EMPLOYMENT ELIGIBILITY VERIFICATION SYSTEMS

HEARING

BEFORE THE

SUBCOMMITTEE ON SOCIAL SECURITY

OF THE

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

ONE HUNDRED TENTH CONGRESS

FIRST SESSION

JUNE 7, 2007

Serial No. 110–45

Printed for the use of the Committee on Ways and Means

U.S. GOVERNMENT PRINTING OFFICE

47–008 WASHINGTON : 2009

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

CHARLES B. RANGEL, New York, *Chairman*

FORTNEY PETE STARK, California
SANDER M. LEVIN, Michigan
JIM MCDERMOTT, Washington
JOHN LEWIS, Georgia
RICHARD E. NEAL, Massachusetts
MICHAEL R. MCNULTY, New York
JOHN S. TANNER, Tennessee
XAVIER BECERRA, California
LLOYD DOGGETT, Texas
EARL POMEROY, North Dakota
STEPHANIE TUBBS JONES, Ohio
MIKE THOMPSON, California
JOHN B. LARSON, Connecticut
RAHM EMANUEL, Illinois
EARL BLUMENAUER, Oregon
RON KIND, Wisconsin
BILL PASCRELL, JR., New Jersey
SHELLEY BERKLEY, Nevada
JOSEPH CROWLEY, New York
CHRIS VAN HOLLEN, Maryland
KENDRICK MEEK, Florida
ALLYSON Y. SCHWARTZ, Pennsylvania
ARTUR DAVIS, Alabama

JIM MCCRERY, Louisiana
WALLY HERGER, California
DAVE CAMP, Michigan
JIM RAMSTAD, Minnesota
SAM JOHNSON, Texas
PHIL ENGLISH, Pennsylvania
JERRY WELLER, Illinois
KENNY HULSHOF, Missouri
RON LEWIS, Kentucky
KEVIN BRADY, Texas
THOMAS M. REYNOLDS, New York
PAUL RYAN, Wisconsin
ERIC CANTOR, Virginia
JOHN LINDER, Georgia
DEVIN NUNES, California
PAT TIBERI, Ohio
JON PORTER, Nevada

JANICE MAYS, *Chief Counsel and Staff Director*
BRETT LOPER, *Minority Staff Director*

SUBCOMMITTEE ON SOCIAL SECURITY

MICHAEL R. MCNULTY, New York, *Chairman*

SANDER M. LEVIN, Michigan
EARL POMEROY, North Dakota
ALLYSON Y. SCHWARTZ, Pennsylvania
ARTUR DAVIS, Alabama
XAVIER BECERRA, California
LLOYD DOGGETT, Texas
STEPHANIE TUBBS JONES, Ohio

SAM JOHNSON, Texas
RON LEWIS, Kentucky
KEVIN BRADY, Texas
PAUL RYAN, Wisconsin
DEVIN NUNES, California

Pursuant to clause 2(e)(4) of Rule XI of the Rules of the House, public hearing records of the Committee on Ways and Means are also published in electronic form. **The printed hearing record remains the official version.** Because electronic submissions are used to prepare both printed and electronic versions of the hearing record, the process of converting between various electronic formats may introduce unintentional errors or omissions. Such occurrences are inherent in the current publication process and should diminish as the process is further refined.

CONTENTS

EMPLOYMENT ELIGIBILITY VERIFICATION SYSTEMS

THURSDAY, JUNE 7, 2007

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

The Subcommittee met, pursuant to notice, at 10:01 a.m., in Room B–318, Rayburn House Office Building, Hon. Michael R. McNulty (Chairman of the Subcommittee) presiding.

[The Advisory of the hearing follows:]

ADVISORY

FROM THE COMMITTEE ON WAYS AND MEANS

SUBCOMMITTEE ON SOCIAL SECURITY

FOR IMMEDIATE RELEASE
June 07, 2007
SS–3

CONTACT: (202) 225–1721

McNulty Announces A Hearing on Employment Eligibility Verification Systems

Congressman Michael R. McNulty (D–NY), Chairman, Subcommittee on Social Security of the Committee on Ways and Means, today announced that the Subcommittee will hold a hearing on current and proposed employment eligibility verification systems and the role of the Social Security Administration in authenticating employment eligibility. **The hearing will take place on Thursday, June 7, in room B–318 Rayburn House Office Building, beginning at 10 a.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:

Since 1986, United States immigration law has prohibited employers from knowingly hiring or continuing to employ aliens who are not authorized to work under the Immigration and Nationality Act (INA). All employers are required to request that employees, once hired, produce documents that show they are authorized to work in the United States. Verification of the validity of the documents is not mandatory. The Social Security card is one of a number of items that an employee may use in combination with other identity documents to demonstrate work authorization.

