, JR., CHAIRMAN OF THE BOARD OF DIRECTORS OF THE AMERICAN COUNCIL ON INTERNATIONAL PERSONNEL, ON BEHALF OF THE HR INITIATIVE FOR A LEGAL WORKFORCE

Mr. FRAGOMEN. Thank you, Mr. Chairman, Ranking Member Becerra, Members of the Subcommittee. I wish to thank you for your kind invitation to share my thoughts on employment eligibility verification and the problems U.S. employers face.

Before we discuss E–Verify, I would like to acknowledge the fine job done by the U.S. Citizenship and Immigration Services in expanding and improving the program. Based on the agency's last numbers, enrollment is up to 254,000 employers, and you just heard that 98.3 percent of the queries result in automatic response within 24 hours, which shows a steady improvement over the past decade. However, the number of participants only represents about 3 percent of all employers, and scalability is still a concern.

While E–Verify has become very effective in matching a name with a Social Security number, it is not effective in making certain that the employee is who he or she claims to be on the form I–9. According to a December 2009 report, 54 percent of unauthorized workers who undergo E–Verify are erroneously confirmed as work-authorized.

E–Verify has made some progress towards solving this problem. One example is the incorporation of photographic images from green cards, Department of Homeland Security work authorization cards and U.S. passports. And we appreciate that there are plans to include driver's license data from motor vehicle departments around the country, but so far there is only one State involved in a pilot program.

Over the past 2 years, the employer community has witnessed much more scrutiny by Immigration and Customs Enforcement Agency, not that I am objecting to enforcement of the law, I think that is perfectly appropriate. But employers want certainty. Employers want to know they have a true safe harbor when they obey the law, and those are really the two cornerstones.

Under the status quo, employers do not have clear guidance on what to do when informed of a Social Security record mismatch, or when the information does not match government records, there is no assurance that the employers are not victims of identity fraud.

I believe the solution to the unauthorized employment problem and ultimately an important weapon in addressing illegal migration is reliable employment eligibility verification. Before we can eliminate false nonconfirmations in E–Verify, there must be sufficient resources allocated to the Social Security Administration to clean up its records. We also need clear guidance on what to do with Social Security number mismatches. However, we do not believe it is necessary for all employers to reverify their entire workforce.

For the system to be effective, additional steps are necessary to stop identity fraud. Matching photographs, of course, will have a positive impact, but it does not eliminate subjectivity on the part of the employer. Instead, this will require incorporating biometric technology, such as that proposed in the Johnson-Giffords New Employment Verification Act, and other comparable technology. If we can stop identity fraud, it will give law-abiding employers a safe harbor and at the same time take away the subjectivity that encourages discrimination, either deliberate or inadvertent.

Further, having an effective and reliable system would strengthen the argument for Federal preemption in immigration enforcement, something that business and immigrant rights advocates both want.

Finally, an effective eligibility program is a critical component of law enforcement filling the gaps that border control and visa tracking currently leave in the process.

Thank you for this opportunity to share my thoughts.

Chairman JOHNSON. Thank you, sir.

[The prepared statement of Mr. Fragomen follows:]

This testimony is embargoed until April 14th at 2:00 p.m.

TESTIMONY OF AUSTIN T. FRAGOMEN
BEFORE THE
HOUSE COMMITTEE ON WAYS AND MEANS
SUBCOMMITTEE ON SOCIAL SECURITY
April 14, 2011

Mr. Chairman, Ranking Member Becerra, members of the subcommittee, thank you for your kind invitation to share my thoughts and experience on the topic of employment eligibility verification, and the problems U.S. employers face concerning identity fraud.

I appear today in my capacity as chairman of the board of the American Council on International Personnel (ACIP).ACIP has been a leading voice on corporate immigration compliance for almost 40 years. Our membership consists of over 220 of the nation's largest employers across all industries, including financial services, technology, health care, manufacturing, entertainment, higher education, and non-profit research.

Since 2007, ACIP and the Society for Human Resource Management (SHRM) have co-chaired the Human Resource Initiative for a Legal Workforce. SHRM is the world's largest association devoted to human resource management. Representing more than 250,000 members in over 140 countries, the Society serves the needs of HR professionals and advances the interests of the HR profession. Founded in 1948, SHRM has more than 575 affiliated chapters within the United States and subsidiary offices in China and India.

The HRI supports a federal electronic employment verification system to improve the existing system. Our objective is to promote a secure, efficient and reliable system that will ensure a legal workforce and help prevent unauthorized employment.

In addition to my experience with ACIP and HRI, my remarks are based to a great extent on my experience as chairman of Fragomen, Del Rey, Bernsen & Loewy, LLP, a global business immigration law firm with 35 offices that advises some of the largest corporations on employment eligibility verification worldwide.

Background:

In 1986, Congress enacted the Immigration Reform and Control Act (IRCA). It introduced, for the first time, civil and criminal penalties against *employers* who hire unauthorized workers. IRCA requires employers to verify the employment eligibility of each of their employees in the United States. This is commonly called the Form I-9 process, referring to a form that the employer and employee both have to complete as part of the verification process. Furthermore, IRCA contains a prohibition against employment discrimination based on an employee's national origin and citizenship status.

In sum, the I-9 process requires the employee, on the first day of employment, to complete the first section of the form indicating name, address, and citizenship or

immigration status. Within three days of employment, the employee must present a document or combination of documents enumerated on the form to demonstrate identity and eligibility to work in this country.

The employer's representative, typically a human resources professional in the organization, attests on the same form that he or she has examined the document or documents and that the document or documents appear genuine and that they reasonably relate to the employee.

In essence, IRCA's worksite enforcement requirements utilize the employer, as a partner of the government, to verify each employee. Failure to follow the proper I-9 procedure carries a penalty. At the same time, IRCA prohibits the employer from asking for more or different documents due to its perception of the employee's national origin or immigration status. Employees who believe they have experienced such discrimination may file a complaint with the Office of Special Counsel for Immigration-Related Unfair Employment Practices.

It should not be surprising that the process has been vulnerable to fraud from the beginning. Soon after implementation, it became clear that employees can present completely false documents; they can look genuine on their face, and employers have no way to discern if they are actually fraudulent documents. Moreover, unscrupulous employers can deliberately overlook the fact that employees are presenting documents that appear suspicious.

The solution, many thought, was in the creation of an electronic verification system that would allow the employer to use government databases to verify the information presented. In 1996, through enactment of the Illegal Immigration Reform and Immigrant Responsibility Act (IIRIRA), Congress authorized the "Basic Pilot" program. The former Immigration and Naturalization Service (INS) administered the pilot program, which verified employment eligibility by cross-checking information with the Social Security Administration (SSA) or INS databases. Basic Pilot eventually became "E-Verify." Participation was voluntary, though as discussed below, various federal and state mandates make participation effectively mandatory for many employers today.

E-Verify is a web-based system that requires an employer to enter into it identity information on the employee (name, Social Security or work authorization number, and date of birth). The E-verify program then compares this information against the Department of Homeland Security database for work-authorized foreign nationals or against the Social Security database for U.S. citizens.

After entering the data, the employer receives a response—either confirming that the data entered by the employer matches a government database, or it does not (known as a tentative non-confirmation). If the data is confirmed, the employee is allowed to begin work. If the employer receives a tentative non-confirmation, the employee is directed to contact the appropriate federal agency to resolve the discrepancy. The employer is required to allow the employee to work while this discrepancy is being resolved.

The E-Verify program is scheduled to expire in September 2012. It has undergone tremendous growth under INS's successor agency, U.S. Citizenship and Immigration Services (USCIS). Last December, the GAO reported that USCIS has reduced tentative non-confirmations (TNC) from 8 percent during the period from 2004 through 2007, to about 2.6 percent in fiscal year 2009. Moreover, only 0.3 percent of the employees who receive an initial TNC are later found to be work-authorized.

According to USCIS's own website, in FY 2010 the percentage of queries resulting in automatic confirmation improved to 98.3 percent, or 1.7 percent TNCs. The total number of employers enrolled in E-Verify rose from 2,300 (2005 GAO report) to nearly 217,000 (2010 GAO report). USCIS informed me this week that the actual enrollment is now up to 254,000 employers.

The growth in participation is due, in part, to new federal laws. In September 2009, after a lengthy review, the Obama administration implemented an amendment to the Federal Acquisition Regulation (FAR) that was promulgated by the Bush administration. It would require most federal contractors and their subcontractors to use E-Verify.

Unlike the Form I-9 process, which applies only to new hires, this regulation requires reverification of all existing workers who will be working on the contract. Employers may choose to re-verify their entire workforce, as well. Moreover, the White House has continued another Bush-era regulation that permits only employers who use E-Verify to extend the work authorization of certain foreign graduates of U.S. universities. In addition to regulatory mandates, U.S. Immigration and Customs Enforcement (ICE) often incorporates E-Verify participation as part of a settlement agreement with an employer found to be in violation of IRCA's provisions.

The federal government is not the only entity expanding the mandate to participate in what Congress intended in 1996 to be a voluntary program. A fast-growing number of states and even some municipalities are requiring E-Verify enrollment and/or state-mandated verification procedures, either as a condition to government contracts, or as a condition for doing business at all.

According to the latest figures, more than half of the states currently have some kind of requirement to use E-Verify or other laws related to eligibility verification, with several additional states considering similar legislation. A vast array of state and local laws creates a great deal of confusion and uncertainty for employers with operations in multiple jurisdictions. On December 8, 2011, the Supreme Court heard arguments on the issue of whether states have the authority to impose these requirements, or if federal law preempts the states. The decision of the court should dictate whether state and local governments may continue to impose E-Verify and other immigration-related laws and ordinances.

Notwithstanding the remarkable surge in participation and improvement in the confirmation rate provided by E-Verify, overall participation still is only about 3 percent of the total employer population. The most common disincentive to participation is the

fact that E-Verify does not eliminate the need for the so-called I-9 process. Some services are available to electronically streamline the I-9 and E-Verify processes, but both still represent an additional administrative burden.

Within industries that do not have a high occurrence of unauthorized employment, employers don't perceive a significant benefit in using E-Verify, compared to the required investment of time and money. Finally, because E-Verify remains, in effect, a "paper-based" system because of its reliance on a subjective review of documents, it is unable to detect many forms of document fraud and identity theft. This is because E-Verify does not authenticate the identity of the *person* presenting the documents. It only verifies that the data on the documents matches information in the federal databases.

While E-Verify continues to expand, so has ICE enforcement against employers. During the Bush administration, enforcement officials used criminal identity theft statutes to prosecute unauthorized workers. However, on April 30, 2009, Homeland Security Secretary Janet Napolitano announced that ICE would redirect enforcement of immigration law away from the unauthorized workers and toward *employers*—for both unauthorized hiring and I-9 paperwork violations, even where there is no unauthorized worker present.

In the months following that announcement, ICE implemented this new policy by increasing the number of audits against employers. For example, just before the July 4th weekend in 2009, ICE issued I-9 audit notices to 652 employers nationwide, 149 more than the total for the Bush administration's final year. Just before the Thanksgiving weekend in 2009, ICE issued another 1,000 audit notices.

According to a recent announcement from Secretary Napolitano, from January 2009 through the end of fiscal year 2010, which ended on September 30, 2020, "ICE has audited more than 3,200 employers suspected of hiring illegal labor, debarred 225 companies and individuals, and imposed approximately $50 million in financial sanctions—more than the total amount of audits and debarments than during the entire previous administration." Most of the penalties have been assessed against employers for paperwork violations.

The Problem:

One continuing criticism against E-Verify is that the system is susceptible to identity fraud. Indeed, while E-Verify's capability and accuracy have improved immensely in matching a name with a Social Security number, it cannot confirm that the person presenting the document is who he or she claims to be. According to a December 2009 report by Westat, 54 percent of the unauthorized workers who are checked through E-Verify are confirmed as work-authorized. The December 2010 GAO report reiterated this assessment.

Identity fraud, including the inability of employers to be certain about employees' employment eligibility, poses substantial problems for not only employers, but also for government and legal U.S. workers.

First, it is a problem for law enforcement. Rather than focusing scarce resources on employers who intentionally violate the law, immigration officers have a tendency to look with suspicion at all employers. Ironically, IRCA made employers partners of law enforcement in the law's implementation, yet employers have become the suspects. Consequently, law enforcement resources are spread thin across the entire employer community, instead of focusing just on the bad actors.

Second, the uncertainty over eligibility poses legal and financial risks for employers. While it is true that employers who use E-Verify enjoy a presumption of compliance, employers remain vulnerable when they do not know with certainty that they have a legal workforce. This has already presented a problem for many U.S. employers.

Time and again, we hear of yet another E-Verify-participating employer who has to shut down business operations because its workers are determined to be unauthorized after an ICE raid or audit. In most of these cases, the employers are found not liable for any violations and, in fact, have followed the I-9 and E-Verify regulations strictly. Nonetheless, the financial loss and reputation damage can be more severe than any civil fine.

My point is not that the government should not conduct raids or audits. Rather, it should explore why an employer that completes all of its I-9s and uses E-Verify can still have unauthorized workers on staff. What more could the employer do?

Third, while I again acknowledge the tremendous improvement that E-Verify has made in data accuracy, mistakes still occur. False non-confirmations are not created by the E-Verify system itself, but by inaccuracies in the SSA and DHS databases. In this regard, depending on the particular circumstances, the employee and the government both bear the responsibility for failing to update the information. In any event, the erroneous result can result in administrative burden for the employers, and inconvenience or even financial hardship to the employee in the rare case of an erroneous final non-confirmation.

Finally, the system imposes burdens on legal U.S. workers who must ensure their documents are in order when applying for a job, giving them yet another reason to worry about identity theft. And one unexpected consequence of the Hurricane Katrina disaster was that employers were hesitant to hire those who had fled the area without their documents. In addition, U.S. workers assigned to federal contracts have had to take time off work to go to the Social Security Administration to obtain new cards, or to correct other errors that appear during the E-Verify reverification process.

Under the current system, the level of uncertainty may foster skepticism toward all employees, especially those who are perceived to look or sound "foreign." The less certainty there is for employers, the more likely unsophisticated employers will revert to personal biases in an abundant exercise of caution. An easy and certain "yes/no" in the verification process would mean that employers could no longer use subjectivity as an excuse for discriminatory hiring practices.

As early as 1993 and 1994, I testified before the House Subcommittee on International Law, Immigration and Refugees in favor of a credit card-like verification system which checks the government databases to confirm identity and work authorization. My concern was that the system subjected *law-abiding* employers to penalties because of inadvertent clerical errors on the I-9, while the lack of effective enforcement allowed *law-breakers* to continue employing illegal workers with impunity.

I have the same concern today. As technologies have advanced, so have fraudulent practices. The ultimate solution is a system that offers employers who wish to follow the law the assurance of certainty.

Recently, USCIS has been incorporating photographs from U.S. passports and DHS-issued immigration documents ("green cards" and employment authorization cards) into E-Verify. That allows employers to compare the photograph in the system with the photograph on the document that the employee presents, *if* the employee chooses to present a passport, green card or employment authorization card from DHS.

The "Records and Images from DMV's for E-Verify" (RIDE) initiative, to be implemented later in 2011, will enlarge significantly the pool of photographs for comparison purposes. But that will only happen if all or nearly all of the states elect to participate in the program *and* improve their respective data integrity by complying with Real ID Act requirements or taking similar steps. USCIS should be commended for its relentless efforts to stop identity theft, but at this point, the agency does not have access to sufficient data across the country to stop identity fraud in a meaningful way.

In addition, this photo-comparison effort only stops fraud successfully when there has been a photo substitution on a document. It does not remove subjectivity on the part of the employer who must determine whether the employee *resembles* the likeness in the photograph. Because of concerns about discrimination, employers are hesitant to ask for more or different documentation if the person reasonably resembles the photograph. It also should be noted that many identity theft schemes begin with fraudulent breeder documents, which can lead to subsequent documents being issued "legitimately" to persons who assumed false identities.

Finally, USCIS is to be commended for launching the E-Verify "Self Check" last month. This feature allows individuals to check their own employment eligibility *before* having to undergo verification for a new job, allowing U.S. workers to resolve any errors before starting a new job. A crucial part of the Self Check process is that it requires employees to confirm their identity through a process that ensures that they are running a check on themselves. An independent service generates an identity assurance quiz on demographic and/or financial data about the individual that is generated by a third-party service—in the case of this pilot phase, the credit rating agency Equifax. This identity information is not shared with the DHS in any way, with the department notified only that a user's identity is verified and that self-check may proceed.

The chairman of this subcommittee should be recognized as having introduced this concept in the New Employee Verification Act (NEVA). Self Check is not designed to prevent identity theft in this current construct, but it certainly should be considered.

The Solution:

An accurate and responsive electronic system is a critical component of an effective employment verification program. Congress and agency officials must address the shortcomings of the current program. The following are some recommendations for policymakers in both the legislative and executive branches to consider:

1. *Provide funding and resources to reconcile mismatches in the Social Security database:*

First, whatever requirements are placed on the Social Security system must do no harm to the system or affect its mission of providing benefits to retirees, those with disabilities, or survivors.

Second, the data errors in the Social Security Administration's database must be cleaned up. Advance appropriated resources and staffing must be provided to Social Security to address this issue before any more requirements are placed on the agency.

According to a SHRM survey, 92 percent of U.S. employers actually want to participate in an electronic verification program—provided the system is accurate, efficient and easy to use. To accomplish that, the underlying databases upon which the verification is based must be accurate.

For most U.S. citizens and lawful permanent residents, E-Verify checks the information on the Form I-9 against the Social Security Administration's database. Errors in the database result in a "non-confirmation" response from the system. While it is the employee's responsibility to correct this information, the employer must continue to employ and train the worker during this time. If employers are mandated to use an electronic verification system, the government must invest the resources to minimize the false non-confirmations for legal workers, and to establish systems that allow the employee to correct errors quickly and easily.

2. *Provide clearer instructions on Social Security mismatches:*

While the government works on reconciling the SSA database, employers need better guidance on the potential impact of mismatch notices on work authorization. The Department of Homeland Security promulgated regulations on this issue in 2006, and again in 2008, to comply with a federal court order. ACIP and SHRM supported this regulation because it provided safe-harbor procedures for employers to follow. The regulation was rescinded in July 2009.

Now, even though there is no longer a regulatory mandate to act affirmatively, an employer's inaction after receiving notice of a Social Security mismatch still can be corroborating evidence to be used against the employer in a worksite action. The problem is that SSA and the Internal Revenue Service continue to notify employers of mismatches, and in fact, this month, SSA is resuming the practice of sending "decentralized correspondence" to employers again when the employees involved in the

mismatch do not have a valid address. Meanwhile, there is not any clear instruction from ICE on what the employer should do.

I do not question the Department of Homeland Security's decision to rescind the regulation, nor am I here to defend the merits of that particular rule. I do, however, emphasize that if employers are to remain responsible for resolving Social Security mismatches, then employers should have clearer guidance from the government.

One tool which is available to employers to reconcile payroll records with the SSA database is the Social Security Number Verification Service (SSNVS). It can be effective in identifying name and number mismatches, but its utility is limited as it is not linked to any immigration databases, and it is ineffective against identity theft. In fact, the Department of Justice Civil Rights Division, SSA, and even ICE have repeatedly instructed employers that SSNVS is to be used only for payroll purposes, not employment eligibility verification. This instruction is important to prevent discriminatory acts, but the government needs to do a better job explaining what employers *should* do in case of a mismatch from SSNVS. The current instructions confuse employers on what they can or must do with information from SSNVS.

3. Verification should only apply to new hires.

To use enforcement resources wisely and to limit the impact on government databases, only new hires should be required to be checked for work authorization. As you know, there are 145 million individuals employed in the U.S. and, due to job turnover, there are approximately 60 million new hires annually. On average, most individuals would be run through an employment verification system within three to four years.

One issue that has raised substantial concern for many employers is the idea of mandatory re-verification. Under current law, only federal contractors are required, and permitted, to re-verify the existing workforce. Employers learned from experience implementing the FAR amendment that re-verification can be very costly, up to several million dollars for some of America's largest employers.

For industries that typically do not have a problem with unauthorized employment, it is hard to get them to support mandatory re-verification because the cost far outweighs the benefit. On the other hand, there are other sectors where employers want to re-verify the current workforce. If E-Verify is mandated for all employers, re-verification should not be required, but be available for those who wish to reverify their existing workforce. Of course, employers would not be permitted to re-verify in a discriminatory fashion, and must have a consistent and nondiscriminatory policy.

Right now, the employer is stuck between a rock and a hard place. Perceived inaction will result in prosecution from ICE, overzealous follow-up can result in charges of discrimination, and the employer does not know where the line is drawn.

4. Incorporate biometric or other "paperless" technology to remove "guessing."

The government must appreciate that IRCA's verification requirements are premised on *trust*, not *skepticism*, between the employer and the government. Additionally, the purpose of the statute is to curb unauthorized employment, not to penalize unsuspecting employers for paperwork or procedural errors.

Presently, even though ICE does target industries that are either critical to infrastructure protection or have higher instances of unauthorized employment, the focus still is on employers' paperwork errors. It makes little sense to entrust, and to burden, employers with the I-9, and in many cases E-Verify obligations, if the results cannot be trustworthy anyway. Enforcement action therefore must be consistent with that statutory intent and be executed in a cooperative and not adversarial spirit.

The best long-term solution is to create a system that provides a much higher degree of certainty, thereby placing the burden of ensuring data integrity on the government. Moreover, as part of the "certainty," the system must have the capability to stop identity theft.

There may be no other way to achieve this certainty than to establish a truly paperless process that incorporates biometric identifiers in the verification process. This also was a proposal in the Johnson-Giffords NEVA bill. Ultimately, regardless of what kind of technology the government ultimately chooses, the end product must be fast and accurate. In other words, employers deserve a "yes" or "no" answer that is unambiguous.

The benefit to biometric technology, or comparable technology ensuring the same degree of certainty, is that the employer only has to attest to having gone through the process of verification. It does not have to make subjective judgments or risk having an unauthorized worker because the system is inherently unreliable.

I am aware of the skepticism toward creating a biometric-based system because of anticipated cost, but it truly is the most effective way to stop illegal migration. Border security is critical, but we already have seen smuggling patterns adjusting to border enforcement. At what point will enforcement stop being practical and we fence the entire country, including coastlines?

In addition, while SEVIS and US-VISIT are important programs to track the compliance of temporary visa holders, they alone cannot stop temporary visa holders from overstaying. An effective worksite enforcement program, along with strong border and interior enforcement, is critical to ensuring the integrity of our immigration system.

While we speak of the importance of immigration enforcement and stopping unauthorized employment, it is equally important to protect the rights of those who are *legally* in the workforce, regardless of appearance, accent, or citizenship status. We must commend the Office of Special Counsel and organizations such as the National Immigration Law Center, and many others, for protecting the rights of all legal workers, especially those who are most vulnerable because of their national origin or citizenship status.

As Westat found in 2009, naturalized citizens are especially adversely affected by government database errors, as are immigrants with hyphenated names. As impressive as the E-Verify improvements have been over the past five years or so, we must be sensitive to how devastating it must be for work-authorized persons and their families to lose a job because of government error, or misuse of verification tools.

At the same time, we must understand that employers discriminate, either deliberately or out of ignorance, because the current system allows subjectivity. The benefit of achieving certainty in the verification process extends beyond just ensuring a legal workforce. By removing subjectivity, employers would no longer experience the anxiety of not knowing whether the workforce is legal. Employers would no longer have the tendency to treat certain workers disparately, either in making hiring decisions or in document examination. At the same time, employers who do discriminate intentionally would have no credible defense for their actions.

5. *Create a truly federal electronic verification system that preempts the confusing patch-work of state laws.*

An effective employment eligibility verification system at the federal level will strengthen the argument for federal preemption of state and local immigration enforcement laws, which is supported by business and civil rights communities.

Currently, one of the often repeated refrains against preemption is that the federal government is not "doing its job" in stopping illegal immigration or unauthorized employment. An effective verification system will refute that argument and support federal preemption.

Employers, of course, welcome federal preemption because it is much easier to comply with one set of laws than 50 state laws, plus additional local ordinances. This constant shift makes it very difficult for employers in multiple jurisdictions to remain compliant.

Recently, the governor of Minnesota let his predecessor's executive order mandating use of E-Verify to lapse. Of course, to obey the previous executive order, many employers had already invested the money and training to get the programs in place. Earlier this year, the governor of Florida issued an executive order that mirrors the FAR and mandates re-verification of current workers. But since the legal basis for re-verification is not there for the Florida executive order, compliance with the state requirement could mean violation of federal law.

In addition, as E-Verify expands we should make it a truly electronic system by eliminating the current paper-based I-9 process and establish a streamlined process for attestation and verification.

Conclusion

Vigilant enforcement of immigration laws at the worksite is an integral part of any successful immigration reform package. Effective enforcement is only possible with a system that provides employers with certainty and treats employers as partners—not suspects.

Incorporation of biometric or accurate technology is an important component to achieving the desired level of certainty, which then leads to fewer cases of discrimination and racial profiling, as well.

Finally, an effective federal worksite enforcement program will justify strong federal preemption, thus eliminating the need for inconsistent state and local laws that confuse employers.

Chairman JOHNSON. What is the State that is using the driver's license?

Mr. FRAGOMEN. Mississippi.

Chairman JOHNSON. Thank you.

We have got a vote. There will be two votes. I am going to put the committee in recess for 30 minutes, or if we get back sooner. Thank you. We stand in recess.