While the Department of Homeland Security (DHS) is responsible for enforcing the INA prohibitions on unauthorized employment, the Social Security Administration (SSA) plays a key role in the verification process. Since 1996, employers have had the option of verifying names and Social Security numbers (SSNs) of new hires against SSA's database through an employment eligibility verification system (EEVS, formerly known as the Basic Pilot) operated jointly by SSA and DHS. Until 2003, the Basic Pilot was restricted to operate in only five states, but has since been expanded nationally. Currently, about 16,700 employers at 73,000 hiring sites (less than 1 percent of all establishments) participate in the EEVS. Most participating employers do so voluntarily, but some are required to use the EEVS by law or because of prior immigration violations.

In 2006, the system received over 1.6 million requests for verification. Of these, 1.4 million cases were resolved by SSA. The bulk of the remaining cases were referred to DHS for further verification of work-eligibility.

The Government Accountability Office (GAO) and the SSA Inspector General have found that the current system is hampered by inaccuracies in the records maintained by DHS and SSA. GAO and other auditors also have found that the current EEVS is vulnerable to identification document fraud, prohibited and privacy-violating uses by employers, as well as discriminatory abuse.

Recent immigration reform proposals have included provisions to expand some version of an employment eligibility verification system. Some of the proposals would build on the current EEVS and require employers to verify all new hires,

making the system mandatory for all 7.4 million private and 90,000 public sector employers in the United States. These employers account for 60 million hires per year, according to SSA. Other proposals include a requirement that the Social Security card be enhanced with tamper-proof, counterfeit-resistant or biometric features.

In announcing the hearing, Chairman McNulty stated **"If employment eligibility verification is to be a key enforcement tool for immigration policy, we must ensure the system is effective, efficient and feasible. We need a better understanding of the possible consequences and impact on the Social Security Administration if they are to undertake this expanded responsibility without compromising their core mission of administering Social Security."**

FOCUS OF THE HEARING*:*

The hearing will examine the current EEVS system and proposed expansions, including the potential costs and increased workloads that would be faced by SSA. The hearing also will examine the potential impact on workers and employers; how it would interact with REAL ID and other identification methods; and the privacy implications, especially in light of proposed data-sharing arrangements between agencies.

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 "110th Congress" from the menu entitled, "Committee Hearings" (*http:waysandmeans.house.gov/Hearings.asp?congress=18*). 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, completing all informational forms and clicking "submit" on the final page, an email will be sent to the address which you supply confirming your interest in providing a submission for the record. You MUST REPLY to the email and ATTACH your submission as a Word or WordPerfect document, in compliance with the formatting requirements listed below, by close of business **Thursday, June 21, 2007**. 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.

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.

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

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.

Chairman MCNULTY. I want to welcome all of our witnesses and all of our guests here today. Our hearing today will focus on current and proposed systems for verifying the employment eligibility of American workers under immigration law.

We are particularly interested in the impact of these proposals on the Social Security Administration, an agency in which this Subcommittee has a keen interest, and which already is very busy administering retirement, disability, and survivor benefits.

The employment eligibility verification process relies heavily on SSA to confirm the validity of Social Security numbers assigned to workers. We currently have a modest employment eligibility verification system, formerly called Basic Pilot and now called EEVS. It is used by about 17,000 employers at 73,000 hiring sites.

The major immigration reform proposals being considered all envision a massive expansion of the system to cover all employers, at an estimated 7½ million hiring sites. These employers account for about 60 million hiring decisions per year.

This expansion would present a very substantial new burden on SSA, which would receive upward of 60 million queries per year. If an employee's information does not match SSA's records, he or she must contact SSA, often in person, to present documentation and correct the record in order to keep their job.