[Recess.]

Chairman JOHNSON. The committee will come back to order.

I would like to ask Mr. Fragomen, the most critical issue facing America today is jobs. And I think without jobs and job creation,

our country is doomed to a lower standard of living for decades to come. What steps need to be taken, in your opinion, to ensure that employment verification, in particular an expanded E–Verify, doesn't complicate or impede creating a job and hiring the right person for the job?

Mr. FRAGOMEN. I think that is a very critical issue. The most important factor is to move into this slowly if we have mandatory verification, and to make sure that it is possible to scale the system to the level that it would need to be and to, as they say, get it right. Now, in order to get it right——

Chairman JOHNSON. When you say "scale the system," what do you mean?

Mr. FRAGOMEN. In terms of increasing it. The system now covers about 3 percent of employers.

Chairman JOHNSON. We have been fighting that for years.

Mr. FRAGOMEN. It needs to cover 100 percent, which means we have to add about 7.5 million employers to the system, which means that the volume of transactions that the E–Verify, for instance, would have to be able to accommodate would be multiples of what it is currently. And you know the problems that software encounters when you try to increase its capacity by that magnitude. And the second thing is——

Chairman JOHNSON. I know. But Social Security claims they have the most modern system available today. I mean, that is what they tell me.

Mr. FRAGOMEN. They might. Except the number of tentative nonconfirmations, when you multiply it by that number of employees, becomes a very significant number if you figure about 1 to 1.5% percent of the cases wind up as tentative confirmation. There are ones that don't get resolved easily.

The other aspect of it is that there be adequate resources dedicated to Social Security so that they do it right, that the system be fully electronic, that it incorporate biometrics or other fraud-prevention technology or software; and secondly, that we have a uniform law, that this applies everywhere, and it preempts the current State laws.

I think it is very important that the employer is offered a safe harbor, because at the end of the day, it is really the government's responsibility to get the system right to protect the employer, and to offer a safe harbor, and to protect the employees against potential discrimination. But to accomplish all of those goals, it really has to be a government-driven system that can prevent identity fraud.

Chairman JOHNSON. Well, every expert we have talked to acknowledged the fact that E–Verify can't detect identity fraud very well and may, in fact, encourage it. So that puts the employer on the frontline of trying to detect and prevent identity fraud. So can you tell us the challenges faced by your companies in their attempts to detect identity illegalities and yet fill the jobs that Americans need?

Mr. FRAGOMEN. I think it is very frustrating to companies who have to go through this process, because essentially they have to accept the documentation that is given to them by the employee as long as it looks reasonable on its face. And there is really nothing

further, no further steps they can take. If they ask for additional documentation, they could easily be accused of discrimination. And the companies, of course, are generally very concerned about making certain they do things right and they don't hire workers that aren't legally authorized to work because, of course, they could lose these employees in an enforcement action, and then, of course, that would hinder their ability to deliver the service that they are delivering.

So it is counter—it is a counterintuitive situation because you have—you are presented with documentation, you really don't like the way the documentation looks, but you have no reason to say with certainty that there is anything inappropriate, you just have to accept it. So I think it puts the companies in an extremely difficult position. And of course, if it turns out that the documentation, in fact, is fraudulent, then the employer's whole business is at risk, and an enforcement action, and he loses a big portion of his workforce.

Chairman JOHNSON. Thank you very much.

My time has expired. Mr. Becerra, you are recognized.

Mr. BECERRA. Mr. Chairman, thank you very much. And I thank each of and every one of you for your testimony.

I don't believe there is a person in this Congress and, I suspect, sitting here in this audience who wouldn't agree that as a sovereign Nation, we have to do everything we can to make sure that we understand who is in our country and who is securing employment in our country. And I know that we continue to try to figure out the best way to get there. So your testimony is important because Congress is going to make every effort to try to take us to a place where we can tell the world—not just Americans, tell the world—that we are going to determine the best way to figure out who should come into the country and who should be able to work in our country. And so I wish you great deal of good fortune as you continue to assemble the information and the data that will help us make the best decisions here.

I am concerned about two things in particular: As we try to move forward in verification for employment, that we are not undermining the essential work that is supposed to be done by the agencies that might be placed in a position of charge to do the work. So in the case of Social Security Administration, you are already backlogged in trying to deal with disability claims from Americans who are trying to get their benefits. You are backlogged when it comes to trying to secure the different resources you need to do the other things that come from having the most popular identifier in the world, the Social Security number. So I am wondering if you can give us a better sense.

Right now E–Verify is a program used in 2 or 3 percent of the employment community. And if you expand it and make it mandatory throughout the Nation, we are expanding it dramatically. And we have already heard the stories of the potential fraud, potential misuse of identity, and certainly the dramatic dislodgement of employment that an American may have secured rightfully and then loses it. How are we prepared, then, to move to a fully national mandatory system?

And so perhaps what I can do is ask Mr. Stana first to give us a sense if you think any of the Federal agencies that would be in charge of a nationwide mandatory system are equipped today with resources and personnel to go to ramp up to full 100 percent participation of the employment community.

Mr. STANA. Well, I think, as you pointed out in your statement, the CBO estimated it would take billions of dollars to make sure that Social Security and DHS and whoever else would be involved would have both the technology and the personnel to make this happen. Currently do they have that to ramp up right away to a mandatory system? Probably not. But with proper resources, they could get there.

The other questions you raised about the ID theft and making sure that you don't have false negatives, the system will need adequate resources to get on top of these issues. The challenges do not pertain to the 95 percent of the population that is properly handled, it is about the 5 percent that is problematic.

Mr. BECERRA. But the 95 percent of the population might pay the price as we try to deal with that 5 percent.

Mr. STANA. You can't ignore the 95 percent.

Mr. BECERRA. But, Ms. LaCanfora, let me ask you this. Social Security in this tough budget environment is taking a hit in this 2011 budget. Chances are it might take a hit in the 2012 budget. You are already having a difficult time dealing with all of these other responsibilities you have to our Americans who are applying for retirement benefits, for disability benefits, survivors' benefits. Can Social Security ramp up to a 100 percent E–Verify participation without sufficient resources to do this?

Ms. LACANFORA. The simple answer is no, Mr. Becerra. We appreciate and share your concerns about funding. It really depends largely on what you consider mandatory 100 percent expansion. Right now E–Verify is largely used for new hires, with few exceptions, and if you look at the current volume, we get about 16.5 million queries a year. If you ramp it up to new hires nationwide, that would be around 60 million queries a year. If you ramp it up even further to include current employees, you could be getting up to 140 million queries a year or more.

So it depends on the mandate. But certainly any mandate would have a significant impact on Social Security, increased traffic in our local offices, and we would need to be funded for that.

And I would also support the comment made by one of my colleagues earlier to say that any mandatory move should be phased in so that we have the opportunity to ramp up and hire as needed.

Mr. BECERRA. And, Dr. Antón, and, I hope, Mr. Fragomen, you as well will continue to provide us with some information that helps us pinpoint some of what your testimony really focused on, and that is how you make this work. How do you collect the information? How do you deal with this Internet fraud that is out there? We really need that to be able to move forward.

Ms. Moran, I hope you will continue to give us the real case, real live examples of individuals, U.S. citizens, lawful permanent residents who have been impacted because we haven't done this perhaps as quickly in implementing a workable program as we would

like. So as we continue to figure out how to ramp up, I hope you all will continue to give us information.

Unfortunately my time has expired, but I would have loved to have gotten into it more with you all. But I appreciate very much your time with us today.

Thank you, Mr. Chairman.

Chairman JOHNSON. Thank you. I appreciate your comments.

Mr. Paulsen, you are recognized for 5 minutes.

Mr. PAULSEN. Thank you, Mr. Chairman.

Mr. Fragomen, small businesses are top job providers. How much of a barrier is not having Internet access for using E–Verify for those folks?

Mr. FRAGOMEN. Well, not having Internet access certainly makes it much more difficult. As you know, you could make verification available by telephone again, but that is not a particularly desirable way to do it. I suppose the good news is this is becoming less of a problem as telephones now are morphing into Internet-enabled devices. So I think it will become less of a problem over a period of time. But certainly it is an issue now.

And the other big issue, too, I think, for small businesses is just the impact on the small businesses if they have a small staff. Since they tend to not have too many employees that have to go, quote, hang around the Social Security office with thousands of other people who will be doing the same thing at the same time, you can imagine what the impact of that would be on these smaller companies.

Mr. PAULSEN. I was kind of wondering if you thought smaller employers essentially should be held to the same standard as larger companies in terms of a compliance measure. They can't get access to the Internet like larger employers. Are you concerned that a work verification system might not only discriminate against the workers, but also against potential small employers?

I should ask you, what about the situation where a potential worker is caught in a tentative nonconfirmation problem, and the need for communications between Social Security and the employer become critical?

Mr. FRAGOMEN. Once again, that is a big issue. I think, in fact, most situations are going to require the employee to actually go to the Social Security office or whatever to try to get these problems resolved. I don't know how many of them are really going to be successfully resolved electronically. But certainly, not having Internet access would be a big problem, and I think it would require on behalf of the smaller employers that they may just have to try, as I say—try to use some of these technologies so that they can get more in the game.

Now, whether it would be reasonable to exempt them, I think that becomes difficult when you consider the number of small employers there are, and the fact that frequently these small employers are where the undocumented immigrants may be employed. So I think giving them sort of exemption would probably be a good idea maybe for a period of time.

Mr. PAULSEN. That was my follow-up. I was curious if you thought it would be a reasonable option to give them an exemption for a certification for a business, the smaller ones in particular, if

they have shown to be good employers or they have had a good-faith effort to actually abide by the law.

Mr. FRAGOMEN. Yeah, I think it would be very reasonable to do that for, as I say, a period of time, because as we discussed a minute ago, it would be important to phase in the program, and the larger employers could be phased in first before smaller employers.

Mr. PAULSEN. Thank you.

I yield back, Mr. Chairman.

Chairman JOHNSON. Thank you, sir.

Mr. Berg, you are recognized for 5 minutes.

Mr. BERG. Thank you, Mr. Chairman.

My question, Ms. LaCanfora, concerns some new hires are authorized to work. We heard a little bit about receiving an erroneous tentative nonconfirmation from the E–Verify system. It seems like we have got too much bureaucracy in here that is really creating a problem for people that are obviously getting kicked or flagged with the system. So I guess my question is, we know Social Security can extend the deadline, and we have field office employees that can make the entry into the electronic system, the EV–STAR. What is SSA doing to try to improve this and keeping people from falling through the cracks?

Ms. LACANFORA. Thank you for the question. Over the past 2 years, we have worked closely with DHS to decrease the number of tentative nonconfirmations. It used to be somewhere, I think, as my colleague said, up around 8 percent. Right now tentative nonconfirmations are around 1.7 percent of the total, and less than 1 percent actually come to Social Security. So the other tentative nonconfirmations may be resolved through DHS. So we get less than 1 visit for every 100 queries coming through the system. That is far lower than it has been in previous years.

In terms of the EV–STAR System, we have, as a matter of fact, next week an enhancement to the system coming in where if someone walks into one of our offices as a result of a tentative nonconfirmation, they don't have to tell our employee that. They can say, listen, I have some sort of discrepancy I need to resolve. And what will happen is when our employee goes into the system, an alert will pop up saying, check EV–STAR, so we can assure that we catch every one of these cases and then document it properly in the system. We expect that that enhancement will significantly increase our use of EV–STAR.

Mr. BERG. Thank you.

I yield back, Mr. Chairman.

Chairman JOHNSON. Thank you, sir.

Mr. Smith, you are recognized for 5 minutes.

Mr. SMITH. Thank you, Mr. Chairman.

Mr. Fragomen, would you talk about the impact of the patchwork of laws on employers? If you could emphasize that, and then about the challenges this creates for Homeland Security in determining the volume of E–Verify workloads.

Mr. FRAGOMEN. Well, impact is very significant. The State laws basically differ from each other. They frequently differ from the Federal law. States sometimes struggle with issues that would seem very simple, but in a modern economy, it becomes les obvious.

For instance, what is the place of employment; if you physically work in one location, but you report into and you are paid by an employer or an office that is in the State; or perhaps there is no office at all in the State, but you actually, in fact, render services that benefit, for instance, a company with whom you have a contract in that State. So they have a lot of difficulty identifying what the different standards are. And then, of course, you have your virtual employees who are just working at home.

So the bottom line is that it is a very, very expensive proposition for corporations to try to track all of these different rules and try to comply with them on a State-by-State basis.

Mr. SMITH. And, Ms. LaCanfora, everything is fully reimbursed at Social Security, right?

Ms. LACANFORA. Yes. DHS reimburses us for all of our costs.

Mr. SMITH. Can you elaborate how that reimbursement takes place?

Ms. LACANFORA. Sure. What happens is at the beginning of the year, DHS will estimate the number of queries that they expect. We at Social Security estimate the amount of the fallout that we expect to happen; in other words, the number of people that will actually walk into a field office. And with those two numbers, we then estimate the amount of money that DHS should reimburse us for the year, and they pay us that money up front, and then at the end of the year, after we know how many queries we actually got and how many field office visits we actually got, then we reconcile those numbers and we sort out the change.

Mr. SMITH. Thank you.

Thank you, Mr. Chairman. I yield back.

Chairman JOHNSON. Thank you.

Mr. Tiberi.

Mr. TIBERI. Thank you, Mr. Chairman.

As I left, I told Mr. Fragomen—just to let everybody else know before I ask the question—just this morning I had an employer talk to me about this issue. A family-owned business, participating voluntarily in the E–Verify system, has been very frustrated with the lack of continuous continuity in the system. Sometimes it takes up to 7 days for verification. At that point, usually if it takes that long, the applicant that he is going to hire is gone and goes to another employer who doesn't have an E–Verify system. So he is frustrated from that perspective.

He is frustrated that this small business owner who owns 12 restaurants in Ohio was audited in a voluntary manner by ICE and found that 83 of his employees in total that were E–Verified had given him incorrect information on the I–9 form, so he got fined. He fired the 83 employees, and they are probably working somewhere else. And here is an employer who is actually trying to participate in the system.

So I have grave concerns about how a mandatory system would work when clearly the voluntary system is not working for employers—some employers today. So I would like to ask each of you—and we can start at the end here, what do I tell my constituents about why I should support a mandatory system when clearly the voluntary system is not working?

Mr. STANA. When we did our work that resulted in the report that was issued a few months ago, we went out to the State of Arizona and North Carolina and a few other places and talked to employers and employer groups, and asked them what they wanted in an E–Verify system. Some of the issues you are bringing up today really weren't on their radar screen. They said they want something that is reliable, fast and not burdensome. And they are worried about other employers having a competitive advantage because they misuse the system. They fear they could lose an employee who later goes down the street to another employer who misuses the system and gets hired.

So I think what I would say to your constituent is that to the extent that this system is reliable, fast and not burdensome, it would be ready for prime time, in our estimation.

Mr. TIBERI. But today he would argue—I am not sure it is not reliable—the E–Verify system is not reliable, sometimes takes up to 7 days, and in this case not very timely or accurate.

Mr. STANA. Without knowing the facts and circumstances of that case, maybe he described it differently. He shouldn't have sent the information into the E–Verify system until he actually hired the individual. You shouldn't use it for screening. That is a no-no. But if it takes 7 days to get a response, that is an exception. If such delays happen a lot, then that is of concern.

Mr. TIBERI. It happens a lot, he said.

Ms. LACANFORA. I would say SSA has a very limited role in E–Verify. We obviously have a database, as was mentioned earlier, with over 450 million records of Social Security numbers, which include dates of birth and some citizenship information. But DHS is responsible for all other aspects of the E–Verify system. I have to defer to them largely to respond to your question.

Mr. TIBERI. Ms. Moran.

Ms. MORAN. I am not going to convince you to support a mandatory system. In fact, I don't think that you should. What we need to do is find a solution to the broken immigration system. The employer in your state wants those 83 employees. They need employment. We need to just find a solution so that employer in good faith isn't liable for immigration violations, and he or she can get the workers that they need.

Mr. TIBERI. Thanks.

Ms. ANTON. I would just like to point out there is another issue that has been raised that affects small employers, which is the fact that small employers generally don't have the resources to properly secure their systems. And so in addition to being fined for that kind of thing, they are going to have data breaches, they are going to have databases which contain information that identifies other people, and they are going to be easy targets for people to hack into their systems, insider or out. So that is another consideration is they don't have the resources; not just Internet access, but the fact that their systems are vulnerable to botnets they don't even know that are on there, viruses, et cetera.

Mr. TIBERI. Great point. Thank you, sir.

Mr. FRAGOMEN. Well, it seems to me that if the government mandates that you go through this process, that they then have to assure that as a trade-off, that the system will be certain, and you

will be given a safe haven if you do what you are supposed to do. So before the system, in my mind, is ready for prime time, it has to be—it has to be improved to the point where that is possible. And it has to address this whole issue of identity fraud. And until it addresses identity fraud, has adequate resources, fully electronic, et cetera, it should not be mandated because it is not reliable.

Mr. TIBERI. Thank you. I yield back.

Chairman JOHNSON. Thank you.

Mr. Brady, you are up.

Mr. BRADY. Chairman, thank you for holding this hearing.

I really appreciate the comments of all of the witnesses today. I am convinced in the broader issue that we have to close the back door of illegal immigration so that we can keep open the front door of legal immigration. Workforce verification being timely and accurate is the key to that, to do it successfully and fairly.

Dr. Antón, you had an interesting comment in your testimony about mission creep and how databases start to tie into one another, and before you know it, you are going to have a dangerous situation. Some have suggested that Social Security, IRS and Homeland Security share taxpayer data in the workforce hires. We hear that often. We, the committee, have been very apprehensive about any sharing of taxpayer data. Now, our jurisdiction regarding Section 6103 in the IRS Code prevents it. In fact, our staff asked the Joint Committee on Taxation to prepare a report on these provisions in preparation for this hearing, and, Mr. Chairman, I request that this report be entered into the hearing record.

Chairman JOHNSON. Without objection.

Mr. BRADY. So, Doctor, can you speak to the taxpayer data issue and mission creep and workforce issues.

Ms. ANTÓN. Certainly. So from a privacy point of view, clearly when you start commingling IRS data with other databases in the United States, that raises a lot of red flags.

As a technologist, I can say that requiring, for instance, authentication—for authentication, let us say that you had to provide what was the figure on line 19 of your IRS statement from tax returns from last year. That is something that no one else can get. That is something that only I can look at. So, from that perspective as an authenticator, it is pretty strong. But the concern, then, is that that raises a lot of risks once you start providing that kind of access between systems, and every time you start piggy-backing databases, then you are ultimately increasing the risk of security problems, transmission of information, data leaks, data peeping, like when there is celebrity peeping, et cetera. So it raises a lot of the different risks that have to be considered, and how do you secure all of those transactions as well.

Mr. BRADY. In laymen's terms, businesses and agencies today focus on keeping their data secure. How much greater does the risk increase when you start sharing those types of data across agencies?

Ms. ANTÓN. Ultimately the more data that you have about someone in a database, the easier it is to access a lot more information and cobble together new identities, and so it becomes a very rich target for attack. So that is something the government has to think about is what do we really—there is no such thing as a se-

cure system. We have centuries of experience with war to show that there is no such thing as a secure system or country, et cetera. And so with that knowledge, we have to think about do we really want a system that will eventually be broken into, that will make it easier for people to propagate identity fraud.

Ms. ANTON. So there are just different risks that we have to do. And we need to consider how do you design the system in such a way that we address the real problem at hand instead of patching things on in the hopes that we keep putting Band-Aids on—okay, well, maybe if we just check people to see whether or not they are eligible to work—and then we have all of these other problems. And the real problem, I think, is an immigration problem. So I will just throw that there.

Mr. BRADY. Got it. Chairman, thank you.

Chairman JOHNSON. Thank you, Mr. Brady. That is interesting. You know your line 19 on your IRS form?

Ms. ANTON. I don't. I just threw that out there. But the point is that I would have to look it up. And if I have to look it up, then someone else can't use it.

Chairman JOHNSON. I am not sure I could find mine 10 days after I file the form.

You know, all of you, use of biometric data is always another proposal for ID and authentication. We have been talking about that for a long time, and, of course, it is not perfect either. But can each of you comment on biometrics and what you think of this?

Mr. STANA. Let me answer that two ways. First off, it could be very expensive to do it right. And to do it right might be something other than putting a chip in a card and sliding it into a reader, because those kinds of systems have been hacked in a matter of hours. So that is not good. You have to have a separate data set. So that could be very expensive, but maybe in some form necessary to make this thing work.

Second, biometrics raise all kinds of privacy concerns. How much of your identity should the government have? That is a question that I am not ready to answer. Should the government have my retina scan? Should the government have my fingerprint? Well, they already have my fingerprints, but how much information do you want the government to have? And then you get into the data privacy and security issues.

Chairman JOHNSON. I would like to give it to them so I can get through the airport quicker.

Mr. STANA. Well, that is the other thing. Some people would be perfectly willing to give it up if they could bypass the system somehow; they'd like to put their hand on a reader, and instantly be work-authorized. Others are very sensitive about that.

Ms. LACANFORA. I will preface my comment by saying I am not an expert in biometrics, but I do agree that incorporating biometrics into E–Verify would be a costly proposition. DHS, it was mentioned earlier, is allowing employers now to access passport photos and is working to obtain driver's license photos. And looking at photos is one means of identity assurance, although not foolproof. I think decision makers need to weigh those options against the biometric option to see what is cost-effective and what gets the job done to the extent possible.

Chairman JOHNSON. Thank you.

Ms. MORAN. So the cost and the accuracy issues have already been mentioned. And I encourage you to look at some studies of the Transportation Worker Identification Credential, the TWIC card. It is like a billion dollars, huge error rate, it is kind of in a mess. So I would encourage you to look at that. I think it is the closest thing.

The point is that——

Chairman JOHNSON. It worked, though.

Ms. MORAN. I mean, for some it does, but there has also been some very high error rates, and also the census folks got a 20 percent error rate on fingerprints when they tried to do it for the workers last time around.

So I think the point is that E–Verify, biometrics, nothing is a magic bullet. Again, not to repeat myself, but if you still have undocumented workers in the economy, just like E–Verify, they are just going to go underground and get around the system.

Chairman JOHNSON. Thank you.

Ms. ANTON. So I would just note that if you also add biometrics to a database, that becomes a very, very rich, wonderful asset for anyone who wants to gain access to it.

And another challenge with biometrics is this is another single-factor authentication approach. And so we really are advocating a layered approach where we have multiple ways to authenticate people.

There are places in which biometrics, I think, work very well. For instance, to enter in the Olympic Village, there is always hand geometry, and your hand geometry gets compared to your badge. That isn't retained in any database. So I have to have my credential with me to get in. And so that is a very nice way, approach to do it because you don't have the responsibility of having a database with all the biometrics stored in it.

On the other hand, it is extremely expensive because it means you have to have a reader every single place, and there can be hardware failure associated with that.

Chairman JOHNSON. Thank you.

Mr. FRAGOMEN. If over half of the unauthorized workers who undergo E–Verify are erroneously confirmed as work-authorized, it seems as though we are creating a pretty vast system which impacts on the whole populace, and we are not being very effective at ferreting out unauthorized workers. So it seems to me that as problematic as it might be because of the cost, you still must stop the use of false breeder documents which can lead to issuance of fraudlulent identification suggesting you are someone different from who you really are, and which can cause obvious data security problems. It seems to be that unless we tackle identity fraud and false breeder document problems, at the end of the day, I don't know that we are being very effective in keeping unauthorized workers out of the workforce.

Chairman JOHNSON. It is a cumbersome idea, but it might work.

Mr. Becerra, do you care to question?

Mr. BECERRA. You actually inspired a question that sort of stems from something Dr. Antón mentioned earlier. You mentioned

that trying to expand E–Verify when is prone to errors, prone to intrusion, and loss of privacy, and at the very end you close by saying it is almost as if we are trying to build a system that hasn't been proven to work effectively because we have a decrepit immigration system that is not helping us keep tabs of folks in the first place we are authorized to work. So it sounds like we are piling on top of a broken system.

Other systems that we are not quite sure are ready for prime time may cause difficulties for Americans' privacy and security and may lead to a lot of businessmen and women having to go through some expense and perhaps difficulties with their business if they must go through a system that doesn't always give them the check they need. And so it seems like we would rather than pile on, we should clear the dust and deal with the foundation of why we are talking about coming up with a verification system in the first place.

Ms. ANTÓN. Yes, I wholeheartedly agree, and as you were speaking, it reminded me of everything we would read about business process for engineering during the late 1980s, early 1990s, where one of the problems is that people were building systems that automated existing broken business processes and practices. And so that is why systems become obsolete.

And so I think it is really good to think out of the box and think it would be really big, this is a grand challenge, if you will, and how do we solve a problem; and then build a system that really supports a well-designed business practice.

Mr. BECERRA. Mr. Fragomen, a question for you. If you could take control of this, could you devise a system that would work for verification purposes?

Mr. FRAGOMEN. Well, I think it would be possible. You have to start with the premise that you have to try to limit the number of persons that enter the U.S. illegally. That has to be the first step. You have to have more effective border security. You have to have better systems to keep persons who enter legally from overstaying their status and becoming illegal.

You have to then—once you have a more secure entry system and better control, it seems to me then you definitely have to have a workplace enforcement system that is driven by bioidentifiers.