We will hear from SSA and other experts about how there are errors and discrepancies in the databases that would be used by the system. Even a low error rate of 4 percent, the estimated percentage of errors in a key SSA database, would result in millions of American workers having to contact SSA before they can be hired. Most of them would be U.S. citizens.

We will also hear from an EPR panel of witnesses who will testify on how the proposed system would impact workers, their employers, and the privacy rights of American taxpayers, all of whom will be affected by the proposed EEVS legislation.

Finally, we must also be wary of proposals that depend on the Social Security Administration to create a new national ID card, which is very costly and runs counter to efforts here and in the states to combat identity theft.

If EEVS is to be a key enforcement tool for immigration policy, we must ensure that the system is effective, efficient, and feasible for SSA, for employers, and for employees. We must also ensure that if SSA is going to be given a major new role in enforcing immigration law, it must be provided with adequate resources to fulfill this new charge without compromising its core duty to administer Social Security.

At this time I would like to yield to my very good friend, distinguished veteran, and colleague, Sam Johnson, for an opening statement.

Mr. JOHNSON. Thank you, Mr. Chairman. I thank my colleague from New York. With New York and Texas on board, we can probably get it done. What do you think, Sandy?

Mr. LEVIN. I think so. That is called power.

Mr. JOHNSON. I appreciate you holding this hearing on current and proposed employment eligibility verification systems. I support helping employers who want to do the right thing and obey our immigration laws. I want to see our immigration laws enforced to deter those employers from knowingly breaking the law and hiring illegal immigrants.

Because ID verification is an essential component of worksite enforcement, I want to protect workers from having their identities stolen by someone working under their name and their Social Security number.

Right now the Social Security Administration works with the Department of Homeland Security to help employers voluntarily verify the identifying information and employment eligibility of their new hires. This verification system, known as the Employment Eligibility Verification System, or EEVS, formerly referred to as the Basic Pilot Program. Now any employer can use it for free if they choose.

Our colleagues in the Senate are now debating immigration overhaul. One section of the Senate bill would require employers to verify that all their employees are work-authorized. In other words, for the first time, businesses would be required to obtain Federal approval for their employees from a law enforcement agency.

I find this to be a little chilling, and I think most Americans would oppose having to go through a law enforcement agency to gain work authorization. Also, this new and unfunded employer mandate would place significant burdens on employers, particularly small business, and the Social Security Administration.

GAO and others have raised concerns regarding the accuracy of the underlying databases this system would rely on and whether responses would be timely if all employers were required to use the system, as opposed to less than 1 percent of employers using the system today.

Worse, the current system relies on a number of so-called identity documents which don't stop identity thieves or the creation of false documents. We need to find common sense solutions to these problems.

The lure of employment opportunities in the United States has long been acknowledged as a major reason for immigration, both legal and illegal. Cutting off the demand for illegal workers through enforcement of employment laws will help us secure our borders.

This Subcommittee has had eight hearings in the past 4 years focusing on Social Security number verification as well as ID issues. It is now time for us to improve the employment eligibility verification process so that American employers can confidently hire people to work. Today's witnesses will help us determine the best way how.

Thank you, Mr. Chairman.

Chairman MCNULTY. I thank the distinguished Ranking Member. Without objection, any additional opening statements by Mem-

bers of the Committee will be included in the record. Of course, the statements by the witnesses will be included in the record in their entirety. We would ask, as usual, that in your testimony, you summarize your testimony within about 5 minutes so that we can allow for a maximum amount of time for the various questions.

Panel No. 1 consists of Frederick Streckewald, Assistant Deputy Commissioner for Program Policy, Office of Disability and Income Security Programs, of SSA; Steve Schaeffer, Assistant Inspector General for the Office of Audit, Social Security Administration, Office of the Inspector General; and Richard Stana, Director of Homeland Security and Justice, Government Accountability Office.

I thank all of you for being here today. We will start with Mr. Streckewald, and take all of your testimony together, and then proceed to questions.

Mr. Streckewald.

STATEMENT OF FREDERICK G. STRECKEWALD, ASSISTANT DEPUTY COMMISSIONER FOR PROGRAM POLICY, OFFICE OF DISABILITY AND INCOME SECURITY PROGRAMS, SOCIAL SECURITY ADMINISTRATION

Mr. STRECKEWALD. Mr. Chairman and Members of the Subcommittee, thank you for inviting me here today to discuss SSA's role in helping to administer the Department of Homeland Security's Employment Eligibility Verification System or EEVS. This system, formerly known as the Basic Pilot Program, allows employers to verify the employment eligibility information provided by newly hired employees.