Interior enforcement doesn't work. For instance, the law that Arizona passed and, of course, was just found unconstitutional, it doesn't really work, and it never has, because you can't basically formulate reasonable suspicion to believe who is in the U.S. illegally, which would then arguably give you a right to question that person; reasonable suspicion to believe that they are an alien unlawfully present in the U.S. So you really can't do that without using racial appearance as a primary factor. So that is never going to work.

So really your only shots at this are border enforcement, a legal immigration system that allows a larger number of people to come into the country to work legally, and workplace enforcement. I think you need those three things combined.

Mr. BECERRA. It sounds like you have just read off the litany of things that most people say we need for comprehensive immigration reform.

Mr. FRAGOMEN. It is certainly a number of those pieces.

Mr. BECERRA. Thank you. I appreciate all of your testimony, and we will probably have you back again soon.

Chairman JOHNSON. Thank you all for being here. I appreciate you taking the recess with us. We did do two votes, and, you know, the world is still turning.

Thank you all so much. This meeting is adjourned.

[Submissions for the Record follow:]

Prepared Statement of The Honorable Mr. Dreier

STATEMENT OF THE HONORABLE DAVID DREIER
Before the House Ways and Means Subcommittee on Social Security
April 14, 2011

It is imperative that we improve the security of Social Security cards to safeguard against identity theft, protect the integrity of the Social Security program and enhance our employment verification system. My bill, H.R. 98, the Illegal Immigration Enforcement and Social Security Protection Act, provides a strong foundation on which to build upon.

The Social Security number (SSN), first issued in 1936, was originally intended to only keep track of individual contributions to the Social Security program. Yet, over time, the SSN has become a ubiquitous identifier for government purposes. For example, individuals must furnish SSNs to be eligible for a variety of federal programs, such as federal student loans and welfare assistance.

The SSN is also frequently used to verify identity in the private sector. Call your phone company to check your bill, and you will be asked for the last four digits of your SSN. Apply for life insurance, and the application may ask for your SSN. Shop for a new car and the dealership will probably check your credit rating with a credit agency which has your SSN.

As we also know, the SSN card is one of 26 documents listed on the I-9 Employment Eligibility Verification Form, which individuals can use in 102 different combinations to prove their authorization to legally work in the country. The ease with which individuals can submit false or stolen SSNs undermines the employment verification system, forces employers to be de facto identity document experts and plays right into the hands of those who commit identity theft.

The 1996 Illegal Immigration Reform and Immigrant Responsibility Act sought to improve the reliability of the employment verification system by creating the Basic Pilot Program, now known as E-Verify, which allows employers, on a voluntary basis, to use an online system to verify the work authorization status of new employees by checking the validity of SSNs with the Social Security Administration. The implementation of this program has been a step in the right direction. However, several studies have found that the E-Verify program is unable to detect identity fraud, allowing those with valid, but stolen documents, to secure employment.

For example, a December 2010 Government Accountability Office report stated that an Immigration and Customs Enforcement (ICE) investigation in December, 2006 found that "...approximately 1,340 employees – all of whom ICE believes were processed through E-Verify – were not authorized to work in the United States. Of the 1,340 unauthorized workers, 274 were charged with identity theft, including the use of valid Social Security numbers belonging to others to get jobs."

H.R. 98 builds on E-Verify's successes by creating a secure, tamper-proof Social Security card, which employers can use to electronically verify the work authorization status of prospective employees. The new card includes a digitized photo of the cardholder, as well as an encrypted electronic signature strip, allowing employers to instantaneously verify a prospective employee's work authorization status with the Department of Homeland Security's Employment Eligibility Database, either through a toll-free number or an electronic card-reader.

A secure, counterfeit-proof Social Security card used in combination with an electronic employment verification system will enhance the integrity of SSNs and help to prevent identity fraud. This plan will also provide small business owners with an easy-to-use system to verify the work authorization status of new employees and allow them to focus on what they do best: run their businesses. I look forward to continuing our work together on this important issue.

Prepared Statement of AARP

AARP

601 E Street, NW
Washington, DC 20049

T 202-434-2277
1-888-OUR-AARP
1-888-687-2277
TTY 1-877-434-7598
www.aarp.org

April 14, 2011

The Honorable Sam Johnson
Committee on Ways and Means
Subcommittee on Social Security
1102 Longworth House Office Building
U.S. House of Representatives
Washington, D.C. 20515

The Honorable Xavier Becerra
Committee on Ways and Means
Subcommittee on Social Security
1102 Longworth House Office Building
U.S. House of Representatives
Washington, D.C. 20515

Dear Chairman Johnson and Ranking Member Becerra:

On behalf of our members and all older Americans, we write today to voice our continuing concerns with respect to further expansion of SSA's administrative burdens. In light of insufficient funding for the SSA to perform its core functions now, expanding the agency's duties will further diminish the ability of SSA to deliver timely services to beneficiaries. For this reason, AARP opposes any proposal that would divert Social Security funds to expand the agency's non-core activities or mandate new ones, including proposals to mandate electronic verification of employment beyond current law, until such time as the Congress has provided all of the resources SSA requires to perform its core responsibilities.

Mandating employee verification provisions would significantly increase the administrative burdens of the SSA -- without any surety of added personnel or funding -- detracting from the agency's ability to serve Social Security recipients. In 2008, the Congressional Budget Office analyzed the budgetary impact of H.R. 4088, a bill to require verification of all employees. CBO concluded that the bill would cost the SSA nearly $9 billion over five years, and over $1 billion in the first year alone. Moreover, the General Accounting Office reported last December that "USCIC's cost estimates do not reliably depict current E-Verify cost and resource needs or cost and resource needs for mandatory implementation."

This extra work given to SSA by Congress would come at a time when the nation is confronting a significant, long-anticipated demographic challenge, the coming of retirement age of the Baby Boom generation, which will add nearly 80 million new beneficiaries to the Social Security rolls. At the end of this decade, these Boomers will reach traditional retirement age at the rate of one every eight seconds. It is not difficult, then, to understand the enormity of the task the agency faces in currently foreseeable work alone.

With the increases in funding Congress has provided over the last three years and significant increases in employee productivity, SSA has been able to make some progress in customer service. However, the unforeseeably long-lasting economic downturn has caused even more Americans to turn to the Social Security Administration. Claims for retirement and disability benefits have risen to record levels. In FY 2010, SSA received nearly 3,225,000 initial disability claims, the highest in its 75-year history. SSA ended fiscal year 2010 with just over 700,000 pending hearings nationwide – the lowest level in five years.

As such, AARP is very concerned about the pending FY 2011 funding level agreement, H.R. 1473; we continue to believe that nothing short of $11.679 billion, with no rescission of IT funds, would ensure the ability of the SSA to adapt to the many critical challenges that confront it this year and enable SSA to prepare for the future. Over the past six months, the denial of critical funds to SSA has resulted in a hiring freeze and suspension of overtime – both have been vital to improvement in disability claims processing. Underfunding of modernization and highly cost-effective program integrity initiatives will also handicap the agency's ability to fulfill its public trust responsibilities today and tomorrow.

At a time when Social Security recipients and applicants are facing ever-greater delays in the prompt delivery of needed services and disabled Americans are enduring long waits for their earned benefits, we urge that you not further compromise the agency's ability to respond to workload issues with tasks that are not fully resourced and unrelated to its core mission. If you have any further questions, feel free to call me, or please have your staff contact Cristina Martin-Firvida of our Government Relations staff at 202-434-3760.

Sincerely,

David P. Sloane
Senior Vice President
Government Relations and Advocacy

Prepared Statement of American Civil Liberties Union

Written Statement of the
American Civil Liberties Union

Laura W. Murphy
Director, Washington Legislative Office

Christopher Calabrese
Legislative Counsel

Before U.S. House Committee on Ways and Means
Subcommittee on Social Security

April 14, 2011

Electronic Employment Verification

Chairman Johnson, Ranking Member Becerra and members of the Subcommittee

On behalf of the American Civil Liberties Union ("ACLU"), America's oldest and largest civil liberties organization, and its more than half a million members, countless additional supporters and activists, and 53 affiliates across the country, we write to express our concerns regarding E-Verify and to oppose any legislative proposal that would expand its use or require a national ID card with a biometric component. E-Verify has proven to be a flawed and burdensome electronic employment eligibility screening system that imposes unacceptable burdens on America's workers, businesses and society at large. A biometric ID system would be unworkable and impose significant privacy and civil liberties costs. The costs to lawful workers, businesses, and taxpayers associated with both these proposals are significant while the benefits are speculative.

Electronic Employment Verification

The ACLU opposes a mandatory Electronic Employment Verification System (EEVS) for five reasons:

(i) it poses unacceptable threats to American workers' privacy rights by increasing the risk of data surveillance and identity theft;

(ii) data errors in Social Security Administration ("SSA") and Department of Homeland Security ("DHS") files will wrongly delay or block the start of employment for lawful American workers and may lead to discrimination;

(iii) it lacks sufficient due process procedures to protect workers injured by such data errors;

(iv) neither SSA or DHS are able to implement such a system and SSA's ability to continue to fulfill its primary obligations to the nation's retirees and disabled individuals would deteriorate; and

(v) it will lead to rampant employer misuse in both accidental and calculated ways.

I. Mandating Electronic Employment Eligibility Verification Poses Unacceptable Threats to American Workers' Privacy Rights

A nationwide mandatory EEVS would be one of the largest and most widely accessible databases ever created in the U.S. Its size and openness would be an irresistible target for identity theft. Additionally, because the system would cover everyone (and be stored in a searchable format), it could lead to even greater surveillance of Americans by the intelligence community, law enforcement and private parties.

The current E-Verify system, implemented in a small fraction of the country's workplaces, contains an enormous amount of personal information including names, photos (in

some cases), social security numbers, phone numbers, email addresses, workers' employer and industry, and immigration information like country of birth. It contains links to other databases such as the Customs and Border Patrol (CBP) TECS database (a vast repository of Americans' travel history) and the Bureau of Citizenship and Immigration Services (CIS) BSS database (all immigration fingerprint information from US VISIT and other sources).[1]

The data in E-Verify, especially if combined with other databases, would be a gold mine for intelligence agencies, law enforcement, licensing boards, and anyone who wanted to spy on American workers. Because of its scope, it could form the backbone for surveillance profiles of every American. It could be easily combined with other data such as travel, financial, or communication information. 'Undesirable' behaviors – from unpopular speech to gun ownership to paying for items with cash – could be tracked and investigated by the government. Some of these databases linked to E-Verify are already mined for data. For example, the TECS database uses the Automated Targeting System (ATS) to search for suspicious travel patterns. Such data mining would be even further enhanced by the inclusion of E-Verify information

Without proper restrictions, American workers would be signing up for never-ending digital surveillance involuntarily every time they applied for a job. In order to help protect Americans' privacy, we recommend that Congress limit the retention period for queries to the E-Verify system to three to six months, unless it is retained as part of an ongoing compliance investigation or as part of an effort to cure a non-confirmation. This is a reasonable retention limitation for information necessary to verify employment. By comparison, information in the National Directory of New Hires, which is used on an ongoing basis to allow states to enforce child support obligations, is deleted after either 12 or 24 months.[2] The current retention period for E-Verify (set by regulation) is an astonishing 10 years. Deadbeat dads have greater privacy protections than American workers.

We also recommend strict limits on the use of information in any employment verification system. It should only be used to verify employment or to monitor for employment-related fraud. There should be no other federal, state, or private purpose. However, as a recent Westat report commissioned by CIS points out, any employer who signs on to a memorandum of understanding (MOU) can access E-Verify and therefore the data in the system could be used for other purposes. For example, such data could provide information about whether a mortgage or credit applicant is likely to be a poor credit risk.[3] Data should be bound by strict privacy rules, such as those that protect census data, which sharply limit both the disclosure and use of that information.[4]

Additionally, the system must guard against data breaches and attacks by identity thieves. Since the first data breach notification law went into effect in California at the beginning of 2004, more than 510 million records have been hacked, lost or disclosed improperly.[5] In 2007, it

[1] 73 Fed. Reg. 75449.
[2] The data retention limitation for the National Directory of New Hires is governed by 42 U.S.C. §653 (i).
[3] Westat Report, p 201
[4] Protections for census data can be found at 13 U.S.C. §9.
[5] Privacy Rights Clearinghouse Chronology of Data Breaches, http://www.privacyrights.org/ar/ChronDataBreaches.htm.

was reported that the FBI investigated a technology firm with a $1.7 billion DHS contract after it failed to detect "cyber break-ins".[6] The December 2010 GAO Report on E-Verify repeatedly references the risk of identity theft associated with the system. In one example, Immigration and Customs Enforcement (ICE) found that 1,340 employees of a meat processing plant were unauthorized workers even though each had been processed through E-Verify. Of the 1,340 unauthorized workers, 274 were charged with identity theft, including using valid Social Security numbers of others in order to work[7]. Data breaches continue to be a contributing factor to identity theft and a constant erosion of Americans' privacy and sense of security. An E-Verify database must not be subject to such threats.[8]

II. Data Errors Will Injure Lawful Workers by Delaying Start Dates or Denying Employment Altogether and May Lead to Discrimination

Recent government reports acknowledge that huge numbers of SSA and DHS files contain erroneous data that would cause "tentative non-confirmation"(TNC) of otherwise work-eligible employees and, in some cases, denial of their right to work altogether. CIS reported that 2.6%, or over 211,000 workers, received a TNC and, according to the Westate report, about 0.8% of these TNCs are erroneous.[9] Since only 0.3% of those mistaken TNCs were resolved, approximately 0.5%, or **80,000 legal workers,** were improperly denied the right to work due to faults in the system.[10] In many of these cases workers simply don't have the time or don't know they have the right to contest their determinations and seek different employment. Finding another job is a difficult option for many unemployed Americans in this economy and certainly means countless hours of red tape and frustration.

In American cities and states where E-Verify has been implemented, the results have been disastrous. A survey of 376 immigrant workers in Arizona (where use of E-Verify is required) found that 33.5% were fired immediately after receiving a TNC and never given chance to correct errors in the system. Furthermore, not one of those workers was notified by the employer, as required in the MOU, that he or she had the right to appeal the E-Verify finding. When Los Angeles County audited its use of E-Verify for 2008-09, it found that 87% of its E-Verify findings were erroneous. Implementing a system this flawed nationwide would be a train wreck for American workers.

These error rates are caused by a variety of factors. First, women or men who changed their names at marriage, divorce or re-marriage may have inconsistent files or may never have informed either SSA or DHS of name changes. Second, simple key stroke or misspelling errors contribute to the volume of erroneous data. Third, individuals with naming conventions that differ from those in the Western world may have had their names anglicized, transcribed improperly, or inverted. The GAO predicted that if E-Verify were made mandatory for new

---

[6] Ellen Nakashima and Brian Krebs, *Contractor Blamed in DHS Data Breaches*, WASHINGTON POST, Sept. 24, 2007.

[7] GAO, *Federal Agencies Have Taken Steps to Improve E-Verify, but Significant Challenges Remain,* p. 24

[8] The breech last week at the Dallas based marketing firm Epsilon which revealed millions of Americans names and email addresses was only the most recent example of this trend.

[9] Westat Report, *Findings of the E-Verify Program Evaluation*, can be found at: http://www.uscis.gov/USCIS/E-Verify/E-Verify/Final%20E-Verify%20Report%2012-16-09_2.pdf

[10] GAO, *Federal Agencies Have Taken Steps to Improve E-Verify, but Significant Challenges Remain,* p.19.

hires nationwide, approximately 164,000 citizens per year would receive a TNC just for name change related issues. [11] It would be even more damaging if applied not just to new hires, hut to existing workers as well.

The high number of error rates occurring among certain cultural groups can lead to an appearance of discrimination in the employment process. Five out of 25 employers acknowledged to GAO that TNCs were more likely to occur with Hispanic employees having hyphenated or multiple surnames.[12] Additionally the TNC rate for employees who were eventually authorized to work was approximately 20 times higher for foreign-born employees than for U.S.-born employees from April through June of 2008.[13] These striking disparities could easily lead employees to believe they were being judged on more than just their credentials. Moreover, employers may shy away from hiring non-native-born individuals or those with foreign names because of a fear they would be harder to clear through the system.

III. Pending Legislative Proposals Lack Meaningful Due Process Protections for Lawful Workers Injured by Data Errors

Workers injured by data errors will need a means of quickly and permanently resolving data errors so they do not become presumptively unemployable. Workers face two distinct challenges. The first is to learn that there are errors in their record and the second is the lack of fundamental due process protections in resolving those errors.

Self-Check

We commend the USCIS for beginning the process of creating a self-check system that allows workers to check on their E-Verify data. It is a fundamental privacy principle that individuals should have access to their own information in order to assure its completeness and correctness. However, it is important to note that this self-check process is still in its infancy and has only heen rolled out on a limited basis.

We have some specific concerns about how the self-check program will be implemented. First of all, self-check is a tool for allowing workers to correct their records; it must not be used as a pre-screening tool. If employers were to impose a self-check requirement – effectively serving as an E-Verify pre-screening tool – they would shift the cost from the employer to the employee – and, in keeping with the statistics cited above, those costs would fall disproportionately on members of minority classes. This would undermine the anti-discrimination provisions built into the system to ensure that authorized workers are able to contest TNCs and document their eligibility to work.

Second, to the system must protect the privacy of both employers and employees. Considering high rates of identity fraud associated with the E-Verify system, it is no surprise that individuals are very concerned ahout the retention of their personal information in a datahase to

[11] *Id.* p. 19.
[12] *Id.* p. 20.
[13] *Id.* p. 40

which more and more people are gaining access. There must be clearly defined limits in regard to potential sharing of personal information.

Third, there must be an option for self-check access to people without credit histories. If self-check relies on background check information, then it will be unavailable to populations of foreign nationals who have only recently arrived in the U.S. and have not yet developed a credit history. This would include some of those with the most complicated immigration situations such as refugees, asylum seekers, and people with temporary protected status.[14]

Due Process Protections

Senior officials in the DHS Privacy Office have said that individuals face formidable challenges in correcting inaccurate or inconsistent information. The Office of Special Counsel for Immigration-Related Unfair Employment Practices and DHS Office of Civil Rights and Civil Liberties have both said that employees have expressed difficulty in understanding the TNC notification letters and the process by which they have to correct errors. Moreover, as of 2009 the average response time for these Privacy Act requests was a staggering 104 days.[15] This is time that an employee would be unable to work under a mandatory E-Verify system. Congress must prevent the creation of a new employment blacklist – a "No-Work List" – that will consist of would-be employees who are blocked from working because of data errors and government red tape.

Under current law there are no due process protections for those who lose their jobs due to government or employer errors. The best current model for due process protections can be found in Title II of the "Comprehensive Immigration Reform for America's Security and Prosperity Act of 2009, H.R. 4321 from the 111th Congress. This provision would have created worker protections for both tentative and final non-confirmations, allowed workers to recover lost wages when a government error cost them a job, limited retention of personal information, and created accuracy requirements for the system.

IV. Government Agencies are Unprepared to Implement a Mandatory Employment Eligibility Prescreening System

As government reports evaluating E-Verify have repeatedly made clear, both SSA and DHS are woefully unprepared to implement a mandatory employment eligibility pre-screening system. The most recent GAO report expressed concerns over how CIS has estimated the cost of E-Verify. It found that the estimates do not reliably depict current E-Verify cost and resource needs for mandatory implementation and that they fail to fully assess the extent to which their workload costs could increase in the future.[16] In order to implement such a system, both agencies would need to hire hundreds of new, full-time employees and train staff at every SSA field office. DHS has an enormous backlog of unanswered Freedom of Information Act (FOIA) requests from lawful immigrants seeking their immigration files. Those files, many of which are

---

[14] The American Immigration Lawyers Association, *E-Verify Self Check Program*, November 29, 2010

[15] Department of Homeland Security, 2009 Annual Freedom of Information Act Report to the Attorney General of the United States

[16] Peck, Amy, *Latest Report on E-Verify: the Good, the Bad, and the Unresolved*, January 20, 2011

decades old, are the original source of numerous data errors. If DHS cannot respond to pending information requests in a timely fashion now, how much worse will the problem be when lawful immigrants, including naturalized citizens, lawful permanent residents, and visa holders need the documents immediately to start their next jobs? Consequently, DHS would need to hire hundreds more employees to respond to these FOIAs.

Businesses seeking to comply with any newly imposed system would also put additional strain on these government agencies. Problems can be anticipated in attempting to respond to employers' requests and in establishing connectivity for businesses located in remote regions or that do not have ready access to phones or the internet. These agency deficiencies will surely wreak havoc on independent contractors and the spot labor market for short-term employment.

Scaling up the existing software platform for E-Verify to respond to the enormous task of verifying the entire national workforce is likely to be a very difficult task. It makes little sense to adopt a system that is pre-destined to cause chaos within these agencies, not to mention the lives of the thousands of Americans wrongfully impacted.

V. CIS has Not Been Able to Achieve a Sufficient Degree of Employer Compliance in Order to Protect Worker's Rights

Despite the fact that CIS has more than doubled the number of staff tasked with monitoring employers' use of E-Verify since 2008, it still does not have the means to effectively identify and address employer misuse or abuse of the system. A recent report from the SSA Office of the Inspector General (OIG) found that SSA itself had failed to comply with many of regulations put in place to protect employees. They failed to confirm the employment of 19% of the 9,311 new employees hired for fiscal year 2008 through March 31, 2009 and, of those who were processed, they did not comply with the 3-day time requirement for verifying eligibility. The OIG also found that SSA verified the employment eligibility of 26 employees who were not new hires but had sought new positions within the agency, 31 volunteers who were not federal employees and 18 job applicants who SSA did not hire.[17] If the government is unable to maintain compliance within its own agencies, we cannot expect private businesses to follow the regulations put in place to protect workers.

Employer misuse has resulted in discrimination and anti-worker behavior in the past and there is no reason to suggest that pattern will change with a new verification system in place. From the inception of E-Verify, the Government Accountability Office and DHS studies have repeatedly documented various types of misuse. The CIS's Westat report also confirmed the fact that many employers were engaging in prohibited activity. Of the employers they contacted, they found that 17.1% admitted to restricting work assignments until authorization was confirmed; 15.4% reported delaying training until employment authorization was confirmed; and 2.4% reported reducing pay during the verification process.

If Congress imposes a mandatory system, it will need to create effective enforcement mechanisms that prevent the system from being a tool for discrimination in hiring. Such

[17] Social Security Administration, Office of the Inspector General, *The Social Security Administration's Implementation of the E-Verify Program for New Hires*, A-03-09-29154, January 6, 2010.

discriminatory actions will be difficult to prevent and even more difficult to correct. Congress should ask: how will the government educate employers and prevent misuse of E-Verify or any similar system?

Biometric National ID System

In response to concerns about the E-Verify system it has been suggested that a possible solution is the use of biometric identification.[18] The ACLU opposes the use of biometric identification because it effectively creates a national ID system with enormous negative implications for privacy, civil liberties and due process.

I. A Biometric National ID System Will Create a Hugely Expensive New Federal Bureaucracy and Will Not Stop Unauthorized Employment

In order to understand the practical problems with national ID, it is necessary understand how the system would work. The key to a biometric system is the verification of the individual. In other words, an individual must visit a government agency and must present documents such as a birth certificate or other photo ID that prove his or her identity. The agency must then fingerprint the person (or link to some other biometric) and place the print in a database. The agency might also place the biometric on an identification card. Such a process would create a quintessential national ID system because it would be nationwide, would identify everyone in the country, and would be necessary to obtain a benefit (in this case the right to work).

The closest current analogy to this system is a trip to the Department of Motor Vehicles to obtain a drivers' license. The federalizing of that system (without the addition of a new biometric) under the Real ID Act was estimated to cost more than $23 billion if carried out to completion, though 24 states have rejected the plan, putting its completion in grave doubt.[19] The cost to build such a system from scratch would be even more staggering. It would involve new government offices across the country, tens of thousands of new federal employees and the construction of huge new information technology systems. Every worker would have to wait in long lines, secure the documents necessary to prove identity, and deal with the inevitable government mistakes. Imagine the red tape necessary to provide documentation for 150 million U.S. workers. It is far beyond the capacity of any existing federal agency.

These problems are not hypothetical. After spending billions, the United Kingdom effectively abandoned its efforts to create a biometric national ID card, making it voluntary. Dogged by public opposition, data privacy concerns, and extensive technical problems, the program has been an embarrassment for the British government.

II. A Biometric National ID System Will Not Prevent Unauthorized Employment

Despite a popular assumption to the contrary, a biometric national ID system would largely fail to solve the problem of undocumented immigration. Security systems must be

[18] A biometric is a physical characteristic of an individual that can be used to uniquely identify them. Common examples include fingerprints, DNA and facial characteristics.
[19] 72 Fed. Reg. 10820.

judged not by their successes, but rather by their failures. After enduring a host of bureaucratic hassles and costs, most Americans would likely be able to enroll in the biometric system. But that does not make the system a success – those workers were already working lawfully. The system only succeeds if it keeps the undocumented workers in this country from securing employment and a biometric national ID system is unlikely to do that.

The first and most obvious failure is that this system would do nothing about employers who opt out of the system altogether (work "off the books"). Already, by some reports, more than 12 million undocumented immigrants are working in the United States. Many of these workers are part of the black market, cash wage economy. Unscrupulous employers who rely on below-market labor costs will continue to flout the imposition of a mandatory employment eligibility pre-screening system and biometric national ID. These unscrupulous employers will game the system by running only a small percentage of employees through the system or by ignoring the system altogether. In the absence of enforcement by agencies that lack resources to do so, employers will learn there is little risk to gaming the system and breaking the law.

Law abiding employers, however, will be forced to deal with the hassle and inconvenience of signing up for E-Verify and a biometric system. Then they'll be forced to watch and wait when they are blocked from putting lawful employees to work on the planned date due to system inaccuracies or other malfunctions. The inevitable result will be more, not fewer, employers deciding to pay cash wages to undocumented workers. Similarly, cash wage jobs will become attractive to workers who have seemingly intractable data errors. Instead of reducing the number of employed undocumented workers, this system will create a new subclass of employee – the lawful yet undocumented worker.

Additional failures will come when the worker is initially processed through the system. Crooked insiders will always exist and be willing to sell authentic documents with fraudulent information.[20] Undocumented immigrants will be able to contact these crooked insiders though the same criminals whom they hired to sneak them into the United States. Securing identification will simply be added to the cost of the border crossing.

Worse, since 2004, more than 260 million records containing the personal information of Americans have been wrongly disclosed.[21] Many individuals' personal information, including social security numbers, are already in the hands of thieves. There is nothing to prevent a criminal from obtaining fraudulent access to E-Verify (pretending to be a legitimate employer), verifying that a worker is not already registered in the system and sending an undocumented worker to get a valid biometric using someone else's information.

Additional problems inherent in any biometric will materialize both when an individual is enrolled, and at the worksite. For example, according to independent experts there are a number of problems that prevent proper collection and reading of fingerprints, including:

- Cold finger

[20] Center for Democracy and Technology, "Unlicensed Fraud." January 2004 (www.cdt.org/privacy/**2004**0200dmv.pdf).

- Dry/oily finger
- High or low humidity
- Angle of placement
- Pressure of placement
- Location of finger on platen (poorly placed core)
- Cuts to fingerprint; and
- Manual activity that would mar or affect fingerprints (construction, gardening).[22]

When these failures occur it will be difficult and time consuming to re-verify the employee. Running the print through the system again may not be effective, especially if the print has been worn or marred. Returning to the biometric office for confirmation of the print is not likely to be a viable solution because it creates another potential for fraud; the person who goes to the biometric office may not be the person who is actually applying for the job. These are complex security problems without easy solutions.

There would also be mounting pressure to "fix" many of these problems with more databases filled with identifying information such as birth certificates or DNA in an attempt to identify individuals earlier and more completely. This would mean more cost, more bureaucracy and less privacy. From a practical point of view a biometric system is the worst of both worlds. It puts enormous burdens on those already obeying the law while leaving enough loopholes so that lawbreakers will slip through.

III. A Biometric National ID System Will Trammel Privacy and Civil Liberties

The creation of a biometric national ID would irreparably damage the fabric of American life. Our society is built on privacy, the assumption that as long as we obey the law, we are all free to go where we want and do what we want – embrace any type of political, social or economic behavior we choose. Historically, national ID systems have been a primary tool of social control. It is with good reason that the catchphrase "your papers please" is strongly associated with dictatorships and other repressive regimes. As Americans, we have the right to pursue our personal choices all without the government (or the private sector) looking over our shoulders monitoring our behavior. This degree of personal freedom is one of the keys to America's success as a nation. It allows us to be creative, enables us to pursue our entrepreneurial interests, and validates our democratic instincts to challenge any authority that may be unjust.

A biometric national ID system would turn those assumptions upside down. A person's ability to participate in a fundamental aspect of American life – the right to work – would become contingent upon government approval. Moreover, such a system will almost certainly be expanded. In the most recent attempt to create a national ID though a state driver's license system called Real ID, at the outset the law only controlled access to federal facilities and air travel. Congressional proposals quickly circulated to expand its use to such sweeping purposes as voting, obtaining Medicaid and other benefits, and traveling on interstate buses and trains.[23]

---

[22] International Biometrics Group, http://www.biometricgroup.com/reports/public/reports/biometric_failure.html

[23] See, e.g. H.R. 1645, the Security Through Regularized Immigration and a Vibrant Economy Act of 2007 (110th Congress).

Under a national ID system, every American would need a permission slip simply to take part in the civic and economic life of the country.

The danger of a national ID system is greatly exacerbated by the huge strides that information technology ("IT") has made in recent decades. There is an enormous and ever-increasing amount of data being collected about Americans today. Grocery stores, for example, use "loyalty cards" to keep detailed records of purchases, while Amazon keeps records of the books Americans read and airlines keep track of where they fly. Congress has acknowledged these practices and has held numerous hearings to discuss the issues of online privacy.[24] A biometric national ID system would add to these problems by helping to consolidate this data.

The sordid history of national ID systems combined with the possibilities of modern IT paint a chilling picture. These problems cannot be solved by regulation or by tinkering around with different types of biometrics. Instead, the entire unworkable system must be rejected so that it does not intolerably impinge on American's rights and freedoms.

VI. Conclusion: Congress Must Not Enact a Mandatory Employment Eligibility Pre-Screening System

The goal of E-Verify is to reduce the number of unauthorized workers in the United States. Unfortunately, its success rate is extremely low. According to the CIS's Westat report the inaccuracy rate for unauthorized workers is approximately 54 percent.[25] According to the government's own reports, **E-Verify is fulfilling its intended purpose less than half the time**. In addition, experience in Arizona shows that many employers are failing to comply in spite of it being a state mandate. Therefore, while E-Verify continues to burden employers, cost the government billions of taxpayer dollars, and deny Americans' their right to work—all the while potentially subjecting them to discrimination—it is not even adequately performing its core function.

The ACLU urges the Subcommittee to reject imposition of a mandatory electronic employment eligibility pre-screening system and the use of any biometric system. Each would cause great harm to employers across the country and to lawful workers and their families while doing little to dissuade undocumented workers. The likelihood for harm is great and the prospect for gain has so far proved illusory.

---

[24] *Behavioral Advertising: Industry Practices and Consumers' Expectations: Hearing before the H. Subcomm. on Communications, Technology and the Internet of the H. Comm. on Energy and Commerce, and the H. Subcomm. on Commerce, Trade, and Consumer Protection of the H. Comm. on Energy and Commerce*, 111th Cong. (2009); *The State of Online Consumer Privacy: Hearing before the S. Commerce, Science and Transportation Committee*, 112th Cong. (2011).

[25] 2009 Westat Report at 118.

Prepared Statement of American Federation of State County and Municipal Employees

Statement For The Record
of the American Federation of State, County and Municipal Employees (AFSCME)
For the
Hearing on the Social Security Administration's Role in Verifying Employment Eligibility
Before the
Subcommittee on Social Security
Committee on Ways and Means

U.S. House of Representatives

April 14, 2011

This statement is submitted on behalf of the 1.6 million members of the American Federation of State, County and Municipal Employees (AFSCME), urging all members of the Subcommittee on Social Security of the Committee on Ways and Means to oppose any legislation that would require all employers to use the E-Verify electronic employment verification system. A mandatory E-Verify program would place enormous additional responsibilities on the Social Security Administration; would cause hundreds of thousands of U.S. citizen workers and work-authorized immigrants to lose their jobs due to data errors; and cause our economy to suffer. Comprehensive immigration reform that includes an earned path to citizenship is the only realistic and humane approach to stopping unauthorized work.

The Social Security Administration must focus its limited resources on its core mission of providiug beuefits to millions of seniors, people with disabilities and childreu.

Each month, nearly 60 million Americans receive benefits from the Social Security Administration (SSA). Eligihility determinations/redeterminations and benefits processing require millions of field office visits and phone contacts, and well as hundreds of thousands of full medical continuing disability reviews and hearings each year. With its current caseload, 30 percent of SSA's beneficiaries must wait more than 270 days. As of February 2011, SSA had 774,000 pending initial disability cases. Due to funding shortfalls, SSA discontinued service in over 300 remote service sites throughout the United States and may have to consolidate field offices. And, this does not take into account the nearly 80 million baby boomers who will soon be eligible for Social Security retirement benefits. Every day for the next 19 years, 10,000 baby boomers will turn 65 years old.

Expansion of E-Verify would place an enormous added burden on SSA. Currently, only 250,000 of the nation's 7.4 million employers have registered for E-Verify – or three percent. A mandatory program would require SSA to register and serve millions more employers than it does now. And, SSA would be faced with processing 50-60 million additional queries a year for new hires.

E-Verify as it exists already experiences very high error rates which primarily affect U.S. citizen workers.

Even with its small participation rate, E-Verify's database has a 4.1 percent error rate, resulting in 17.8 million discrepancies. The vast majority of these errors – 12.7 million – relate to native-born U.S. citizens. It is not surprising that workers who change their immigration status, marry, divorce, and/or have hyphenated surnames could falsely be accused of lacking authorization to work. Due to these technological and paperwork errors, millions of both incumbent and newly-hired workers have to go to an SSA field office to correct the mistake.

Another problem with the current system, which would be compounded by a mandatory E-Verify program, is a significant number of E-Verify inquiries result in erroneous "tentative nonconfirmation" notices. This means that the databases cannot immediately confirm that the employee is work-authorized. It is estimated that for every one million workers queried, 8,000 employees who are in fact work-authorized are informed they are not authorized to work. Further, it is estimated that in fiscal year 2010, 80,000 workers lost their jobs due to E-Verify. Under mandatory E-Verify, the Department of Homeland Security conservatively estimates that 1.2 million workers would have to visit a government agency or lose their job, and 770,000 would likely lose their jobs.

E-Verify expansion does not create American jobs, and instead would cause unnecessary harm to our economy.

While many in Congress assert that if we deport all undocumented workers U.S. citizens would move into these jobs, the job market is not so simple. Immigrants and native-born workers are not interchangeable. In reality, our economy is highly dependent on the low-wage, low-skill labor that undocumented workers provide. In the agriculture industry, most policymakers estimate that more than 75 percent of the labor force is undocumented. Deporting all undocumented workers – even assuming that would be possible – would be catastrophic for agriculture and our food supply.

The E-Verify program is having negative consequences on other aspects of our economy as well. In a time of mounting budget deficits, the federal government is spending $23 billion on a program that is of dubious value at best. Besides mistakenly flagging workers who are in fact authorized to work in the U.S., it was unable to detect over half of undocumented workers in FY 2010. The Congressional Budget Office (CBO) estimates that the cost of implementing mandatory E-Verify would be $3 billion in the first five years.

Moreover, most of the workers that E-Verify correctly identifies as undocumented are not leaving the country. Instead, they are going into the underground economy and no longer paying taxes. According to the CBO, implementation of a mandatory E-Verify program without fixing our broken immigration system will result in the loss of $17 billion in tax revenue.

Comprehensive immigration reform is the best course for U.S. workers, immigrants and our nation's struggling economy.

E-Verify is expensive and unworkable in its current form, and will become exponentially more so under a mandatory program. Our seniors, persons with disabilities and children will suffer even greater delays in receiving the benefits they so desperately need and deserve; millions more work-authorized employees will get caught in the net of system errors and our economy will suffer. Instead, AFSCME urges Congress to enact immigration legislation that builds on the economic contributions immigrants provide to our economy and offers an earned path to legalized status.

Prepared Statement of American Immigration Lawyers Association

AILA National Office
Suite 300
1331 G Street, NW
Washington, DC
20005-3142

Tel: 202.507.7600
Fax: 202.783.7853

www.aila.org

Crystal Williams
Executive Director

Susan D. Quarles
Deputy Executive Director

Statement before
House Subcommittee on Social Security of the Committee on Ways and Means
Hearing on the Social Security Administration's Role in Verifying Employment Eligibility

Thursday April 14, 2011
Statement of the American Immigration Lawyers Association

The American Immigration Lawyers Association (AILA) is a voluntary bar association of more than 11,000 attorneys and law professors practicing, researching, and teaching in the field of immigration and nationality law. Our mission includes the advancement of the law pertaining to immigration and nationality, and the facilitation of justice in the field. AILA appreciates the opportunity to offer a statement for the Subcommittee on Social Security of the Committee on Ways and Means' hearing addressing the "Social Security Administration's Role in Verifying Employment Eligibility". Our members' collective expertise and experience makes us particularly well-qualified to offer views that we believe will benefit the public and the government.

AILA members regularly advise and represent American companies, U.S. citizens, lawful permanent residents, and foreign nationals in seeking immigration benefits, including lawful admission to the United States, and in complying with U.S. immigration laws and regulations. Additionally, AILA members are very familiar with E-Verify, the internet-based employment eligibility verification system administered by the U.S. Citizenship and Immigration Services (USCIS) in partnership with the Social Security Administration (SSA). AILA members have worked closely with E-Verify employers and have advised them on evaluation of the system, implementation, management and oversight of accounts. AILA members also have experience with E-Verify employers that have been the subject of government investigations utilizing E-Verify data.

AILA supports governmental efforts to provide employers with effective means to verify that newly hired employees are authorized to work in the United States. AILA likewise concurs with DHS' overall policy goal that tools to verify employment authorization, such as E-Verify, should not be misused, abused, utilized to discriminate, breach privacy or facilitate fraudulent use of the USCIS' Verification Division information. However, any substantial expansion of E-Verify or any other employment verification system cannot take place without some form of legalizing the currently undocumented workforce.

Credible worksite enforcement is a logical component of any practical effort to fix our nation's broken immigration system. However, expansion of any employment verification system built on an inadequate platform and populated by flawed databases will create hardships for U.S. businesses, especially small businesses, in a time of economic challenge. It is misguided to think that any proposal, whether an expansion of E-verify or a new employment verification system, could work without providing a path to legal status for undocumented workers and their families who are already contributing to this economy, and suggests a failure to comprehend the scope and complexity of the situation.

AILA supports American workers and the integrity of our workforce. SSA has a clear, straightforward and vital mission that is to, "Deliver Social Security services that meet the changing needs of the public." Employment eligibility verification is not part of SSA's mission and only serves to divert resources away from its mission.

Enforcement-only policies will not fix our broken immigration system. What we need are solutions, not half measures that will only make the situation worse. Congress should consider a broad approach to immigration reform. Smart immigration policies that include a pathway to compliance for the millions of undocumented immigrants currently living and working in the U.S. would add billions of dollars to the economy and raise the wages of all American workers.

Prepared Statement of American Meat Institute

Testimony for Hearing of the U.S. House of Representatives Subcommittee on Social Security
Committee on Ways and Means

Thursday, April 14, 2011

STATEMENT OF J. PATRICK BOYLE, PRESIDENT and CEO,
AMERICAN MEAT INSTITUTE, WASHINGTON, D.C.

The Social Security Administration's Role in Verifying Employment Eligibility

The American Meat Institute is the largest and oldest meat and poultry trade association in the United States. AMI represents America's meatpackers and processors and their suppliers. Our member companies process 95 percent of red meat and 70 percent of turkey in the U.S. Headquartered in Washington, D.C., AMI monitors legislation, regulations and media activity that impacts the meat and poultry industry and provides rapid updates and analyses to its members to help them stay informed. In addition, AMI conducts scientific research through its Foundation, a 501(c) (3) organization, designed to help meat and poultry companies improve their plants and ensure the safety of their products.

The U.S. meat and poultry industry generates over $832 billion in our nation's economy representing 6 percent of GDP and employs more than 500,000 workers. The industry strongly supports efforts to achieve a practical and functional worksite electronic employment verification system and necessary tools to secure our nation's borders.

The U.S. meat and poultry industry is a strong advocate for the E-Verify program and supports its mandatory application, as long as it provides mechanisms for improvement as recommended below. Such a mandate should be phased in with universal participation over several years to better enable the government to administer the program, and launch a biometric component directed at eliminating identity theft on a pilot voluntary basis.

AMI's Members Have an Extensive History of Voluntary Use of E-Verify and Its Predecessor Basic Pilot Program

AMI's members have been in the forefront of the efforts to bring integrity to employment authorization verification process enacted by Congress in the Immigration Reform and Control Act IRCA) in 1986. After it became apparent that the paper-based employment authorization process was woefully inadequate to screen out fraudulent employment documents, Congress enacted the Illegal Immigration Reform and Immigrant Responsibility Act (IIRIRA) in 1996, establishing the Basic Pilot telephonic and electronic employment verification program. This

program was voluntary and was intended to screen out fraudulent social security numbers and alien work authorization documents provided by job applicants to employers at the time of hire.

In the mid-1990's, AMI members in the Midwest had their meatpacking operations disrupted when they were audited by the Immigration and Naturalization Service (INS) and informed that many of their experienced employees who were vital to their operations had provided fraudulent documents. These employers, in compliance with the paper-based employment verification procedures enforced by INS, were unable to screen out those who provided invalid work authorization documents. While AMI members typically were not cited by INS for violating the immigration laws, they had to terminate large numbers of employees in whom they had invested substantial training costs, they also suffered economic losses due to worker shortages.

Given these enforcement efforts, many AMI members took steps to more carefully scrutinize employment authorization documents and, ironically, faced discrimination charges under the unfair immigration-related employment practice provisions of IRCA for being too vigilant in seeking to employ legally authorized workers. Needless to say, AMI members were and continue to be frustrated by the vise in which they find themselves in trying to comply with IRCA's inherently contradictory provisions. Employers are required to walk an impossible legal tightrope due to the law's failure to provide "bright lines" for compliance.

AMI and its members took the initiative to address this problem by successfully urging Congress in 1999 to extend the scope of the Basic Pilot program beyond the original five pilot states to include the State of Nebraska, where many AMI members are located. This enabled a number of meatpacking companies to enter into agreements with INS to participate in the Basic Pilot program.

E-Verify Is Only Partially Effective. It Does Not Effectively Address the Problem of Identity Theft Involving Social Security Card Information Stolen from Others.

The experience of AMI members participating in the Basic Pilot and E-Verify programs has been mixed. The electronic verification mechanisms of the E-Verify have screened out a number of unauthorized workers at the point of hire and the mere fact that a company is participating in the program deters many individuals from even applying for work. The program, nonetheless, is only partially effective. It does not effectively solve the problem of identity theft, through which individuals who have stolen the name and social security or alien document numbers from their rightful owners who are authorized to work use the stolen information to gain employment. The system cannot determine whether the person presenting the name and document number is the person to whom they relate.

In addition, there are delays by DHS in updating its databases to include the most recent change in status of aliens. These delays can result in an employer receiving false information regarding whether an individual is or is not authorized to work. "Real time" updating of alien status information is critical to the effective functioning of the E-Verify program. It is costly and administratively burdensome for employers to hire and train an individual whom it believes is authorized to work, only to be later informed that a mistake was made and to have to terminate the individual.

Moreover, the E-Verify program does not have the ability to determine through its access to the Social Security Administration's (SSA) database when an individual's name and social security number are being reported by several employers at the same time, especially when the employers are not located in close proximity to each other. Such information should be more

effectively acquired and used to target individuals seeking employment who are engaged in identity fraud.

Unfortunately, the problem of identity theft is widespread and, notwithstanding the extensive use of the E-Verify program by meat and poultry processing companies, it has resulted in the continued disruption of AMI member companies.[1] There have been a number of highly publicized raids of well-known meat packing companies, including AMI member companies, that are participating in the E-Verify program and that have worked closely with DHS in attempting to comply with the law. DHS apparently targeted these companies upon receipt of information that a number of employees had engaged in identity theft. The raids of these companies have been devastating, resulting in significant disruptions of their operations and losses on the millions of dollars. The use of the E-Verify program by law-abiding companies that went the extra mile to seek a legal workforce has not served them well. It will continue as an inadequate system until Congress takes steps to correct its deficiencies.

Industry Position/Recommendations

The U.S. meat and poultry industry strongly supports a practical and functional worksite electronic employment verification system and necessary tools to secure our nation's borders. Inclusive or exclusive of broader immigration reform, the industry supports modifications and a phased in mandate of E-Verify. Several changes can be made to the current E-Verify system to improve the accuracy of results and lessen the burden on employers and employees.

First, employers must be given the tools to determine employee work eligibility. To combat true-identity theft, SSA and DHS must be required to inform employers if an employee's name and SSN are not only legitimate but – whether they are being used in multiple places of employment by persons who have stolen the identity of others.

Employers must also be given the tools to determine to the best of their ability the authenticity of documents provided to them to determine work eligibility of their employees. The number of documents that are currently allowed for submission to determine work eligibility must be reduced to avoid confusion and document fraud. Ideally, a unitary card or only several cards that can be used to establish employment authorization and identity are desirable. The verification system also should utilize or be required to move toward usage of biometric technology that can detect whether the person presenting a document that relates to a real person with a valid Social Security number or alien registration card is in fact the person to whom the card relates.

To lessen the burden on employers and employees, users of the E-Verify system must be given the tools to determine in real time or near real time the legal status of a prospective employee or applicant to work. DHS and the SSA must be given the resources to ensure that work authorization status changes are current and avoid the costs and disruption that stems from employers having to employ, train, and pay an applicant prior to receiving final confirmation regarding the applicant's legal status.

---

[1] In past testimony before this Subcommittee, Richard Stana, Director of Homeland Security and Justice, Government Accountability Office, testified that the prevalence of identity fraud is increasing, "a development that may affect employers' ability to reliably verify employment eligibility in a mandatory EEV program. The large number and variety of acceptable work authorization documents...along with inherent vulnerabilities to counterfeiting of some of these documents may complicate efforts to address identity fraud." "Hearing on Employment Eligibility Verification System," Subcommittee on Social Security, House Committee on Ways and Means, June 7, 2007.

To protect employers and encourage participation in the system, employers that comply with electronic employment eligibility verification requirements must be provided protection from discrimination lawsuits resultant from such compliance. This will require that the legislation establish clear-cut standards for use of the verification system and protection for employers from discrimination charges if applicants or employees are not hired or terminated after compliance with such standards.

Finally, Congress should mandate E-Verify for employers once these changes are addressed, phasing in universal participation over several years to better enable the government to administer the program, and launch a pilot biometric component directed at eliminating identity theft on a voluntary, fee for service basis.

Finally, we strongly urge that mandatory federal E-Verify legislation preempt state and local laws. There should be one clear-cut standard of compliance. Many AMI members operate in many states. The costs and difficulty of complying with multiple and differing state and local "E-Verify type laws" is frustrating for AMI's members.

We appreciate the opportunity to submit AMI's views on this subject, and your efforts to improve the electronic employment verification system. A practical and functional worksite electronic employment verification system is vital to achieving a stable, legal workforce and necessary to secure our nation's borders. The meat and poultry industry strongly supports your efforts to develop such a system. Thank you again for your time.

Name: J. Patrick Boyle, President & CEO, American Meat Institute

Organization: American Meat Institute

Address: 1150 Connecticut Avenue Northwest

12th Floor

Washington, DC 20036

Phone Number; (202) 487- 4248

Contact E-mail Address: bbeshears@meatami.com

Title of Hearing: Social Security Administration's (SSA's) Role in Verifying Employment Eligibility

Prepared Statement of Asian American Center for Advancing Justice

ASIAN PACIFIC AMERICAN LEGAL CENTER
ASIAN AMERICAN JUSTICE CENTER
ASIAN AMERICAN INSTITUTE
ASIAN LAW CAUCUS
MEMBERS OF ASIAN AMERICAN CENTER FOR ADVANCING JUSTICE

Written Statement Submitted by the Asian American Center for Advancing Justice

House Committee on Ways and Means
Subcommittee on Social Security

Hearing on Social Security Administration's Role in Verifying Employment Eligibility

April 14, 2011

Today, the U.S. House of Representatives' Subcommittee on Social Security will hold a hearing on the Social Security Administration's (SSA) role in verifying employment eligibility. The Asian American Center for Advancing Justice ("Center for Advancing Justice") would like to express deep concern and opposition to implementing a mandatory E-Verify program nationwide. Imposing mandatory E-Verify will have a destructive impact on workers, employers, and ultimately our economy.

Collectively, the members of the Center for Advancing Justice are non-profit, non-partisan organizations that enrich and empower the Asian American and Pacific Islander (AAPI) community and other underserved populations through public policy, advocacy, litigation, research and community education. Our mission is to promote a fair and equitable society for *all* by working for civil and human rights and empowering AAPIs and other underserved communities.

E-Verify will have a particularly devastating impact on AAPI workers and small business owners. A 2009 Westat report found the error rate for foreign-born workers was *20 times higher* than that of U.S.-born workers. For our community, this is particularly troublesome because more than 8 million AAPIs are foreign born. If E-Verify is made mandatory, a disproportionate number of AAPIs will be wrongly identified and have their jobs jeopardized. The E-Verify program is of particular concern for the Limited English Proficient members of our community. The already confusing E-Verify program will be impossible to navigate for the nearly 50% of the AAPI community who speak English less than very well – where citizen and legal resident workers alike will be unduly burdened by constant misidentifications in the system.

E-Verify promotes discrimination against AAPIs, as under-trained employers may assume a worker is undocumented and unduly fire the worker or simply not hire them at all. Many AAPIs, both citizens and non-citizens, may experience tentative non-confirmations (TNCs) simply because of name mismatches if employers are confused by complex names or name order. Government employees unfamiliar with foreign names and different naming conventions might also incorrectly enter information into the databases that E-Verify uses to confirm work authorization, which also leads to errors in the confirmation process. According to USCIS,

22,512 TNCs (76% of which were for citizens) resulted from name mismatches in 2009. Other TNCs can arise when government files are not updated, like in the case of Fane:

Fane is a Tongan woman, and a naturalized U.S. citizen since 1993. When Fane started a new position at a security company, her employer told her that there was a problem with her I-9 work authorization where she received a company letter asking her to verify her eligibility to work. Fane went immediately to the Social Security Administration (SSA), where she received written verification that her social security number matched her identity. But despite showing her company the SSA verification, her U.S. passport and her Certificate of Naturalization, her company informed her that she was not allowed to return to work because her name was flagged as still having problems. As a result, Fane lost her job. This has caused extreme hardship for her, as she is a single mother. Fane was flagged simply because when she naturalized the Department of Homeland Security (DHS) did not tell SSA that she had become a U.S. citizen. This is a problem that many AAPI immigrants face, as they do not know to inform SSA of their change in citizenship status themselves.