Worksite enforcement is key to successful immigration reform, and a critical component of worksite enforcement is a strong employer verification system. The Administration supports mandatory participation in an employment eligibility verification system by all United States employers. We are pleased that you are holding the hearing today to discuss the impact of the expansion of EEVS on SSA, employers, and their employees.

Let me begin with a little background on the current system. In 1996, Congress enacted the Immigration Reform and Immigrant Responsibility Act, which required testing three alternative methods of providing an effective, nondiscriminatory employment eligibility confirmation process. The current EEVS was one of these methods.

Today there are more than 17,000 employers participating in EEVS at more than 77,000 worksites. So, far in 2007, we have handled more than 1.8 million queries, an increase of 96 percent over the same period last year.

Employers participate voluntarily, and they register with DHS to use the automated system to verify an employee's Social Security number and work authorization status. The employer submits to the system information from the employee Form I–9. DHS then sends this information to SSA to verify for all new employees that the Social Security number, name, and date of birth match SSA records.

For individuals alleging U.S. citizenship, SSA will also confirm citizenship status, thereby confirming work authorization. For all non-citizens, if there is a match with SSA, DHS then determines

the current work authorization status. DHS then notifies the employer of the result. Ninety-two percent of initial verification queries are confirmed within seconds.

Proposals pending in Congress would require all employers in the United States to use the EEVS to verify employment eligibility and the identity of all new hires. These proposals would phase in participation over a period of time. Every year, however, approximately 60 million individuals start a new job. Therefore, we would expect mandatory participation to have a substantial effect on our Agency.

SSA's role in EEVS relies upon the information in our Numident database, which houses the name, date of birth, and Social Security number of more than 441 million individuals. We have great confidence in the integrity of the Numident, but in any large system of records there will be some that require updating or correcting.

Our current experience with voluntary EEVS shows that for every 100 queries submitted to the system, SSA field offices or phone representatives are contacted three times. We anticipate that in a mandatory system, the percentage of individuals coming to us will be higher than in the current voluntary system.

If Congress enacts a mandatory EEVS, it is crucial that the tools and resources be in place to ensure that the system works efficiently and effectively, and that the proper safeguards are built in to guarantee that United States citizens and work-authorized noncitizens receive prompt confirmation of their work authorization status.

Again, thank you for inviting me here today. We are grateful for your ongoing efforts to ensure the Agency has the funding it needs to accomplish its mission. On behalf of SSA, I want to thank you for your continuing support for the Agency, for our mission, and for our dedicated workforce.

I will be happy to answer any questions you may have.

[The prepared statement of Mr. Streckewald follows:]

Chairman MCNULTY. Thank you.

Prepared Statement of Frederick G. Streckewald, Assistant Deputy Commissioner for Program Policy, Office of Disability and Income Security Programs, Social Security Administration

Mr. Chairman and Members of the Subcommittee:

Thank you for inviting me here today to discuss the Social Security Administration's (SSA's) role in helping to administer the Department of Homeland Security's (DHS) Employment Eligibility Verification System (EEVS). This system, formerly known as the Basic Pilot Program, allows employers to verify the employment eligibility information provided by newly hired employees.

Worksite enforcement is key to successful immigration reform, and a critical component of worksite enforcement is a strong employer verification system. The Administration supports—and proposals currently pending before Congress incorporate—mandatory participation in an employment eligibility verification system by all United States employers. We are pleased that you are holding this hearing today to discuss the impact of the expansion of EEVS on SSA, employers and their employees. We are keenly aware of the need to ensure that the system works the way it is intended.

The History of the Current Voluntary System

The Immigration Reform and Control Act (IRCA) of 1986 required employers for the first time to examine worker documents to check the employment eligibility of newly hired employees. Ten years later, in 1996, Congress enacted the Illegal Immigration Reform and Immigrant Responsibility Act (IIRIRA), which required testing

three alternative methods of providing an effective, nondiscriminatory employment eligibility confirmation process; the current EEVS was one of the three methods.