A U.S. Department of Homeland Security study found that employer noncompliance with the E-Verify pilot program's rules was "substantial," where: 1) employers engaged in prohibited practices such as pre-employment screening, 2) took adverse employment actions based on tentative non-confirmation notices, and 3) failed to inform employees of their rights. A recent report by the U.S. General Accountability Office also indicates that USCIS remains limited in its ability to identify and prevent employer misuse of the E-Verify program, with no authority to impose penalties against employers misusing the system. Making E-Verify mandatory gives advantage to unscrupulous employers that find ways around the system.

The GAO report also stated that resolving tentative and false non-confirmations, as well as combating discrimination, remains challenging for employees. Responding to TNCs can be very time-consuming and confusing for workers. When workers have an error in their records, they often have to take unpaid time off from work to follow up with SSA, which may take more than one trip. In fiscal year 2009, 22% of workers spent more than $50 to correct database errors and 13% spent more than $100. Moreover, in 2009, the wait times for SSA office visits were 61% longer than they were in 2002. American Council on International Personnel members report that corrections at SSA usually take in excess of 90 days, and that employees must wait four or more hours per trip, with repeated trips to SSA frequently required to get their records corrected.

E-Verify will also increase the regulatory burden on employers, particularly small business owners, and siphon off already scarce governmental and financial resources. E-Verify would require all employers to spend money on compliance training, employee verification, and capable infrastructure for electronic submission and verification. These compliance costs will disproportionately affect small businesses, which have fewer resources to spare. Throughout the U.S., AAPIs own more than 1.1 million small businesses, the majority of which have small workforces and cannot afford to lose any employees actually qualified to work. According to the U.S. Census Bureau, these businesses have provided jobs to 2.2 million employees, had receipts of $326.4 billion, and generated payroll of $56 billion. With the flagging economy, we cannot afford to burden AAPI businesses any further.

Lastly, the U.S. cannot afford to divert scarce governmental and financial resources towards

funding this deeply flawed program. According to the U.S. Congressional Budget Office (CBO), implementation of a mandatory program (without legalizing the current undocumented population) would increase the number of employers and workers who resort to the black market, outside of the tax system. This would decrease federal revenue by more than $17.3 billion over ten years. Making E-Verify mandatory will worsen our deficit in the long run. Mandating use of E-verify for all employers will tax the resources of an already overburdened SSA. During the period March 1, 2009 through April 30, 2010, about 3.1 million visitors waited more than 1 hour for service, and of those visitors, over 330,000 waited more than 2 hours. Further, in fiscal year 2009, about 3.3 million visitors left a field office without receiving service.

Therefore, for the reasons aforementioned, we oppose a mandatory E-Verify program. Instead of layering E-Verify on top of a broken immigration system, we need to fix the system. We need broad reform of our immigration system that includes a path to legal status for unauthorized immigrants. This would result in a large economic benefit—a cumulative $1.5 trillion in added U.S. gross domestic product over 10 years. Thank you.

Prepared Statement of Jessica St Pierre

Statement of Jessica St. Pierre

U.S. Citizen, Negatively Impacted by E-Verify

House Committee on Ways and Means

Subcommittee on Social Security

Hearing on the Social Security Administration's Role in Verifying Employment Eligibility

April 14, 2011

My name is Jessica St. Pierre and I am a U.S. citizen, born and raised in Florida. On November 09, 2010, my life changed forever because I was fired due to an error in the employment verification system called E-Verify. I was wrongly identified as not having employment authorization. After my firing, I remained unemployed for months. This is my story.

I was fired from my job despite providing supporting documents to government agencies and my employer and explaining over and over again that I was authorized to work in the United States. At first, my employer indicated that there was problem with my work authorization and suggested I visit the Social Security Administration (SSA) office. My father and I went to my local SSA office and they told us everything was correct in their system. This office gave me a print-out indicating that my information matched, but the print-out did not indicate that I was work-authorized. After my first trip to the SSA office, I told my employer about the document and they said it wasn't enough, noting that "Well that's not what it says in our system." It was only then that my employer told me that they were using E-Verify and that the program indicated that there was an error.

As the days and weeks passed, I tried to correct this error, in vain, in numerous ways. For example, the following week, I went down to a legal services organization and they referred me to the Equal Employment Opportunity Commission (EEOC). When I talked with my local EEOC office, they told me that I didn't really have case but advised me to call E-Verify and find out what was going on. I took the advice and immediately researched the number to E-Verify. I called the hotline and waited almost an hour just to hear the representative say that after running my name in the system that everything is okay. I felt relieved and I asked if she could send that documentation in the mail so that I could take it back to my employer. She said that she could not send me this information, but could contact my employer. I said okay and asked her to do so. Again, I could not receive any information

confirming E-Verify's error. Despite the call from the E-Verify program, my employer still could not straighten out this mess. I thought a call from E-Verify to my employer would get my job back, but I contacted the employer and was told there was nothing I could do to get my job back. In desperation, I went back to my local SSA office and received the same print-out—the document that had failed me before—from SSA staff.

Angry and frustrated, I thought knew this wasn't right. I have done everything right, including going to all the proper agencies to get this situation resolved. What else is a worker supposed to do? I was hurt and because I felt helpless and like there was nothing that I could do even though I followed all the right steps. I had decided to just give up but then decided to Google exactly what I got fired for "failure to provide employment eligibility". I was shocked to find an article on what I was going through and with that article were other stories of people who are US citizens going through the exact same thing! I was not alone and now I knew there was a number that I could call to share my story and I did. In the month of December I contacted the National Immigration Law Center and they were ready to help free of charge. They did everything in their power to get me the answer that I was looking for. As it turns out, the employer had placed two spaces after my last name which prompted and SSA tentative nonconfirmation (TNC). Four months later in February 2011, I met with the employer and they claimed I could come back to my position. However, after being out of work over 3 months, I have since moved on to another company. Though my current position has significantly lower pay, I realized that the money wasn't what motivates me. This employer didn't put me through the E-Verify rollercoaster ride, so I decided to stay with my new job. I would like to take this time out to thank the NILC for all of their time, patience, and hard work. For I know without them I probably would have never known that there was an answer to my problem.

Prepared Statement of Joint Committee on Taxation

THE SOCIAL SECURITY ADMINISTRATION'S ROLE IN VERIFYING EMPLOYMENT ELIGIBILITY: BACKGROUND AND PRESENT LAW RELATING TO SECTION 6103 AND EMPLOYMENT VERIFICATION

Scheduled for a Public Hearing
Before the

HOUSE COMMITTEE ON WAYS AND MEANS
SUBCOMMITTEE ON SOCIAL SECURITY
On April 14, 2011

Prepared by the Staff
of the
JOINT COMMITTEE ON TAXATION

April 12, 2011
JCX-25-11

CONTENTS

Page

INTRODUCTION 1

OVERVIEW OF SECTION 6103 AND TAX RELATED PENALTIES 2

INTRODUCTION

The House Committee on Ways and Means Subcommittee on Social Security has scheduled a public hearing on the Social Security Administration's role in verifying employment eligibility on April 14, 2011. The hearing will focus on the progress made, and challenges created, by E-Verify, an internet-based system designed to electronically verify work eligibility and operated by the Department of Homeland Security ("DHS") and the Social Security Administration ("SSA"). The Subcommittee will examine ways to improve the system and, in that context, review various proposals to expand employment eligibility verification, including increasing enforcement through the sharing of taxpayer wage information and taxpayer identity information.

The proposals that provide for increase enforcement through sharing of taxpayer wage information and taxpayer identity information require amendments to the Internal Revenue Code[1] which classifies this information as confidential return information protected by section 6103 and prohibits its disclosure except under specifically identified circumstances.

This document,[2] prepared by the staff of the Joint Committee on Taxation and submitted to the House Committee on Ways and Means Subcommittee on Social Security, provides a brief overview of section 6103 of the Code which prohibits disclosure of tax returns and tax return information except in specific circumstances, such as disclosure of certain tax return information to the SSA.

[1] Unless otherwise stated, all section references and reference to the "Code" are to the Internal Revenue Code of 1986, as amended.

[2] This document may be cited as follows: Joint Committee on Taxation, *The Social Security Administration's Role in Verifying Employment Eligibility: Background and Present Law Relating to Section 6103 and Employment Verification* (JCX-25-11), April 12, 2011. This document is available on the internet at www.jct.gov.

OVERVIEW OF SECTION 6103 AND TAX RELATED PENALTIES

Background

Congress reviewed the tax information disclosure rules in depth in 1976.[3] At that time, the rules had not been reviewed by Congress for 40 years and a growing number of rules allowing disclosure of tax information had been established by executive order. Prior to 1976, tax returns were considered public records, and were subject to disclosure pursuant to executive order. There was substantial controversy over the extent of actual and potential disclosure of returns and return information to other Federal and State agencies for nontax purposes and whether such disclosures breached a reasonable expectation of privacy on the part of the American citizen with respect to such information. This controversy led to the concern as to whether the public's reaction to such an abuse of privacy would impair compliance with the Federal voluntary tax assessment system. In addition, questions were raised about whether tax returns and tax information should be used for any purpose other than tax administration.[4]

Due to concerns regarding the possible misuse of returns and return information, section 6103 was amended in the Tax Reform Act of 1976. In reviewing each of the areas in which returns and return information were subject to disclosure, Congress sought to balance a particular office's or agency's need for the information with the citizen's right to privacy and the related impact of the disclosure upon the necessary continuation of voluntary compliance with the country's tax assessment system. Legislation at that time clarified the rules governing disclosure of taxpayer return information, providing that returns and return information are confidential and not subject to disclosure except in those limited circumstances set forth in section 6103 in which Cougress determined that disclosure was warranted.

General rule and scope of information protected by section 6103

Under present law, section 6103 provides that returns and return information are confidential and may not be disclosed by the IRS, other Federal employees, State employees, and certain others having access to such information except as provided by specified exceptions.

---

[3] For further detail, see Joint Committee on Taxation, *General Explanation of the Tax Reform Act of 1976* (JCS-33-76) December 29, 1976 at 314; 1976-3 C.B. 314 (Vol. 2) at 326.

[4] As the Senate Finance Committee noted: "It has been stated that the IRS probably has more information about more people than any other agency in this country. Consequently, almost every other agency that has a need for information about U.S. citizens, therefore logically seeks it from the IRS. However, in many cases, the Congress has not specifically considered whether the agencies which have access to tax information should have that access. . . Questions have been raised and substantial controversy created as to whether the present extent of actual and potential disclosure of return and return information to other Federal and State agencies for nontax purposes breaches a reasonable expectation of privacy on the part of the American citizen with respect to such information. . . In a more general sense, questions have been raised with respect to whether tax returns and tax information should be used for any purposes other than tax administration...[R]eturns and return information should generally be treated as confidential and not subject to disclosure except in those limited situations delineated in the newly amended section 6103 where the committee decided that disclosure was warranted." S. Rep. No. 94-938 at 317, 1976-3 CB 355.

Returns and information returns (including Forms W-2)

A "return" means any tax or information return, declaration of estimated tax, or claim for refund which, under the Code, is required (or permitted) to be filed on behalf of, or with respect to, any person. It also includes any amendment, supplemental schedule or attachment filed with the tax return, information return, declaration of estimated tax or claim for refund. For example, Form W-2, Wage and Tax Statement, is an information return, and is the return of both the employer who filed it with the IRS and the employee with respect to whom it was filed.

Return information

The Code defines "return information" broadly. It includes a taxpayer's identity (the name of the person with respect to whom a return is filed, his or her mailing address, his or her taxpayer identifying number ("TIN"), social security number ("SSN") or a combination thereof). In addition to taxpayer identity, return information includes any information gathered by the IRS with regard to a taxpayer's liability under the Code, including the following data:

- the nature, source or amount of income, payments, receipts, deductions, exemptions, credits, assets, liabilities, net worth, tax liability, tax withheld, deficiencies, overassessments, or tax payments;
- whether the taxpayer's return was, is being, or will be examined or subject to other investigation or processing;
- any other data, received by, recorded by, prepared by, furnished to, or collected by the Secretary with respect to a return or with respect to the determination of the existence, or possible existence, of liability (or the amount thereof) of any person under this title for any tax, penalty, interest, fine, forfeiture, or other imposition, or offense;
- any part of any written determination or any background file document relating to such written determination which is not open to public inspection under section 6110;
- any advance pricing agreement entered into by a taxpayer and the Secretary and any background information related to the agreement or any application for an advance pricing agreement; and
- any agreement under section 7121 (relating to closing agreements), and any similar agreement, and any background information related to such agreement or request for such agreement (sec. 6103(b)(2)).

The term "return information" does not include data in a form that cannot be associated with or otherwise identify, directly or indirectly, a particular taxpayer. However, return information with the identifiers (name, address, SSN) simply removed is still protected by section 6103.

Taxpayer return information

"Taxpayer return information" is another defined term for purposes of section 6103 and is a subset of return information. Taxpayer return information means return information that is

filed with, or furnished to, the IRS by or on behalf of the taxpayer to whom such return information relates. For example, information filed with the IRS by a taxpayer's attorney or accountant is taxpayer return information. Information transcribed directly from a taxpayer's return is taxpayer return information. Thus, identity information taken from a return or information return is taxpayer return information. The distinction between return information and taxpayer return information is significant for the disclosures of nontax criminal matters for which a court order generally is required to obtain taxpayer return information.

Exceptions to the general rule of confidentiality

Section 6103 contains a number of exceptions to the general rule of confidentiality that permit disclosure in specifically identified circumstances when certain conditions are satisfied.[5] The primary use of tax information is for tax administration purposes, which is addressed in several broadly drawn exceptions.[6] For nontax civil matters, section 6103 provides narrowly tailored exceptions that generally provide the minimum amount of information necessary to achieve the requesting agency's purpose. As discussed above, the tailoring of the exceptions reflects the balance between a taxpayer's legitimate expectation of privacy in their communications with the IRS and an agency's nontax program need, and is based on the notion that maintenance of an expectation of privacy promotes tax compliance.

Nontax criminal matters (section 6103(i))

In the case of criminal matters unrelated to tax administration, Congress has indicated that a taxpayer's communications with the IRS, which are compelled by the Internal Revenue Code, should be afforded the same degree of privacy as those private papers maintained in a taxpayer's home:

> The Committee decided that the information that the American citizen is compelled by our tax laws to disclose to the Internal Revenue Service was entitled to essentially the same degree of privacy as those private papers maintained in his or her home. Present law and practice does not afford him that protection – the Justice Department and other Federal agencies, as a practical matter, being able to obtain that information for nontax purposes almost at their sole discretion.[7]

---

[5] See section 6103(c) (disclosure by taxpayer consent); 6103(d) (disclosure to State tax officials); 6103(e) (disclosure to persons having material interest); 6103(f) (disclosure to committees of Congress); 6103(g) (disclosure to the President and certain other persons); 6103(h) (disclosure to Federal officers and employees for tax administration purposes); 6103(i) disclosure to Federal officer and employees for administration of Federal laws not relating to tax administration); 6103(j) (statistical usc); 6103(k) (disclosure of certain returns and return information for tax administration purposes); 6103(l) (disclosure for purposes other than tax administration); 6103(m) (disclosure of taxpayer identity information); 6103(n) (tax administration contractors); and 6103(o) (disclosure of return and return information with respect to certain taxes).

[6] For example, see secs. 6103(f)(1) and (2), 6103(h), and 6103(k).

[7] S. Rep. No. 94-938 at 328.

For criminal matters unrelated to tax administration, present law section 6103(i) draws a distinction between returns and information provided by the taxpayer or his or her representative to the IRS ("taxpayer return information") and all other return information. Return information that is not also within the subset of data known as taxpayer return information includes witness statements or records gathered by the IRS from third party sources (e.g., witnesses and banks). Stricter requirements must be met to obtain returns and taxpayer return information.[8]

To obtain a return or return information that was provided to the IRS by the taxpayer or his or her representative (taxpayer return information), an ex parte court order must be obtained. Such order is made only if the court finds that the application for the court order meets certain specificity and relevancy requirements.[9]

In contrast, for return information (other than taxpayer return information) a court order is not required and may be disclosed upon receipt of a written request, meeting the statutory content requirements, from the head of a Federal agency and certain other statutorily identified persons. In addition, on its own accord and without a written request, the IRS may disclose return information (other than taxpayer return information) in writing which may constitute evidence of a violation of nontax Federal criminal law to the head of a Federal agency responsible for administering such law.[10] The IRS may also disclose return information to Federal and State law enforcement agencies in cases of imminent danger of death or physical injury.[11]

Exception for disclosures to the Social Security Administration

For purposes of administering the Social Security Act, present law authorizes disclosure to the Social Security Administration ("SSA"), upon written request, of returns and return information relating to self-employment taxes (Chapter 2 of the Code); Federal Insurance Contributions Act ("FICA") taxes (Chapter 21 of the Code); and taxes withheld at the source on wages (Chapter 24 of the Code).[12]

Documents which may be disclosed to the SSA under this provision include but are not limited to:

- Schedule C, Form 1040, Profit (or Loss) from Business or Profession,

---

[8] Sec. 6103(i)(1)(A).

[9] See sec. 6103(i)(1). While less restrictive standards apply to disclosures related to terrorism investigations, an ex parte court order is still required to obtain returns and taxpayer return information. Sec. 6103(i)(7)(C).

[10] Sec. 6103(i)(3)(A).

[11] Sec. 6103(i)(3)(B).

[12] Sec. 6103(l)(1)(A).

- Schedule E, Form 1040, Supplemental Income Schedule-Part III, Income or Loss from Partnerships,
- Schedule F, Form 1040, Farm Income and Expenses,
- Schedule SE, Form 1040, Computation of Social Security Self-Employment Tax,
- Form 1065, U.S. Partnership Return of Income,
- Form 941, Employer's Quarterly Federal Tax Return,
- Form 942, Employer's Quarterly Tax Return for Household Employees or portions Schedule H, Form 1040,
- Form 943, Employer's Annual Tax Return for Agricultural Employees,
- Form W-2, Wage and Tax Statement (limited to those portions of the W-2 relating to Chapters 21 and 24), and
- Return information related to the bullets above.[13]

For administering section 1131 of the Social Security Act, Code section 6103(l)(1)(B) authorizes disclosure to the SSA of return information described in section 6057(d) pertaining to pension, profit-sharing, stock bonus plans, etc. to which part I of subchapter D of Chapter 1 of the Code applies.[14]

Section 6103(l)(5) authorizes disclosure of information returns to the SSA for: (1) carrying out an effective returns processing program; (2) the Combined Annual Wage Reporting ("CAWR") Program; and (3) certain disclosures for epidemiological and similar research. The information returns which may be disclosed under section 6103(l)(5) are those filed under Part III, Subchapter A, Chapter 61 of the Internal Revenue Code. These include primarily Form W-2; Form W-3 (Transmittal of Wage and Tax Statements); and Form 1099-R (Distributions from Pensions, Annuities, Retirement or Profit Sharing Plans, IRAs, Insurance Contracts, etc).[15]

Safegnards against and penalties for unauthorized disclosure or inspection of returns and information

Safeguards

Section 6103 requires as a condition for receiving tax information, that recipient agencies establish, to the satisfaction of the IRS, physical, administrative and technical safeguards to the

[13] Internal Revenue Service, Internal Revenue Manual, *Disclosure of Official Information: Administration of the Social Security Act - Social Security Administration*, Ch. 11.3, sec. 11.3.29.3 (9-1-2009).

[14] Section 6057(d) covers statements, notifications, reports and other information received by the IRS pursuant to the annual plan registration requirements of section 6057. Section 1131 of the Social Security Act relates to notification of Social Security claimant with respect to deferred vested benefits.

[15] Internal Revenue Service, Internal Revenue Manual, *Disclosure of Official Information: Disclosure of Information Returns to Social Security Administration*, Ch. 11.3, sec. 11.3.29.3.2 (9-1-2009).

protect the confidentiality of the information received.[16] Such safeguards include a standardized system of records with respect to requests for disclosure of tax information and the reason for such disclosure, secure storage for the tax information, restrictions which limit access to the tax information to persons whose duties and responsibilities require access, and other safeguards as the IRS deems appropriate. The IRS is to review the safeguards established by such agencies and is permitted to terminate access if the safeguards are found unsatisfactory.

Civil and criminal penalties for unauthorized disclosure or inspection

The Code provides for criminal penalties and civil damages in the event of an unauthorized disclosure. The willful unauthorized disclosure of tax information is a felony punishable by a $5,000 fine, up to five years imprisonment, or both.[17] Willful unauthorized inspection of tax information is a misdemeanor punishable by a $1,000 fine, up to one-year imprisonment or both.[18] Federal employees and officers are required to be discharged from employment upon conviction of willful unauthorized disclosure or inspection.

An action for damages against the United States is permitted when any Federal officer or employee knowingly or by reason of negligence inspects or discloses tax information in violation of any provision of section 6103.[19] A plaintiff is entitled to: (1) actual damages sustained as a result of unauthorized disclosure (including punitive damages for willful or grossly negligent disclosures), or (2) liquidated damages of $1,000 per disclosure, whichever is greater, as well as costs of the action and in certain cases, attorney fees. No liability arises from a good faith but erroneous interpretation of section 6103 or a disclosure made at the request of the taxpayer.

---

[16] Sec. 6103(p)(4). See also Internal Revenue Service, Publication 1075, *Tax Information Security Guidelines for Federal, State and Local Agencies: Safeguards for Protecting Federal Tax Returns and Return Information* (Rev. 6/2000).

[17] Sec. 7213(a)(1).

[18] Sec. 7213A(a)(2)(b).

[19] Sec. 7431.

Prepared Statement of National Committee to Preserve Social Security and Medicare

NCPSSM **National Committee to Preserve Social Security and Medicare**

Barbara B. Kennelly
President & CEO

Statement for the Record by Barbara B. Kennelly, President and CEO
National Committee to Preserve Social Security and Medicare
10 G Street, N.E. Suite 600
Washington, DC 20002

House Committee on Ways and Means
Subcommittee on Social Security

Hearing on the Social Security Administration's Role in Verifying Employment Eligibility

April 13, 2011

As President and Chief Executive Officer of the National Committee to Preserve Social Security and Medicare, I appreciate the opportunity to submit this statement for the record. With millions of members and supporters across America, the National Committee is a grassroots advocacy and education organization devoted to the retirement security of all citizens.

Chairman Johnson, Ranking Member Becerra and members of the Subcommittee on Social Security, the National Committee appreciates your holding this hearing to examine the impact of a national employment verification system on the Social Security Administration's ability to serve retirees, people with disabilities, and workers of all ages.

Mr. Chairman, the members and supporters of the National Committee are very concerned about the negative consequences of expanding the E-Verify program, which would assign new immigration-related workloads to an already overburdened Social Security Administration (SSA). Creating a national employment verification system, using SSA databases and employees, to confirm the employment status of every American worker would divert crucial resources from an already overburdened agency thus impeding its central mission of serving its own beneficiaries. As the President and CEO of an organization that has worked tirelessly to enhance the financial resources of the Social Security Administration, I am deeply troubled by the effect this new, mandatory workload would have on the agency's ability to continue providing services to its core beneficiaries – the American workers who contribute their Social Security payroll taxes year after year to this program and who have earned a right to collect Social Security benefits in a timely manner.

Our Primary concern with proposals to expand the E-Verify program is the high cost imposed on SSA at a time when it is struggling to maintain adequate service delivery, reduce backlogs, and adjust to recent cuts to its already underfunded budget. According to a 2008 Congressional Budget Office report, the cost to SSA of extending and expanding the E-Verify program would be more than $1 billion – nearly 10 percent of the agency's administrative budget – in just the first year of implementation. Over 10 years, the plan would cost over $9 billion. Even though the authors of such legislation have the highest expectations that sufficient appropriations will be provided to cover these costs, recent experience with legislators implementing and demanding more cuts to SSA leads us to believe that the agency would not be provided with sufficient resources to handle this massive new workload.

As you are well aware, the Social Security Administration is already facing several significant challenges. Over the last few years, SSA has experienced a dramatic increase in retirement, survivor, disability, and Supplementary Security Income claims. The additional claims receipts are driven by the initial wave of the nearly 80 million baby boomers who will be filing for Social Security benefits by 2030 – an average of 10,000 per day. Concurrently, the recent economic downturn has caused new disability claims to skyrocket.

Nationwide, over 3.2 million new disability claims were filed and sent to the Disability Determination Services in FY 2010. This surge of increased claims has created backlogs of pending initial disability claims. Despite these unprecedented challenges, SSA continues to utilize the modest additional resources received in the last three fiscal years to clear more disability claims and hearings cases. Unfortunately, the number of claims and hearings pending is still not acceptable to Americans who need Social Security or Supplemental Security Income for their basic income, health care costs, and support of their families.

The increased number of claims has imposed a significant strain on SSA field offices charged with processing the additional claims and providing other vital services to the American public. Nationally, visitors to Field Offices increased from 41.9 million in FY 2007 to 45.4 million in FY 2010. SSA is also experiencing unprecedented telephone call volumes, and in FY 2010, SSA completed 67 million transactions over the 800-Number telephone network.

Currently, the agency is attempting to address the FY 2011 workload demands with FY 2010 resource levels. As a consequence of operating at this inadequate funding level, the agency has had to institute a number of cutbacks that further threaten its ability to deliver quality service to the public, including a hiring freeze and termination of most employee overtime. Most recently, SSA has had to suspend the mailing of annual earnings and benefits statements to millions of tax payers. These statements play a vital role in communicating to American workers important information about the Social Security program: estimates of the amount of benefits they will receive in retirement or if they become disabled so they may properly prepare for a secure retirement.

Given the strain on the workload SSA currently faces and the likelihood of continued uncertainty in funding, the National Committee is sympathetic to the situation the agency faces in determining what activities can be funded and what activities must be suspended due to lack of administrative resources. Therefore, we are very concerned about the impact of expanding the E-Verify program and accompanying increase in workloads on an already overburdened agency. Any increase in SSA's workload without a comparable increase in funding would further divert SSA from its central mission of serving its own beneficiaries – the elderly, people with disabilities, and workers of all ages who have contributed and earned the right to collect Social Security benefits in a timely manner. SSA's resources are already being stretched thin by a dramatic increase in claims and a disability backlog challenge while at the same time, the agency is being asked to operate at reduced funding levels. As a result, strains are being placed on other agency services, especially those in local offices where customers are experiencing long waits and unanswered phones. As always, SSA employees are making a strong effort to maintain their high level of productivity and quality service, but it is becoming increasingly difficult.

The National Committee is not taking a position on the underlying goals of any of the immigration bills before the Congress. However, we believe it would be a significant mistake to require SSA to take on the burden of verifying the work status of every American for immigration-related purposes. Given the limited resources that SSA currently has— and the possibility of even further reductions— to carry out its obligations to America's seniors and people with disabilities, we believe it would be unwise to encumber SSA with these costly and unrelated responsibilities and would frustrate the agency's ability to carry out its core responsibilities to America's seniors and people with disabilities.

Prepared Statement of National Council of Social Security Management Associations

United States House of Representatives
Subcommittee on Social Security
of the Committee on Ways and Means

Statement by

Joe Dirago
President
National Council of Social Security Management Associations, Inc.

Oversight Hearing on the Social Security Administration's Role in Verifying Employment Eligibility
April 14, 2011

Chairman Johnson, Ranking Member Becerra, and Members of the Subcommittee, my name is Joe Dirago and I am President of the National Council of Social Security Management Associations (NCSSMA). I have been the manager of the Social Security office in Newburgh, New York for ten years and have worked for the Social Security Administration for 31 years, with 27 years in management. On behalf of our membership, I am pleased for the opportunity to submit this statement to the Subcommittee regarding our concerns on Employment Eligibility Verification and the potential impact on the Social Security Administration (SSA).

NCSSMA is a membership organization of nearly 3,400 SSA managers and supervisors who provide leadership in 1,299 community based Field Offices and Teleservice Centers throughout the country. We are the front-line service providers for SSA in communities all over the nation. We are also the federal employees many of your staff members work with to resolve problems and issues for your constituents who receive Social Security retirement benefits, survivors, disability benefits, and Supplemental Security Income. Since the founding of our organization over forty-one years ago, NCSSMA has considered our top priority to be a strong and stable SSA, one that delivers quality and prompt locally delivered service to the American public. We also consider it a top priority to be good stewards of the taxpayers' moneys.

In May 2008, our organization testified before this Subcommittee on issues related to a mandatory employment eligibility verification system and the potential impact on the Social Security Administration. This statement for the record provides current information and challenges for SSA with the current E-Verify system, key issues confronting our agency, a review of SSA's funding situation, and an assessment of what increasing SSA's role in immigration verification would mean to service delivery.

NCSSMA has critical concerns about the dramatic growth in our workloads and receiving the necessary funding to maintain service levels vital to millions of people. Despite agency strategic planning, expansion of online services, significant productivity gains, and the best efforts of management and employees, SSA still faces many challenges to providing the service that the American public has earned and deserves.

The Social Security Number for Employment Eligibility & Identity Purposes

When the Social Security Act was enacted in 1935, Social Security Numbers (SSN) were established to credit workers with earnings accumulated that eventually entitled them to benefits. The SSN was never intended to be a national identifier. Use of the Social Security Card to assist in determining eligibility for employment was first authorized in 1986, more than 50 years after the first SSN was issued. At that time, employers were required to confirm the eligibility of their new employees by reviewing the original Social Security Card. If the card was not available, the employer was allowed to contact SSA to verify that the SSN matched the new employee's name and age. A voluntary Employer Enumeration Verification System (EEVS) was created to allow employers with a large volume of new hires to check their status quickly.

Because of the prevalence of undocumented workers in certain areas of the country, an electronic verification system known as "Basic Pilot" was established as a joint venture between the U.S. Citizenship and Immigration Service (USCIS) in the Department of Homeland Security (DHS) and SSA's EEVS, as part of the Illegal Immigration Reform and Immigrant Responsibility Act of 1996. The pilot was originally limited to five states: California, Illinois, Florida, New York, and Texas, as these were the states with the largest estimated populations of non-citizens not lawfully present in the United States. Nebraska was added to the Basic Pilot in 1999 due to the prevalence of undocumented workers in the meat packing industry in that state. Employers in these six states were then allowed to expand the program to their locations in other states. National use of the Basic Pilot was authorized in 2003.

DHS introduced the E-Verify system in 2007, which is an updated version of Basic Pilot and in current use. E-Verify is an easy to use web-based system that allows participating employers to determine whether newly hired employees are authorized to work in the United States under immigration law. While DHS is responsible for enforcing the prohibitions on unauthorized employment, SSA plays a key role in the voluntary verification process.

The E-Verify program allows employers to verify employee information taken from the Employment Eligibility Verification Form (Form I-9) against more than 455 million SSA records, more than 122 million Department of State passport records, and more than 80 million DHS immigration records. Employers may use the program once a hiring commitment is made to an employee to verify employment eligibility. If information on the records is discrepant, the employer receives a "tentative non-confirmation notice" (TNC). The notice indicates the source of the discrepancy, and issues a notice to the employee giving them eight days to contact DHS or SSA as appropriate to correct the discrepancy and to keep his/her job. If SSA requires additional information from the employee, more time is provided to correct the discrepant record.

E-Verify is available in all 50 states, the District of Columbia, Puerto Rico, Guam, and the U.S. Virgin Islands. Under federal law, the program is voluntary for employers except for participation by federal agencies, the legislative branch, and federal contract holders. State and local governments in 19 states and 25 localities have also required some level of E-Verify usage. Four states, Arizona, Mississippi, South Carolina, and Utah, and seven localities in California and Nebraska have made the use of E-Verify mandatory for most or all employers in their jurisdictions. The U.S. Citizenship and Immigration Services (USCIS) reports more than

246,000 employers are enrolled in E-Verify, representing more than 850,000 locations. In FY 2010, 16.5 million queries of the E-Verify system were processed. USCIS figures show that 98.3% of employees submitted for verification through E-Verify were automatically confirmed as work authorized. Another 0.3% were confirmed after resolution of the mismatch, and only 1.43% of employees submitted were found not authorized to work.

On March 21, 2011, the Secretary of Homeland Security announced the launch of E-Verify Self Check, allowing prospective employees to access their own information from DHS and SSA systems. This service allows job applicants to check their work-authorized status and correct any discrepancies on federal databases before applying for a job. It is currently available in five states and the District of Columbia, and will be expanded to the rest of the country on a rolling basis.

A number of immigration reform proposals include provisions mandating verification for all 7.7 million private and public sector employers throughout the country. Some proposals, such as H.R. 693, would make the use of E-Verify permanent and mandatory. The majority of employment verification proposals would rely on SSA to play a major role because the agency has a database with information about the entire American workforce, including information on citizenship status.

Challenges for SSA with the Current E-Verify System

Although usage of E-Verify has increased in recent years, it is only used by 11% of the nation's current employers. In a "mandatory use" state such as Arizona, only one-third of its employers use E-Verify. This makes it difficult to project exactly how great an impact E-Verify would have on SSA's workloads if it were mandated nationally, as proposed in H.R. 693. According to USCIS statistics, 1.7% of E-Verify cases are discrepant and almost always require at least one visit to a local SSA office. Information provided by SSA's Office of Budget for an OIG report on E-Verify indicates SSA may see between 210,000 and 700,000 additional visitors at Field Offices over a five-year period. This number constitutes a 5% to 16% increase in visitor traffic to Social Security Field Offices. SSA Field Offices that would be most affected by the mandatory use of E-Verify are already struggling with large volumes of visitors and extensive waiting times. Given the reality of the federal budget process, TNC cases would create still longer waiting times, and negatively affect the ability of Field Office employees to complete core Social Security business.

Not only would the universal use of E-Verify generate a significant number of additional contacts with SSA, there are also problems and limitations related to the process that must be acknowledged regarding use of the program as an employment eligibility verification system.

- **Employer Input Error:** While DHS has added an alert to the employer to reduce the number of input errors made by employers, these errors still occur. The accuracy of the Numident check is only as good as the information input by the employer using the system. Sometimes the difference of a letter in a name (i.e. "Gregg" instead of "Greg") can create a tentative non-confirmation message. Date of birth and SSN input errors can also create this

problem. These errors can cause workers to make unnecessary trips to Social Security Field Offices in order to correct problems that do not exist.

- **Discrepancies in Names Due to Marriage or Language:** While newly married individuals who take their spouse's name should change their records with the Social Security Administration, there is often a delay in doing so. This discrepancy can cause a tentative non-confirmation message. In addition, differences in language customs can cause discrepancies between DHS and SSA records. In either case, eligible employees would receive a TNC notice and require a visit to an SSA Field Office.

- **Repeat Visits to SSA Field Offices to Resolve Discrepancies:** When an employee receives a tentative non-confirmation notice from E-Verify, it is not clear to either the employer or employee what discrepancy caused the problem. The message, "SSN Does Not Match" could relate to any of four discrepancies between the information input into the system and the SSA Numident database. The employee does not learn the real reason behind the discrepancy until he or she reports to the SSA Field Office and a representative reviews the case and informs the employee of the evidence needed. If the problem is due to a date of birth discrepancy, the employee must return with a birth certificate. If a name discrepancy exists due to marriage, a marriage certificate is needed. If the problem is because the citizenship status is discrepant, then immigration documents may need to be submitted. If any of these documents are not in the employee's possession, the employee would need to order a replacement document from the source, which may take weeks to obtain. Meanwhile, the employee's employment status remains unresolved. At the very least, the employee must make multiple trips to the local SSA Field Office to resolve the issue.

- **Ineffectiveness of E-Verify in Identity Theft Cases:** Recent incidents in Nebraska, Minnesota, Texas, Iowa, and Utah communities showed that concerns about the effectiveness of E-Verify checks are well placed. Swift & Company meat packing plants were raided by ICE officers in December 2006, resulting in the detainment of 1,282 employees, many later found to be ineligible to work in the United States. At the time of the raid, Swift was exonerated of any wrongdoing as they were using the Basic Pilot as prescribed by DHS. Identity theft was cited as the cause of undocumented worker employment in this case. In this instance, it was found that Basic Pilot or E-Verify was useless in stolen identity cases. Then DHS Secretary Michael Chertoff said at the time of the raids that Basic Pilot was, "not a magic bullet for every kind of problem."

The Current State of SSA Operations

Over the last seven years, SSA has experienced a dramatic increase in Retirement, Survivor, Dependent, Disability, and Supplementary Security Income (SSI) claims. The additional claims receipts are driven by the initial wave of the nearly 80 million baby boomers who will file for Social Security benefits by 2030 -- an average of 10,000 per day! Concurrently, there has been a surge in claims filed due to worsening economic conditions and rising unemployment levels.

The need for resources in SSA Field Offices is also critical to process these additional claims and provide vital services to the American public. Field Offices are responsible for processing 2.4

million SSI redeterminations in FY 2011, a 100 percent increase over FY 2008. Nationally, visitors to Field Offices increased from 41.9 million in FY 2007 to 45.4 million in FY 2010. SSA is also experiencing unprecedented telephone call volumes. In FY 2010, SSA completed 67 million transactions over the 800 Number telephone network -- the most ever. NCSSMA estimates that Field Offices received an additional 32 million public telephone contacts.

Nationwide, over 3.2 million new disability claims were filed and sent to state Disability Determination Services in FY 2010. This surge of increased claims has created backlogs. At the end of FY 2010, the number of pending initial disability claims was at an all-time high of 824,192 cases -- a 46 percent increase from the end of FY 2008. SSA's largest backlogs are hearings appealing initial disability decisions, processed by the Office of Disability Adjudication and Review. Hearing receipts continue to rise, and as of March 2011, 728,013 hearings were pending which is nearly 23,000 more hearings than at the end of FY 2010.

Social Security Administration Funding

Appropriations to the Social Security Administration are an excellent investment and return on taxpayer dollars. We greatly appreciate the increased funding that SSA received for Fiscal Years 2008 through 2010. Had SSA not received this funding, the service we provide would be much worse and the disability backlog would be unconscionable. With the support of Congress and significant increases in employee productivity, tremendous progress has been made to enhance puhlic service, reduce the hearings hacklog, and to process additional workloads.

SSA Funding for FY 2011

NCSSMA supported the President's FY 2011 budget request of $12.379 billion for SSA's administrative expenses. As NCSSMA President, in March 2011, I testified at a hearing before the Senate Committee on Appropriations, Subcommittee on Labor, Health and Human Services, Education, and Related Agencies, and wrote directly to President Obama and Congressional leaders about SSA's need to receive adequate funding to maintain service levels vital to 60 million Americans. NCSSMA requested that during negotiations on final spending levels for FY 2011, SSA be provided with funding to cover inflationary increases because it was critically necessary to keep up with our growing claims receipts, maintain the progress achieved on reducing the disability hearings backlog, process program integrity workloads, and meet customer service expectations. Despite SSA's enormous challenges, with the federal deficit concerns, attaining this level of funding in FY 2011 was not possible.

Inadequate funding of SSA in FY 2011 and rescissions have already had major repercussions including a hiring freeze, elimination of overtime, and postponements of efficiency initiatives. Reducing resources at the same time SSA workloads are increasing is not prudent and is a prescription for making a very productive agency that efficiently uses the taxpayers' moneys into one with significant service delays and mounting backlogs. Service deterioration resulting from inadequate FY 2011 funding levels will have a collateral negative impact on FY 2012.

President's Proposed FY 2012 SSA Budget

NCSSMA strongly supports the President's FY 2012 budget request for SSA and requests that Congress provides full funding to sustain the momentum achieved to allow the agency to:

- ***Reduce the initial disability claims backlog to 632,000*** by processing over 3 million claims;
- Conduct disability hearings for 822,500 cases and ***reduce the waiting time for a hearing decision below a year for the first time in a decade;***
- Reduce pending hearings to 597,000 from the FY 2010 level of 705,367; and
- ***Complete additional program integrity workloads yielding nearly $9.3 billion in savings over 10 years, including Medicare and Medicaid savings*** by processing 592,000 medical Continuing Disability Reviews (CDRs) and 2.6 million SSI redeterminations.

Assessment of SSA Challenges

Field Office Service Delivery Challenges

SSA Field Offices vary in size, demographics, and location. However, all types of Field Offices are experiencing tremendous pressure because of our increased workloads and additional visitor traffic. The effect of funding Social Security in FY 2011 at FY 2010 levels or below exacerbates the situation and has already had a significant impact on local Field Offices around the country.

Frontline feedback from our busiest urban offices indicates that some have seen their visitor traffic explode with overflowing reception areas and increased waiting times. A manager of a busy SSA Field Office recently provided this comment:

- *We handle close to 2000 visitors a week. Recent losses due to retirement are affecting the service we provide, as we cannot interview the public fast enough. If we cannot hire to fill losses, the public will wait longer and be disadvantaged. In addition, the safety of the employees becomes at risk as the public becomes frustrated at the long waits. (California)*

Most of SSA has been under a hiring freeze because of the current funding situation. ***A hiring freeze for all of FY 2011 could result in a loss of over 2,500 SSA federal employees and up to 1,000 state employees in the Disability Determination Services.*** A SSA Field Office manager recently provided the following feedback about the effect of the current SSA hiring freeze:

- *A hiring freeze will be detrimental, especially to the processing of our disability workloads. In the past 6 months alone, our office staff has been reduced from 57 to 53 employees. We are anticipating a minimum of four more losses and will be down to 49 by the end of the year – a 14% decline in staff. SSA employees take pride in their work knowing that the American public depends on us. Not having the resources to process workloads in a timely manner undermines the positive morale of the staff as well as the public's trust in our agency. (Texas)*

As in-office visitors increase in already busy offices, there has also been an increase in reported security incidents. A November 2010, Office of the Inspector General (OIG) Report, "*Threats against SSA employees or Property,*" indicates, ***"SSA has experienced a dramatic increase in the number of reported threats against its employees or property.*** *The number of threats… increased by more than 50% in FY 2009 and by more than 60% FY2010."* This SSA manager expresses the connection between staff losses and security concerns:

- *A hiring freeze for all of FY 2011 would be devastating. We lost two employees and could not replace them. We are already seeing much more stress on staff members assuming the workloads of the employees we lost, and higher frustration levels from callers and visitors. The American public does not care that we are short on staff, they want to be seen quickly,*

have their calls answered and get their issues resolved. I am concerned that this type of frustration will lead to more threats and acts of violence toward staff members. (Kentucky)

SSA has a highly skilled but aging workforce with about two-thirds of its over 60,000 employees involved in delivering direct service to the public. ***SSA projects 50 percent of its employees, including 66 percent of supervisors, will be eligible to retire by FY 2018.*** Serious concerns exist about the agency's ability to sustain service levels with the tremendous loss of institutional knowledge from SSA's front-line service personnel.

Geographical staffing disparities will occur with attrition leaving some offices significantly understaffed. This is especially problematic for rural SSA Field Offices that serve customers who often live vast distances away, may have no Internet service, and lack access to public transportation. In many rural areas, SSA is the face of the federal government.

SSA workloads are expected to grow exponentially as the baby boomers retire. Reducing resources while work is significantly increasing will result in substantial service delays and inefficiencies as SSA tries to cope with the mounting backlogs. SSA is a very productive agency that efficiently uses the taxpayers' moneys and must be maintained as such.

Program Integrity Investments

SSA takes its stewardship responsibilities seriously and makes every effort possible to ensure the accuracy of benefit payments. SSA issues $800 billion in benefit payments annually to 60 million people and takes its stewardship responsibilities seriously. If SSA is able to fulfill its FY 2011 program integrity targets the estimated program savings over the next ten years is nearly $7 billion! The President's FY 2012 budget request includes $938 million dedicated to program integrity, which saves taxpayer dollars and is fiscally prudent in reducing the federal budget and deficit.

- CDRs determine whether disability benefits should be ceased because of medical improvement. ***Medical CDRs yield $10 in lifetime program savings for every $1 spent.***
- SSI redeterminations review nonmedical factors of eligibility, such as income and resources, to identify payment errors. ***SSI redeterminations yield a return on investment of $7 in program savings over 10 years for each $1 spent, including Medicaid savings accruals.***

SSA budgetary constraints have caused the shortfall between the number of CDRs due and the number conducted each year. A SSA Office of Inspector General (OIG) report in December 2010, titled "***Top Issues Facing Social Security Administration Management—Fiscal Year 2011***" provides OIG's perspectives on the most serious SSA management challenges. The report indicates there is a significant need to increase the number of CDRs conducted by SSA because there is a backlog of approximately 1.5 million cases. ***If SSA completes all of the 1.5 million medical CDRs, the lifetime program savings would be over $15 billion!***

NCSSMA strongly encourages Congress to provide SSA with the necessary funding to reduce the medical CDR backlog and to conduct additional SSI redeterminations. Investment in program integrity workloads ensures accurate payments, saves taxpayer dollars and is fiscally prudent with regard to the federal budget and the ongoing administration of SSA programs.

SSA Online eServices to Assist with Service Delivery Challenges

The expansion of services available to the American public via the Internet has helped to alleviate the number of visitors and telephone calls to SSA. However, the Internet is not keeping pace with the increasing demand for service, and high-volume transactions, such as Social Security Cards and benefit verifications are not available on the Internet, or are only being used to a limited degree. This represents over 40% of the 45.4 million visitors to SSA Field Offices.

NCSSMA believes that SSA must be properly funded in FY 2012 and beyond so that it may continue to invest in improved user-friendly online services to allow more online transactions. If individuals were able to successfully transact their request for services online, this would result in fewer contacts with Field Offices, improved efficiencies, and better public service.

Disability Workload Processes

Eliminating the disability hearings backlog continues to be SSA's top priority, and the agency has made a major resource investment to improve this situation. The agency's goal is to eliminate the backlog by 2013 and to improve processing time to 270 days. Commissioner Astrue has implemented several initiatives to achieve this goal, but this will depend on the available resources provided by SSA funding and the volume of new hearings received.

Annual appropriated funding levels for SSA have a critical impact on the hearings backlog. The increase in the disability hearings backlog is partially attributable to the significant underfunding of SSA. From FY 2004 to FY 2007, the final appropriated funding levels approved by Congress totaled $854 million less than the President's requests. However, from FY 2008 to FY 2010, the cumulative final appropriation level was $203 million more than the President's requests. In addition, SSA received nearly $1.0 billion in American Recovery and Reinvestment Act funding, which was utilized to help address the hearings backlog. The increased resources for SSA were even more essential as the agency's workloads grew at a rapid pace following the economic downturn. With the increased funding SSA has received in the last three fiscal years, the agency has opened or expanded 19 Hearing Offices, including a fifth National Hearing Center, hired 228 Administrative Law Judges and additional support staff.

SSA's efforts have resulted in significant progress in reducing both the number of pending hearings and the amount of time a claimant must wait for a hearing decision. At the end of FY 2010, the pending hearings were reduced to 705,367 cases nationwide, the lowest level in five years. In March 2011, the average processing time for a hearing was 359 days, the lowest level since December 2003. Even though this is positive news, the Hearing Offices are facing a significant wave of new hearings with approximately 400,000 additional hearings filed from FY 2009 through FY 2011 (projected) than were filed in FY 2008. This is attributable to the increased number of disability claims filed since the economic downturn beginning in 2008.

The Congressional Budget Office (CBO) released a report July 22, 2010: "***Social Security Disability Insurance: Participation Trends and Fiscal Implications***." According to this report, disability beneficiaries tripled from 2.7 million to 9.7 million people from 1970 to 2009. The CBO projects the number of ***disability beneficiaries will grow to 11.4 million by 2015***. In FY 2011, SSA anticipates receiving 629,000 more initial disability claims than in FY 2008.

It is essential to provide adequate funding to SSA to maintain the momentum achieved in reducing the number of disability cases pending and the processing time for these cases. Unfortunately, the number of claims and hearings pending is still not acceptable to Americans who need Social Security for support of their families. ***Progress was undermined by the FY 2011 budget impasse, resulting in the suspension of opening eight planned Hearing Offices in Alabama, California, Indiana, Michigan, Minnesota, Montana, New York, and Texas.*** This significantly weakens SSA's efforts to eliminate the hearings backlog by FY 2013.

Information Technology Investments

SSA is confronted with significant challenges in managing its Information Technology (IT) programs to keep up with rapidly expanding workloads. NCSSMA believes it is critical that SSA receive adequate funding to allow for much-needed IT investments. This is vitally necessary for SSA to replace the aging National Computer Center, to maintain systems continuity and availability, upgrade the agency's telephone system, and to improve IT service delivery. SSA's initiatives to implement automation and technological efficiencies are vitally important to the success of the agency.

Considerations Relevant to Increased Use of E-Verify and SSA Service Delivery

Regardless of your perspective on the expansion of E-Verify, one of the key questions before this Subcommittee is the potential impact of mandatory employment eligibility verification on SSA's service delivery. While NCSSMA is not taking a position on the underlying goal of any of the immigration bills before Congress, we believe it would not be prudent to require SSA to assume the burden of verifying the work status of every employee without full consideration of all issues, including the need for adequate funding.

A December 2010 Government Accountability Office (GAO) Report on Employment Verification (*Federal Agencies Have Taken Steps to Improve E-Verify, but Challenges Remain*, GAO-11-146) found that USCIS and SSA have taken actions to prepare for possible mandatory national implementation of E-Verify. However, USCIS's estimates do not include all costs associated with maintaining and operating E-Verify and SSA's estimates do not consider the risk associated with changes in SSA's E-Verify workload. This leaves the agencies at increased risk of not securing sufficient resources to effectively execute program plans in the future.

As noted above, ***SSA's service delivery system is under extreme pressure!*** While SSA is attempting to improve service by means of Internet service expansion, the need for trained and knowledgeable employees to assist the American public will continue to be required. The SSA Field Office is the face of the federal government, and the agency takes great pride in providing a high level of public service. Yet, even the dedication of SSA employees and management would be sorely tested if legislation is enacted requiring SSA to verify employment eligibility for all employees. ***Increases of even 5% to 16%, in SSA visitors because of mandated E-Verify workloads will further delay already strained services to vulnerable populations.*** SSA managers are already making difficult service delivery decisions because of insufficient staff, which either extend waiting times or cause Field Office phones to go unanswered. Any addition of a workload that is outside of SSA's core responsibilities will only exacerbate those problems.

In addition, the infrastructure required to increase the staff and systems capacity and capability to provide increased immigration verification services requires time. A minimum two-year training period is needed to properly prepare a Claims Representative to perform their duties. This training also requires removing some of our most productive employees from the front lines to provide mentoring. Efforts to improve SSA computer systems to deal with already increasing internal and external demands would also be delayed to implement these proposed programs.

NCSSMA understands the need for Congress to consider legislation that would expand or mandate an effective employment verification system to ensure a legal workforce and protect workers' identities, but the Social Security Administration must be safeguarded to achieve its primary mission. Establishing a national employment verification system, using SSA systems and employees, to confirm the employment status of every American worker would have a major impact on the financial resources of the Social Security Administration. This additional workload would hamper the agency's ability to provide services to its core beneficiaries -- the American workers who have paid their Social Security payroll taxes and earned the right to have their Social Security matters handled in a timely manner.

Conclusion

NCSSMA believes that the American public demands and deserves to receive good and timely service for the tax dollars they have paid to receive Social Security. ***We believe the adoption of the provisions being discussed in current immigration legislation could jeopardize SSA's ability to provide these vital services. Any expansion of SSA's responsibilities would require a commensurate increase in funding to support it.***

Social Security is one of the most successful government programs in the world and touches the lives of nearly every American family. We are a very productive agency and a key component of the nation's economic safety net for the aged and disabled, but sufficient resources are necessary. A strong Social Security program equates to a strong America and it must be maintained as such for future generations.

NCSSMA sincerely appreciates the Subcommittee's interest in the vital services Social Security provides, and your ongoing support to ensure SSA has the resources necessary to serve the American public. On behalf of the members of NCSSMA, I thank you for the opportunity to submit this written statement for the record and to state our viewpoints. NCSSMA members are not only dedicated SSA employees, but are also personally committed to the mission of the agency and to public service. We respectfully ask that you consider our comments, and would appreciate any assistance you can provide in ensuring the American public receives the necessary service they deserve from the Social Security Administration.

Contact Information

Joseph Dirago, President

National Council of Social Security Management Associations (NCSSMA)

418 C Street, NE, Washington, DC 20002

202-547-8530

joedirago@yahoo.com or rachele@greystone-group.com

Prepared Statement of National Immigration Law Center

How Errors in E-Verify Databases Impact U.S. Citizens and Lawfully Present Immigrants

FEBRUARY 2011

The E-Verify employment eligibility verification program is being sold as an easy fix that would curb unauthorized employment by immigrants and protect American jobs. But proposals to expand the program entirely ignore the effect the program will have on U.S. citizens and lawfully present noncitizens. At a time when the country is focused on increasing job growth, we should not enact policies that will increase unemployment and jeopardize the job security of American workers.

■ Database errors incorrectly identify U.S. citizens as not authorized for employment.

- A U.S. citizen born in Florida was hired for a well paying telecommunications position in October 2010. After she was hired, information from documents she submitted was processed through E-Verify, but the system issued a "tentative nonconfirmation" (TNC) notice to her. Her employer did not sit down with her to explain what a TNC means, nor to explain any of her rights. The worker visited her local Social Security Administration (SSA) office to try and resolve the situation, but, due to agency paperwork errors, she wasn't able to. She tried to communicate this to the employer, but ultimately the E-Verify system issued her a "final nonconfirmation" (FNC) notice, and the employer fired her. Since then, she has gone to great lengths to correct this error but has been unsuccessful. She was unemployed for over three months, including over the year-end holidays, but recently accepted a new, lower-paid position.[1]
- A U.S. citizen and former captain in the U.S. Navy with 34 years of service and a history of having maintained high security clearance was flagged by E-Verify as not eligible for employment. It took him and his wife, an attorney, two months to resolve the discrepancy.[2]
- A U.S. citizen was hired for a job at a poultry company in Georgia but received a TNC notice. The employee wanted to contest the TNC, but the company did not grant her time off to do so. As a result, the employee had no time to contest the TNC and was fired.[3]
- Juan Carlos Ochoa became a citizen in 2000. When he was offered a job at a car dealership in 2008, his employer used E-Verify to verify his employment eligibility. The employer received a TNC notice due to an error in SSA's database; SSA did not have any record of Ochoa's naturalization. Upon receiving the notice, Ochoa's employer fired him, a violation of E-Verify rules. Because he is out of work, he is late on his rent and his electricity has been shut off. Though Ochoa has a U.S. passport, the local SSA office told him he must bring in his naturalization certificate to prove his U.S. citizenship. Ochoa, however, lost his naturalization certificate years ago and will now have to pay close to $400 and wait up to ten months for a replacement certificate.[4]

NATIONAL IMMIGRATION LAW CENTER
www.nilc.org

LOS ANGELES (Headquarters)
3435 Wilshire Boulevard
Suite 2850
Los Angeles, CA 90010
213 639-3900
213 639-3911 fax

WASHINGTON, DC
1444 Eye Street, NW
Suite 1110
Washington, DC 20005
202 216-0261
202 216-0266 fax

- A naturalized U.S. citizen was hired by an Oregon telecommunications company but received a TNC because SSA records did not accurately reflect his citizenship status. He successfully contested the TNC at an SSA office, but the SSA representative did not correct his record. E-Verify then automatically issued an FNC, at which point the employer is required to dismiss the nonconfirmed worker. The employer did not immediately terminate the worker, however, but ran another query in E-Verify and got another TNC. The employee went back to SSA, and this time a representative updated his record but still failed to post the change to E-Verify. Once again, the employee received an FNC. Finally, he called the Office of Special Counsel for Immigration-Related Unfair Employment Practices (OSC), which called the SSA field office to explain proper E-Verify procedures so that the employee could keep his job.[5]
- A U.S. citizen residing in Florida was terminated by a national department store chain as a result of an erroneous E-Verify finding. The worker recently remarried and changed her name. After she received the TNC notice, she attempted to resolve the matter directly with the local SSA office and was informed by SSA that the matter was resolved. When she returned to work, she was informed that the U.S. Dept. of Homeland Security (DHS) had directed the company to terminate her employment and was told, "[Y]ou are suspected as a terrorist."[6]
- Francisco Romero, a U.S. citizen from Arizona, has been fired twice from jobs as a construction worker after E-Verify failed to confirm his employment eligibility. He has been a U.S. citizen since 1996, but in 2008 he spent months shuttling between SSA and human resource offices trying to obtain confirmation that he is eligible to work. Romero was only able to return to work after a community advocate took on his case and located the error that was keeping him from being able to secure employment.[7]
- A 16-year-old U.S. citizen received a TNC because his mother's maiden name was listed in his SSA records but he used his father's last name on his application. Instead of letting him fill in the application with the correct name, the employer told his mother that his name would have to be legally changed.[8]
- In December 2008, a U.S. citizen was hired by a sporting goods store in Mississippi. E-Verify issued a TNC, but the store manager unlawfully told the worker not to contest the TNC. The corporate office then fired her due to her failure to contest the TNC.[9]
- Ken Nagel, a restaurant owner in Phoenix, Arizona, expressed scorn regarding E-Verify after he hired one of his daughters, a native-born U.S. citizen, and, upon feeding her information into the system, received a nonconfirmation of her eligibility to be employed in the U.S.[10]
- A U.S. citizen applied for a job at an Oklahoma City nursing home and was offered the position. The job offer was rescinded, however, and the nursing home notified her that it had decided to hire someone else. Later, it sent the worker a notice that she had received a TNC and that, as a result, someone else had been hired.[11]
- A U.S. citizen used the services of an employment services company in San Francisco, California, to look for a job. After applying online, she was given an appointment and told that there were a number of employers that would be interested in her based on her extensive work history. The next day, the employment agency told her that she could not be offered a job because the agency could not verify her U.S. citizenship. The employment services company was enrolled in E-Verify and received a TNC about the worker because the system could not make a determination about her work authorization. The employment agency violated E-Verify rules by refusing to give her a copy of the notice, though she requested one in order to seek legal advice. The agency demanded that she sign the notice right away so it

could destroy copies of her documents. When she refused, the employment agency told her that it could not place her because she was ineligible to work in the U.S.[12]

- A U.S. citizen with specialized engineering skills went to a staffing agency in Colorado and obtained a high-paying job. He received an erroneous TNC, however, and, against program rules, the agency did not allow him to continue working until he had corrected the error with the SSA. After the error was corrected, the agency was unable to find a comparable job for the employee.[13]

■ Database errors incorrectly identify lawfully present immigrants and refugees as not authorized for employment.

- A lawful permanent resident was hired by a Colorado children's learning center, but she received an erroneous TNC. She called DHS to contest the TNC, but DHS made no record of her call. E-Verify then automatically issued a final nonconfirmation, and the employee was fired. She did not get her job back until she called OSC, which worked with DHS to correct the error.[14]
- An employment-authorized immigrant was hired by a laundry facility in Minneapolis, Minnesota. When the employee's name was entered into E-Verify, his employer received a TNC because of an error in SSA's database. The worker was able to resolve the issue with the local SSA field office; however, when the employer reentered his information into the system, the employer received an FNC. Although the employer wanted to keep the worker, under E-Verify rules, the employer had to fire the worker or risk being found liable for violating immigration laws.[15]
- A Burmese refugee was hired at a job in Texas, but he received a TNC when his employer entered an incorrect date of birth in E-Verify. The employer then wrongly suspended him until he could resolve the TNC. In addition, the employer failed to provide him with the referral letter advising him to contact DHS by phone, so the refugee visited a DHS office instead. Once he got there, the office could not help him because he did not have the referral letter with his case number. Finally, he contacted OSC for help, and OSC corrected the error and arranged to reinstate the employee with full back pay.[16]
- A refugee attempted to obtain a job with a Texas oil production company, but the company unlawfully processed the refugee's information through E-Verify before hiring him and received a TNC. The refugee went to his local SSA office that same day and corrected the problem, but the company refused to resume the hiring process until the refugee contacted OSC.[17]
- A lawfully present immigrant worker was offered a job by a construction, fabrication, and maintenance company in Texas. The employer was enrolled in E-Verify and received a TNC about the worker. Violating program rules, the employer did not give the worker the opportunity to contest the notice. Despite this, the worker went to the local SSA office and received the appropriate confirmation that he was, in fact, authorized to work. Even with clarification from SSA, the employer refused to take the worker back. The worker even enlisted the help of an attorney, who sent a letter to the employer outlining its obligations under E-Verify. The employer failed to respond.[18]

FOR MORE INFORMATION, CONTACT
Tyler Moran, employment policy director | moran@nilc.org | 208.333.1424

[1] Facts gathered by NILC staff during the course of providing technical assistance to this Floridian, beginning in mid-December, 2010.

[2] Account related at a Jan. 24, 2009, town hall meeting in Ashtabula, OH, sponsored by Building Unity in the Community and billed as "Why We Need Comprehensive Immigration Reform."

[3] Office of Special Counsel for Immigration-Related Unfair Employment Practices, Civil Rights Division, U.S. Department of Justice (OSC), *E-Verify Hotline Interventions*, Feb. 5, 2009.

[4] Veronica Sanchez, "U.S. Citizen Claims He's Victim of Employer Sanctions," *12 News*, Mar. 7, 2008, http://ing.ascentral.com/12news/news/articles/employersanctions030708.html.

[5] OSC, *E-Verify Hotline Interventions*, May 8, 2009.

[6] OSC, *E-Verify Hotline Interventions*, Sept. 2009, emphasis added.

[7] Kerry Howley, "Get in Line! Will Americans Have to Prove Their Right to Work Via an Error-plagued Database?" *Reason*, Oct.1, 2008, p. 30.

[8] OSC, *E-Verify Hotline Interventions*, Jan. 5, 2009.

[9] OSC, *E-Verify Hotline Interventions*, Jan. 9, 2008.

[10] Ronald J. Hansen, "Economy Serves Up Unhappy Meal: Worst Lull in 2 Decades is Hurting Valley Restaurateurs," *Arizona Republic*, Mar. 5, 2008, www.ascentral.com/business/articles/0305biz-more-restaurants0305.html.

[11] OSC, *E-Verify Hotline Interventions*, Dec. 17, 2007.

[12] Technical assistance request call received by NILC in Dec. 2007.

[13] OSC, *E-Verify Hotline Interventions*, Sept. 11, 2007.

[14] OSC, *E-Verify Hotline Interventions*, July 14, 2008.

[15] Case described to NILC staff by Bruce Nestor of De Leon & Nestor, Minneapolis, Minnesota, in April 2008.

[16] OSC, *E-Verify Hotline Interventions*, May 8, 2009.

[17] OSC, *E-Verify Hotline Interventions*, Dec. 4, 2008.

[18] Information provided to NILC by the Southern Poverty Law Center in Jan. 2008.

Prepared Statement of Secure ID Coalition

May 5, 2011

Honorable Sam Johnson
Chairman
Committee on Ways & Means, Subcommittee on Social Security
House of Representatives
Washington, DC 20515

Dear Chairman Johnson:

On behalf of the Secure ID Coalition (SIDC), I am pleased to submit the following comments as follow-up to the Subcommittee Hearing held on April 14, 2011 titled *Social Security Administration's Role in Verifying Employment Eligibility.*

During the course of the hearing, you asked witnesses about the use of biometric data for ID authentication in systems deployments. It was clear from the responses the witness provided that they had limited experience with the deployment and operations of biometric based programs and how expertise of such programs could be applied to the area of E-Verify. The SIDC submits these comments in an effort to dispel the misconceptions held by the panelists and provide factual information about how biometrics can be used for identity authentication as part of the E-Verify program.

First, it is important that we address the question of security of biometric and card-based systems. Statements made at the hearing with respect to biometric card deployments that questioned the security of chip-based identity card systems, also known as 'smart cards', suggesting they were easily hacked "in a matter of hours." This statement is not factual and our industry would like to see the data from the hacking incident referenced by Director Stana of the General Accounting Office.

The truth is that smart card technologies combined with biometrics are considered the 'gold standard' of identity management security, and are used both here and globally to provide the utmost in security, privacy and system performance. The U.S. government has already implemented biometric smart cards in numerous applications requiring the highest security, including the Department of Defense Common Access Card (CAC), the U.S. FIPS 201 Personal Identity Verification (PIV) Card, the U.S. Transportation Worker Identification Credential (TWIC), and the Electronic Passport. Other examples include the Singapore Immigration Automated Clearance System, the Canadian Airport Restricted Area Identification Card, Amsterdam's Schiphol Airport, and the University of Arizona Keyless Access System

919 18th Street, NW, Suite 925 | Washington, DC 20006 | p.202.464.4000 f.202.464.4001

www.secureidcoalition.org

Card. All of these applications reference above have been used for years with the highest degree of system integrity and success.

Cost concerns were also raised in the hearing regarding the implementation of biometrics into the E-Verify system, based on anecdotal evidence from the TWIC program. It should be noted that the deficiencies found in the TWIC program are the results of poor oversight and insufficient program planning and management, not failures in the technology. The SIDC would like to refer to the Committee the GAO's September 2006[1] and November 2009[2] reports on the TWIC program as a chronicle to this point.

If the U.S. government were to implement a worker ID and authentication credential that incorporates biometrics, the actual costs would most likely be modest. In the existing applications mentioned above, the lion's share of costs incurred has not to do with the technology itself, but with the vetting process required by the issuing organizations. As one would imagine, the Department of Defense's Common Access Card requires an extremely high level of assurance that the person being issued the card is who they claim – a level that requires numerous background and security checks. Because of the secure nature of what the card would grant access to – our most sensitive national defense systems – there are a number of additional security measures built into the card, such as anti-tamper technologies, microprinting, and holograms, to name a few. Understandably, these precautions increase the cost of the card, but through a risk-based analysis, the costs are well worth being borne.

Applying the same risk-based analysis to a proposed worker credential, the level of vetting and anti-tamper precautions would be significantly lower because the risk is lower. A worker identification card would certainly have to incorporate technologies to ensure against tampering or counterfeiting, but these would be inexpensive as the security would be built into the smart card's microcontroller and the card form itself can take advantage of existing off-the-shelf anti-counterfeiting measures currently used by those who issue drivers' licenses.

Further cost reductions can be achieved through the architecture of the system. Deploying a biometric card based process for E-Verify would allow the employer to verify the employee without having to be linked to back-end database – the source of a large amount of costs due to the security required. For the purposes of creating a secure, reliable and scalable E-Verify program, SIDC would propose a contact based card solution that would contain a secure chip; these smart cards have been proven secure and cannot be duplicated, skimmed or spoofed. Information stored on the secure chip could include name, account reference information and biometric template. Such an approach would allow the biometric to be compared with the template stored on the card without using an online database.

---

[1] U.S. Government Accountability Office. (September 2006). *Transportation Security: DHS Should Address Key Challenges before Implementing the Transportation Worker Identification Credential Program.* (Publication No. GAO-06-982).

[2] U.S. Government Accountability Office. (November 2009). *Transportation Worker Identification Credential: Progress Made in Enrolling Workers and Activating Credentials but Evaluation Plan Needed to Help Inform the Implementation of Card Readers.* (Publication No. GAO-10-43).

Additional concerns were raised about the collection and storage of worker information, both from a civil liberties and a privacy vantage point. By operating without a back-end database as mentioned above, civil liberty and privacy concerns can be addressed. In the SIDC's proposed system outlined below, only the federal government would collect and store a worker's biometric – as would be necessary for maintaining a reference data set and ensure no one has enrolled twice. This database would be secure and encrypted, and to further protect worker privacy in case of breach, personal information should be held in a database separate from the actual biometrics. Further, these databases should not be allowed to be accessed by the public, and only to those government officials authorized to by law. Citizen concern over the use of the biometric by the government for unintended uses (i.e., those not linked to worker authentication) can be ameliorated by implementing strong civil and criminal prohibitions in the authorizing legislation.

Personal privacy is further protected because the employer would not have access to the government database. Since the worker's biometric would be turned into a template (a computational representation of the biometric) which is then placed on the smart card's chip, the actual biometric is never at risk of being lost. Further the card, and as such the biometric, is carried and controlled by the cardholder not the employer. The employer's card reader would compare the biometric template on the card with the live biometric presented by the worker. If the biometric matches the template on the card that was presented at enrollment, then the worker is approved. At no time would the E-Verify software allow the employer to collect or store the employee's biometric. The only information that would be sent back to the E-Verify program would be whether or not the employee's biometrics matched.

Below is an overview of how such a system might be deployed for E-Verify

- The process would start with a letter from the Social Security Administration to the address of record for the individual (much like the annual Social Security statement previously sent to workers each year).
- The letter would include an individual code which would NOT be the Social Security number (SSN). This code would be a 'cryptographic hash', a mathematical cipher of data including name, address or region, and SSN.
- Each individual's code would be unique and associated with a Social Security record. The letter could only be validated with the correct Social Security number which would need to be provided by the individual. Therefore if the letter was intercepted, the interceptor would also need to also know the SSN associated with the letter and record.
- The letter would offer a reasonable time frame (maybe two weeks to a month) for the individual to come to an enrollment center convenient to them (i.e. their local post office or nearest federal building) to upgrade their Social Security card. The letter would also include the address of the enrollment center facility.
- The individual would be required to bring the letter (with the code) and other supporting documents to facilitate the Social Security card upgrade. At the enrollment center, the individual would provide the letter (something they have) and the associated SSN (something they know) and other documentation (maybe two forms of ID, with one having a photo). The Social Security record would be inaccessible to the enrollment center unless the letter with the correct code is presented.

- At the time of enrollment, the individual would have their biometric (such as a fingerprint, iris pattern, or hand geometry) scanned and enrolled in the system.
- The system would then check the newly scanned biometric against the enrollment database. If the biometric has not been seen before by the system, then the individual account is updated with the newly enrolled biometric. The biometric would then be associated with that individual record. If the biometric is already in the system, then the individual would be sent through a redress process.
- The individual would be issued a new chip-enabled electronic Social Security card that would incorporate the necessary security features and be tamper resistant. The chip would store the information usually found on the front of the legacy Social Security card (name and SSN) as well as a template of the individual's biometric. This ensures the individual's personal privacy as their actual biometric is never stored on the card, just a computational representation of the biometric.
- Upon hire the worker would present the new electronic Social Security card to the employer. The employer would insert the card into the reader and ask the new hire for their corresponding biometric. The reader would determine if the biometric presented by the new hire matches the one presented at the time of enrollment. The employer would immediately receive a green light for 'YES' or a red light for 'NO', as well as a receipt for both the employer and the employee.
- If the system responds YES, the employer is then free to engage the employee as they are now able to show they successfully completed the process. If the system responds NO, the prospective new hire would need to go through a secondary confirmation process.

This outline is merely a rudimentary sketch of how such a system could work for E-Verify, but should give the Subcommittee ideas of where privacy and security can be architected into the system, and how costs can be maintained at an acceptable level.

Thank you for the opportunity to submit comments to the Subcommittee regarding the April 14, 2011 hearing on E-Verify. The Secure ID Coalition would be pleased to serve as a resource to the Subcommittee as they evaluate how to further secure the E-Verify system. Please feel free to contact me directly at kemerick@secureidcoalition.org or 202-464-4000.

Respectfully Submitted,

Kelli A. Emerick
Executive Director

MATERIAL SUBMITTED FOR THE RECORD

Questions from Ana I. Antón, Ph.D.

June 3, 2011

Kim Hildred
Staff Director
Subcommittee on Social Security
Committee on Ways and Means
U.S. House of Representatives
B-317 Rayburn Building
Washington, D.C. 20515

Dear Ms. Hildred:

Thank you again for the opportunity to have Dr. Antón testify before the Social Security Subcommittee on April 14, 2011. In response to the questions in the Subcommittee's letter of May 17, 2011, we include the following responses. The questions are in **bold text**. Should you have any additional questions, please contact me at 202-659-9711.

1) In your testimony you advise against relying on single factor authentication, such as biometric, to identify a person because it makes the factor a target for theft and manipulation. The Department of Homeland Security is beginning a pilot project with the State of Mississippi that will allow an employer to match an employee's driver's license against the state's database. Is this a promising idea if used with another authenticator, and if not, why?

If "another authenticator" means another verified form of ID, then the Mississippi pilot seems to be a promising idea, because it would increase the effort required to commit identity fraud, and it would also increase the chances of such fraud being caught. However, there are still a number of potential problems with the proposal.

The driver's license is only as strong as the system a state uses to verify identity when granting drivers licenses. If a "good enough" false ID is used successfully to obtain a driver's license and that license is then used as the "another authenticator" then the system will be no more effective at verifying identity than it would be if only the single false ID was presented. A false driver's license coupled with knowledge of a matching Social Security number is often sufficient to obtain any number of otherwise legitimate secondary authentication documents. This has happened in other states, so it could be a problem in Mississippi, but we are unfamiliar with the specifics of their particular system.

Besides the possibility of issuing false licenses based on "breeder" documents that are suspect or obviously forged, the driver's license system in Mississippi (and in other states) may be subject to insider misuse. Employees who have access to the system might insert fraudulent records or grant licenses that are entered into the system hy mistake or because of hribes. Several years ago there was one instance where the staff of a driver's license bureau in Virginia was making falsified licenses and entering them into the state computer system, no questions asked, in return for payment of (rather paltry) bribe.

1828 L Street Northwest, Suite 800
Washington, D.C. 20036
http://usacm.acm.org/usacm
202-659-9711 tel
202-667-1066 fax

Another potential problem with this system is that not everyone who is a resident in Mississippi and who will need to have their employment verified will have a driver's license in Mississippi, or a valid 2nd authenticator. Individuals who are unable to drive for reasons of health, disability, economic necessity or simply choice may not have a drivers license or state-issued alternative. The pilot project should not exclude them.

On a related note, there is the possibility that someone may not be able to present his or her documents for verification because of exigent circumstances: consider the many people in southern states, including Mississippi, who have lost all their records recently in tornados and floods. This would not only make it difficult for them to verify their employment, but it might make it difficult or impossible for them be (re)issued a drivers license if the system is not designed with these possibilities in mind. In some states a person must show some ID to obtain a duplicate of an issued driver's license - a clear problem for people in disaster zones.

Of course, employers who falsify E-verify results in some way or fail to closely examine the presented documents will also continue to be a potential weakness.

Although a program connecting a driver's license match with a 2nd authenticator is a promising idea, and may well be more accurate than current practice, weaknesses in the implementation of the system will likely continue. There are clear opportunities for fraud in use of E-Verify even with such a program, but too strict a set of restrictions on proper authenticating documents may well deny employment access to some people with legitimate authority to work. How frequent those instances will be in practice is impossible for us to quantify in advance.

2) Please outline the security of state driver's license systems and the degree to which the risk of document fraud for REAL ID compliant licenses has been reduced.

There are many different systems for driver's licenses, and we have not studied the specifics of their security features and mechanisms. However, many of the REAL-ID features are intended to reduce document fraud by making the physical licenses more difficult to modify or forge, providing mechanisms that may be used to more strongly authenticate the identity of the holder, and to require uniform documentation for obtaining licenses.

To the best of our knowledge, REAL-ID compliant licenses are more difficult to forge or alter than their predecessors. However, this is simply a matter of cost and technology, and eventually forgeries will appear (if they have not already).

The machine-readable features intended to more strongly authenticate the identity of the holder are only as good as the entity conducting the authentication. If someone does not have a 2-D barcode reader, or does not carefully match picture against person, then the extra features in the license are of no extra value than most older licenses.

The process of applying for licenses continues to be a weakness because of significant amounts of identity theft, forgery and other identity-related crime. Individuals are likely still able to

present false documents with valid Social Security numbers and other data to obtain a license that is not a match to their real identity. In a REAL-ID compliant state the documents will be imaged and stored, but that will not prevent the license from being issued. Given the pressure for these licenses, the market for valid forged documents to use in applying for a license will undoubtedly develop. If license personnel are careless or criminally complicit that will only compound the problem.

As noted above, there may be people who will have difficulty obtaining a REAL-ID compliant license because of the loss of documents. A mechanism must be in place for these people to obtain IDs. However, that same system will be ripe for abuse by some individuals wishing to do so. We have seen stories of criminals who joined displaced people from Hurricane Katrina claiming to have lost all their possessions so as to establish new identity documents with no criminal record.

In 2007, the Data Privacy and Integrity Advisory Committee to the Secretary and the Chief Privacy Officer of the Department of Homeland Security issued 12 recommendations for enhanced privacy and security of REAL-ID cards (DPIAC Report 2007-01) to be included in the final rule for REAL-ID. None of them were adopted. USACM has provided comments and briefs over the last 6 years on REAL-ID on the privacy and security challenges of the program. These challenges go beyond issues related to fraud.

3) To obtain a passport or other authentication, one needs a certified birth certificate. However, is the system for obtaining copies of a valid birth certificate protected from fraud within most states?

This is not a topic we have studied. However, from the personal experience of committee members both obtaining a birth certificate and successfully forging one are not difficult tasks in several states, and we suspect that forging or altering a birth certificate from most states are also not difficult. Many birth certificates were, historically, forms that were simply filled in by hand or typewriter. Certified copies were either retyped, or later, photocopied, then stamped or embosed (or both). These kinds of documents are not difficult to forge or alter.

For example, a certified birth certificate one of our members used to obtain his passport had an official stamp and a hand-embossed seal, which was the standard up until recently in many states. The stamp could be recreated on a computer printer in a matter of a few hours, and then run off onto a manual stamp for use with an inkpad. The embossed seal is of the same size and shape as those used by notaries or for marking library books. A little work with carving tools, wax, and pewter would result in a new embosser good for making several hundred counterfeit certificates using aged paper.

Obtaining birth certificates is not difficult in many places. Clerks are often busy and may not be required to ask why a copy is requested. In others, presenting a fake driver's license or other ID in the name of certificate (or a relative) is sufficient justification; when ordering by mail a photocopy of those false IDs may be all that is necessary. As an example, documentation at <http://www.state.nj.us/health/vital/jerseycity.shtml> indicates a case where existing birth

certificates are no longer accepted (likely because of fraud), and a link is provided describing how to order a certified birth certificate by mail.

If you have any additional questions, please do not hesitate to contact me.

Regards,

Cameron Wilson
Director of Public Policy
Association for Computing Machinery

Questions from Austin T. Fragomen, Jr.

FRAGOMEN

ATTORNEYS AT LAW

Austin T. Fragomen, Jr.
Partner of the Firm

Direct: +1 212 891 7501
afragomen@fragomen.com

Fragomen, Del Rey, Bernsen & Loewy, LLP
7 Hanover Square
New York, NY 10004-2756
Main: +1 212 688 8555
Fax: +1 212 480 9930
www.fragomen.com

May 31, 2011

Via electronic mail
Steve.Degrow@mail.house.gov

Hon. Sam Johnson, Chairman
U.S. House of Representatives
Committee on Ways and Means
Subcommittee on Social Security
1102 Longworth House Office Building
Washington D.C. 20515

Re: Response to post hearing questions

Dear Chairman Johnson:

Thank you for the honor of testifying before the Subcommittee on April 14, 2011, and for this opportunity to answer follow-up questions in your May 17 letter. I respectfully submit the following response in the same order in which you posed the questions.

1. *What is a solution for having a good employment verification system, one that does not put individual jobs in jeopardy due to its shortcomings, like failing to detect identity fraud and preventing an unscrupulous employer from lying to the system and certifying an unauthorized worker?*

Protecting American jobs and ensuring integrity of our immigration system can be achieved through a reliable verification system that prevents identity fraud. Indeed, a reliable electronic verification system is a cornerstone to preventing unauthorized employment in the United States. Furthermore, we need a system that minimizes burdens on honest employers so that resources can go to research, job creation, and not just compliance with paperwork requirements.

Employers need a verification system that tells them two things: 1) whether the person is who he or she says she is; and, 2) whether the person is authorized to work. U.S. workers need the government to help them quickly remedy any mistakes in the databases so they can get back to work. There also must be a true safe harbor for employers, not just from prosecution, but also

from the adverse consequences of unknowingly having unauthorized personnel. Instability in the workforce results in loss of productivity and revenue which ultimately hurts the American workers.

The time is ripe for the Department of Homeland Security (DHS) to pursue aggressively pilot programs to eliminate identity fraud and protect employers. Last Thursday, the U.S. Supreme Court ruled in Chamber of Commerce v. Whiting that Arizona's eligibility verification and E-Verify requirements were not preempted by federal law. This decision realistically will lead to one of two results – either Congress enacts stronger federal preemption language as part of E-Verify expansion legislation, or states will rely on the Supreme Court's holding to pass E-Verify and verification legislation even more aggressively than they do today. In either scenario, there will be greater E-Verify mandates, and DHS must address the identity fraud loophole in order for E-Verify to have any credibility among its participants. We believe the federal government, and not the states, is best positioned to test ideas and determine what is the most effective and efficient system to meet our national priorities on immigration.

We believe that the technology exists to greatly reduce the identity theft in the employment verification system. As explained in my testimony and as the chairman of this subcommittee envisioned in his New Employee Verification Act (NEVA), biometric technology is one good way to achieve this objective and is worth pursuing. Regardless of what technology DHS chooses, the bottom line is that the system and technology must prevent identity fraud and provide employers with certainty.

Finally, the Supreme Court's ruling last week underscores the need for the strongest possible federal preemption statute. Many job creators in the United States do business in several states. It can be very burdensome and confusing to them when states impose additional immigration compliance requirements, especially when these state laws are inconsistent with one-another and with federal law.

2. *You pointed out that there are 60 million new hires annually, and that given job turnovers, most individuals would be verified within three to four years. What are the concerns employers have regarding E-Verifying their entire workforce?*

American employers understand they have an important role to play in securing our nation's borders and worksites. Yet, the government must acknowledge that there are substantial costs to employers when they assume this role. Businesses constantly have to balance the costs and benefits of undertaking any task. Reverification of the existing workforce is one area where the costs are likely to outweigh greatly the benefits, both to the nation and to most employers.

E-Verify as it exists currently can be an effective tool for matching a name with a Social Security number (SSN). It is not yet effective in uncovering identity fraud. Therefore, requiring employers to reverify their current employees through E-Verify would not guarantee the legality of the workforce. Also, as employers follow up on SSN no-match letters, a large number of currently unauthorized workers using false numbers will be discovered, and anyone who cannot

be detected through the SSN no-match letter process will not be detected through E-Verify anyway. Furthermore, there are many sectors that attract very few, if any, unauthorized workers so mandatory reverification yields no benefit to them at all. As many federal contractors have discovered in complying with the E-Verify amendments to the Federal Acquisition Regulation (FAR), the cost of using E-Verify on an existing workforce can be considerable, sometimes reaching into millions of dollars for the largest employers. Alternatively, if Congress does mandate reverification of the current workforce, the scope should be limited. At the very least, those hired prior to the enactment of the Immigration Reform and Control Act (IRCA) in November of 1986 should be exempt.

Moreover, as I testified on April 14, there is always a concern about "scalability," meaning whether the system can accommodate a tremendous surge in usage. Currently, only about 3% of the U.S. employers are enrolled in E-Verify and, except for certain federal contractors, they may use it only for new hires. The surge in usage will be astronomical if all employers are required to use it for the entire workforce. DHS must not only assure the public that the system will be ready for the surge, but explain to Congress and the employer community exactly *how* it will accommodate the surge. Otherwise, the administrative cost associated with trying to deal with system errors and inefficiencies also will have an adverse effect on productivity and job creation.

In sum, while industries that frequently struggle with SSN mismatch issues among its workers may welcome the opportunity to use E-Verify on existing workers, many other sectors derive little or no benefit at all. It would not be good public policy to compel all employers to spend resources on reverification that otherwise can be used to grow their businesses and hire more workers. Reverifying the entire workforce, therefore, should be an option, but not a mandate, for employers.

3. *The Department of Homeland Security (DHS) has just implemented a third party authentication system called Self Check. What is your assessment of the system?*

Self Check is a great concept and was included in NEVA. It gives potential job seekers the opportunity to discover errors before they have to undergo E-Verify when reporting to a new job. This reduces or eliminates the burden on compliant employers and legal employees of having to resolve erroneous E-Verify non-confirmations. Of course, Self Check is only useful to compliant employers and legal workers. It is not intended as an enforcement tool against unscrupulous employers or unauthorized workers perpetrating identity fraud. Employers also are not permitted to require the use of Self Check.

Self Check is only available in Colorado, Idaho, Mississippi, Arizona, Virginia and the District of Columbia presently. Only employees logging on from an internet protocol (IP) address in one of these jurisdictions can use it. It is far too early to say whether the program will have significant impact on the overall verification process. More observation and analyses also are needed before assessing whether and how Self Check can be improved. DHS also should evaluate further the Self Check program and determine where it can be enhanced and developed

into a tool that is even more helpful to U.S. workers and employers, not just to residents of the above six jurisdictions.

4. *DHS has also just entered in a pilot program with the State of Mississippi where an employer could match an employee's driver's license photo against the state's database. As the driver's license is the one photo ID most people can present, does this idea hold any promise for better authentication? While the project has not yet begun, after a[n] acceptable time period for testing, how would you define a successful pilot?*

The photo screening tool should be among the pilots that DHS aggressively pursues. It is an important first step but is not enough. Until Mississippi's agreement to participate, photo screening tool's coverage had been limited to DHS-issued employment authorization documents (EAD), "green cards," and U.S. passports.

Undeniably, it makes perpetrating identity fraud more difficult. However, the photo screening tool currently has two major limitations. First, its scope is not wide enough. To avoid triggering the photo screening function on E-Verify, an unauthorized worker can present a fraudulently obtained document other than a passport, green card or EAD. If a fake driver's license is needed, the unauthorized worker would obtain one purporting to be from any jurisdiction other than Mississippi.

Second, the photo screening tool is only effective in detecting illegal photograph substitutions. The screening" is limited to comparing the photograph on the computer screen with the photograph on the document presented. An unauthorized worker still may defraud a state to issue a document under a stolen identity and pass the photographic screening. Furthermore, employers still remain vulnerable as they have to exercise discretion and decide whether the images on the photographs match the persons physically before them.

This is not to say that the photo screening tool can never be effective. After the Chamber of Commerce v. Whiting decision, one would expect the states to become even more engaged in preventing identity fraud and ensuring data accuracy for verification purposes. Thus, whether E-Verify's photo screening tool can become a credible option will depend on DHS's ability to expand the program to all states and territories, and the state government's willingness to meet certain standards (e.g. Real ID compliance) to ensure the integrity of the documents they issue. In addition to just the photographs, E-Verify should authenticate driver's license numbers as well. Though this will not be as reliable as using biometric features, it is an idea worth pursuing if we lack the political will to explore a biometric pilot. The program also must extend to all identity documents acceptable for I-9 purposes so one cannot circumvent the screening. In addition, its function cannot stop at merely matching two photographs, but must ascertain whether the photograph is in fact the likeness of the person being verified. To serve the ultimate purpose of ensuring integrity at the worksite and protecting American jobs, the photo screening tool (or any other DHS pilot) must provide employers a safe harbor from government penalties and adverse economic consequences.

Once again, I thank you and your subcommittee staff for your kind invitation and for all your diligent efforts to improve the employment eligibility verification system.

Respectfully submitted,

Austin T. Fragomen, Jr.

Questions from Marianna LaCanfora

SOCIAL SECURITY
Office of Retirement and Disability Policy

June 14, 2011

The Honorable Sam Johnson
Chairman, Subcommittee on Social Security
Committee on Ways and Means
House of Representatives
Washington, D.C. 20515

Dear Mr. Johnson:

Thank you for your letter of May 17, 2011 requesting additional information in order to complete the record for the hearing on the Social Security Administration's role in verifying employment eligibility. Enclosed you will find the answers to your questions.

I hope this information is helpful. If I may be of further assistance, please do not hesitate to contact me or your staff may contact Scott Frey, Deputy Commissioner for Legislation and Congressional Affairs, at (202) 358-6030, who is available to meet with your staff if requested.

Sincerely,

Marianna LaCanfora

Enclosure

Questions For the Record
April 14, 2011 Hearing on E-Verify

Question #1

a) Do you have updated estimates for the cost of a mandatory E-Verify system for new hires and for using E-Verify for all current workers?

To verify all new workers, we estimate that it would cost about $80 million and require more than 500 workyears over 5 years. To verify all current workers, it would cost approximately $160 million and require 1,175 workyears over 5 years.

We based our estimates on a straight expansion of the *current* E-Verify program. Modifications to the current program requirements could increase our costs significantly. Our estimates include costs to process the fallout work that will come to our field offices, Social Security card centers, and toll-free number, and is based on the assumption that we will phase in these additional verifications over a 5-year period.

b) Do you have an estimate of the visits to the field offices a mandatory system would generate?

A fully implemented mandatory system for new hires would require us to verify more than 100 million individuals over 5 years. Based on the current fall-out rate, this work would generate more than 800,000 additional contacts, resulting in approximately 675,000 field office visits and 130,000 calls. A fully implemented mandatory system for all workers would require us to verify more than 240 million individuals over 5 years. Based on the current fall-out rate, this work would generate almost 2 million additional contacts, resulting in approximately 1.6 million field office visits and 300,000 calls. Field offices in border States like California, Arizona, and Texas handle a disproportionate volume of E-Verify fall-out. Under a mandatory system, this pattern would likely continue.

If Congress makes the program mandatory, it is critical that we receive adequate funding and lead-time to increase not only our systems capacity but our field office capacity as well. Equally important, any mandatory program must be phased-in over a multi-year period to ensure that we effectively support the E-Verify program without compromising our ability to handle our increasing workloads. Without an appropriate phase-in period, field offices across the country could be overwhelmed, and border offices would be disproportionately affected.

Question #2

a) If a mandatory system was put into place and you had a large influx of field office visits, would the SSA have to hire more people?

Yes. The increase in our work would require us to hire additional employees. Over a 5-year period, we would need 125 new employees for the new hire proposal and approximately 250 new employees for the proposal to verify all workers.

b) Would you hire temporary staff for that purpose to hold down SSA's long-term costs?

No, doing so would not be practical, because the complexity of enumeration requires our employees to have in-depth knowledge of Social Security number (SSN)-related policies, procedures, and statutory requirements.

We cannot absorb this work with our current staffing. Our budget has forced us into a hiring freeze and we are continuing to lose staff. We lose about 3,000 employees each year.

Question #3

Various immigration proposals have proposed that SSA send letters to individuals who have multiple wages reported on the annual W-2 statement to alert them for possible identity theft.

a) Tell us how many individuals have multiple wages each year and your estimate of how many of these might be fraudulent.

Each year employers send us 240 million wage reports for approximately 150 million workers. Based on the most recently available data, in tax year (TY) 2009, we estimate that about 38 million workers held more than one job during the year. Almost 1 million worked in five or more jobs. We estimate that more than 37,000 individuals worked in 10 or more jobs that year.

There are many legitimate reasons for a worker to have multiple W-2s for a given year. For example, he or she may work in more than one job at a time during the year, have a job change, or work in an employment field that routinely involves multiple employers. We do not automatically suspect fraud simply because a worker has multiple employers nor can we estimate how frequently fraud may be involved. We process W-2s for the Internal Revenue Service, which may have information on this topic.

b) What would be the cost of mailing such letters and what would be the increased time and financial burden on the field offices?

It is important to note that earnings information may be covered by section 6103(1)(5) of the Internal Revenue Code, which allows us to disclose return information only for purposes of administrating the Social Security Act. Disclosure of W2 earnings information by us for any

other purpose is currently a violation of federal law. We continue to believe that the Internal Revenue Service is better equipped to detect these instances of identity fraud and to contact individuals with multiple W2s in a calendar year.

The proposals' specific costs and the effect on field offices depend upon the details of a specific proposal. If we were required, and the law allowed us, to send notices to the 38 million workers for whom we received more than one wage report in TY 2009, we estimate that the 5-year cost would be more than $340 million and approximately 2,400 workyears. It is important to note that these estimates assume the proposal would not require individuals who receive a letter to contact us. Our costs and related field office workloads would increase substantially if the proposal required all individuals who receive a letter to contact us.

c) Would those costs be reimbursed by the Department of Homeland Security (DHS)?

We are prohibited from using trust fund money to support immigration enforcement activities. Therefore, we require reimbursement for any E-Verify work we do for DHS, and DHS regularly reimburses us for that work.

d) Would such a process result in better protection of the SSN and help individuals protect their identities?

The E-Verify program is designed to provide an immediate front-end confirmation of a new hire's employment eligibility, deterring SSN misuse. By contrast, because of when we get W-2 information, we cannot notify an individual that multiple employers reported wages under his or her name and SSN until 12 to 18 months after the potential SSN misuse occurred. This delay occurs because employers report wages to us during the year following the year in which the wages were earned.

e) Is there some way DHS could help SSA in identifying those SSNs that are being used for fraudulent work authorization purposes?

DHS's United States Citizenship and Immigration Service has staff devoted to monitoring employer use of the E-Verify program. Should DHS identify patterns of possible SSN misuse, it could refer these cases to our Office of Inspector General for further investigation.

Questions from Richard M. Stana

GAO
Accountability • Integrity • Reliability
United States Government Accountability Office
Washington, DC 20548

June 14, 2011

The Honorable Sam Johnson
Chairman
Subcommittee on Social Security
Committee on Ways and Means
House of Representatives

Subject: *E-Verify: Responses to Posthearing Questions for the Record*

On April 14, 2011, I testified before your subcommittee on E-Verify, an Internet-based system that is operated by the Verification Division of the Department of Homeland Security's U.S. Citizenship and Immigration Services (USCIS) and the Social Security Administration (SSA)[1]. This letter responds to four questions for the record that you requested that we address on May 17, 2011. The responses are based on work associated with our December 2010 report on E-Verify[2] and on updated information regarding questions 3 and 4 that we obtained from USCIS on May 27, 2011. Your questions and my responses follow.

1. Under E-Verify, law-abiding Americans' personal information is being checked through the Department of Homeland Security (DHS). What is DHS doing with the personal data? Can this information be mined for other purposes? Can we assure Americans that their personal information may not be used for any other purpose?

According to privacy impact assessments published in connection with the E-Verify program, DHS has committed to using E-Verify only to respond to employment verification inquiries and for other specific and limited purposes, such as to ensure that fraud is not being committed in the system. While it is true that the data collected in the systems that support the E-Verify program could potentially be "mined" for other purposes, DHS has committed not to do so within the E-Verify program. The Implementing the Recommendations of the 9/11 Commission Act of 2007 requires DHS to report annually on activities currently deployed or under development that meet the act's definition of data mining. DHS has not reported any E-Verify actions as data-mining activities under its reporting requirements.

---

[1] GAO, *Employment Verification: Agencies Have Improved E-Verify, but Significant Challenges Remain*, GAO-11-552T (Washington, D.C.: April 14, 2011).
[2] GAO, *Employment Verification: Federal Agencies Have Taken Steps to Improve E-Verify, but Significant Challenges Remain*, GAO-11-146 (Washington, D.C.: Dec. 17, 2010).

DHS has taken actions to minimize risks to the privacy of personal information of employees who are processed through E-Verify. For example, the privacy impact assessment and other published privacy notices set limits on the collection and use of personal information for the E-Verify program. Further, DHS has designed E-Verify to collect and share little personal information about individual employees. Specifically, E-Verify does not require employers to collect any more information on employees than has already been recorded on the Form I-9,[3] and controls have been established within E-Verify's automated system that limit the extent to which management program analysts at DHS can access and use personal information when searching the available databases to confirm citizenship or work authorization status. For example, management program analysts' access is limited to information applicable to the cases that are assigned to them. Controls such as these are intended to provide assurance that the personal information collected by E-Verify will not be used for other purposes, such as data mining.

2. What is the solution for having a good employment verification system, one that does not put individual jobs in jeopardy due to its shortcomings, like failing to detect identity fraud and preventing an unscrupulous employer from lying to the system and certifying an unauthorized worker?

A good employment verification system relies on a combination of factors, including (1) information technology systems that are reliable and have sufficient capacity to notify employers of employment verification results without interruptions in service, and that have quality control procedures to screen for data entry errors; (2) government databases and employee documents that contain accurate and consistent personal information on employees; (3) the ability of employees to access personal information and correct inaccuracies or inconsistent personal information in DHS databases; (4) employers who act in good faith to implement the rules of E-Verify; (5) mechanisms that can determine if employees are presenting genuine identity and employment eligibility documents that are borrowed or stolen; and (6) a credible worksite enforcement program.

With respect to ensuring that individual jobs are not jeopardized because of E-Verify data inaccuracies and willful employer noncompliance, USCIS has taken steps to improve the accuracy of E-Verify, and USCIS's ability to monitor employer compliance should expand further with the planned fiscal year 2012 implementation of a data analysis system for analyzing complex patterns in the E-Verify data that could be indicative of employer misuse. This is a step in the right direction, although USCIS still has a ways to go to staff its E-Verify Monitoring and Compliance Branch up to its authorized level[4] and is generally not in the position to determine whether employers carry out activities required by E-Verify because interactions between

[3] The Immigration Reform and Control Act of 1986 established an employment verification process—the Form I-9 process—that required employers to review documents presented by new employees to establish their identity and employment eligibility.

[4] We noted in our December 2010 report that USCIS's Verification Division Deputy Division Chief told us that USCIS had hired 22 of 44 monitoring and compliance analyst staff budgeted in fiscal year 2010 and planned to hire the additional 22 staff in fiscal year 2011.

employers and employees generally occur privately in workplaces where USCIS has limited capability to monitor employer compliance with E-Verify requirements.

With respect to detecting identity fraud and whether unscrupulous employers hire unauthorized workers, a challenge is that it is difficult to positively link identity documents with the persons who present them. In this regard, thought has been given to the use of biometrics that would provide for such a linkage. While this could resolve some of the weaknesses of the E-Verify system, the use of biometrics could be costly and generate privacy concerns. Further, to investigate, sanction, and prosecute unscrupulous employers, USCIS must rely on U.S. Immigration and Customs Enforcement (ICE). Although USCIS and ICE signed a memorandum of agreement in December 2008 that outlined the processes that the agencies are to use for sharing E-Verify program information, ICE has reported that it has limited resources for investigating and sanctioning employers that knowingly hire unauthorized workers or those that knowingly violate E-Verify program rules, and overall, ICE has expended relatively few resources on carrying out such activities.[5] Policy decisions about how to effect a credible worksite enforcement program using E-Verify have yet to be made. The success of the E-Verify program will ultimately be affected by these decisions.

3. Do you have updated estimates for the cost of a mandatory E-Verify system for new hires and for using E-Verify for all current workers? Do you have an estimate of the visits to the field offices a mandatory system would generate?

With respect to the cost of a mandatory E-Verify system, USCIS said it is currently working on estimating costs. According to USCIS, it has a formula for calculating the funding and resources needed if legislation mandating E-Verify is passed. If E-Verify were mandated for all new hires nationwide, USCIS estimates that about 60 million E-Verify queries would be generated annually. If E-Verify were mandated for all current workers, USCIS estimates that approximately 120 million additional queries would be generated (in addition to the 60 million for new hires) based on 2008 U.S. Census Bureau data. According to USCIS, the formula would need to be adjusted accordingly depending on, among other things, changes in the size of the workforce and the specifics of the legislation.

With respect to field visits resulting from a mandatory E-Verify system, USCIS said that under a phased-in approach, it estimates that there will be an annual query volume of 60 million for new hires. USCIS said this would generate approximately 490,000 visits to SSA field offices, though this estimate would be subject to change.

4. DHS has just implemented a third party authentication system called Self Check. Do you know if DHS is provided with any personal information about the individual from the third party authenticator in the Self Check system?

[5] In fiscal year 2009, ICE spent 5.2 percent of its 10.4 million agent reported workload hours on worksite enforcement, issued 52 fines as a result of Form I-9 audits, and made 444 criminal and 1,654 administrative worksite enforcement arrests.

E-Verify Self Check utilizes a third-party authenticator (independent identity assurance service) to generate an identity assurance quiz and determine whether individuals attempting to check their employment eligibility are who they claim to be. According to USCIS, DHS does not keep any information about the questions asked, the answer options given, and the answers an individual chose. The only information DHS retains from the identity assurance portion of the Self Check process is a transaction identification number and the result of the transaction. USCIS said this information is retained to determine success and to further improve the Self Check process. DHS's information retention policy for Self Check is detailed in a published System of Records Notice and Privacy Impact Assessment.

If you have any questions about this letter or need additional information, please contact me at (202) 512-8816 or stanar@gao.gov.

Richard M. Stana

Richard M. Stana
Director
Homeland Security and Justice Issues

○