The law required the voluntary EEVS to be implemented in a minimum of 5 of the 7 States with the highest estimated population of noncitizens not lawfully present in the United States. The five states were California, Florida, Illinois, New York and Texas.

In March 1999, Nebraska was added to assist employers in the meatpacking industry. Employers in those six states were also allowed to include their work sites located in other states. In 2002, Congress extended authorization for the system for an additional 2 years. In 2003, Congress again extended the EEVS and expanded the voluntary participation to include employers in all 50 States. The system will expire in 2008 under current law.

In December 2004, before the nationwide expansion, there were 2,924 participating employers. Today, there are more than 17,000 employers participating in the EEVS at more than 77,000 sites, and participation is growing by more than 1,000 employers every month. As the number of participating employers has grown, so has the number of queries we handle. In Fiscal Year (FY) 2005, SSA handled approximately 980,000 queries; in FY 2006, we handled over 1,740,000. So far, in FY 2007, we have handled more than 1,800,000 queries, an increase of 96 percent over the same period last year.

The Process

Employers participate voluntarily and register with DHS to use the automated system to verify an employee's SSN and work authorization status. The employer inputs information into the system from the Form I–9, the Employment Eligibility Verification Form. DHS then sends this information to SSA to verify for all new employees that the Social Security number, name, and date of birth submitted match information in SSA records. For individuals alleging United States citizenship, SSA will also confirm citizenship status, thereby confirming work authorization. For all non-citizens, if there is a match with SSA, DHS then determines the current work authorization status. Within three to five seconds, through the system, DHS notifies the employer of the result; employment authorized, SSA tentative nonconfirmation, DHS verification in progress, or DHS tentative nonconfirmation.

Ninety-two percent of initial verification queries are confirmed within seconds. If SSA cannot confirm that the information matches SSA records or cannot confirm United States citizenship, DHS will notify the employer of the SSA tentative nonconfirmation. The employer must notify the employee of the tentative nonconfirmation in order to provide the employee the opportunity to contest that finding. If the employee contests the tentative nonconfirmation, he or she has eight days to visit an SSA office with the required documents to correct the SSA record. The employer must re-query the system to verify that the tentative nonconfirmation has been resolved.

SSA has a good ongoing working relationship with DHS. Together, we continue to work to improve upon the operation of the current system—to make it work more efficiently and more smoothly for employers and their employees. We have begun laying the groundwork to increase our capacity to handle substantially heavier volumes of verification transactions, as the voluntary program continues to grow. If Congress mandates the use of the system, these improvements will facilitate nationwide expansion.

Mandatory Participation

There are several proposals now pending in Congress that would require all employers in the United States to use the EEVS to verify the employment eligibility and identity of all new hires. The bills we have seen provide for some kind of phased-in approach to mandatory participation and require employers operating in the Nation's critical infrastructures to be the first participants. Some proposals also require employers to verify the employment eligibility and identity of their entire workforce and to periodically re-verify the work authorization status of individuals whose temporary work authorization is set to expire.

As I mentioned earlier, SSA and DHS are already working to lay the groundwork for broader employer participation in the current EEVS. Every year, approximately 60 million individuals start a new job. Therefore, we would expect mandatory participation to have a substantial effect on our Agency. It is vitally important that, when Congress makes a decision regarding the implementation of a mandatory program, we have adequate lead-time and resources. With these tools, we can effectively expand the EEVS and ensure that it works successfully without impinging on our ability to handle our other workloads.

SSA Records

SSA matches information submitted by the employer against the information in our Numident database, which houses the identifying information, including name, date of birth, and SSN of more than 441 million individuals. We have great confidence in the integrity of the Numident information. In fact, in a December 2006 report issued to Congress, SSA's Office of Inspector General (OIG) commended the accuracy of Numident information.

Of course, in any large system of records, there will be records that require updating or correcting. For example, the OIG found discrepancies in 4.1 percent of Numident records that might lead to tentative nonconfirmations and that 7 percent of naturalized citizens had not updated their Numident records to reflect their new citizenship status. In the administration of our programs, we update or correct our records at the time an individual applies for a replacement card, requests a change in the record—a name change, for example—or applies for a Social Security benefit. As part of the process to correct our records, we need to verify the identity of the individual whose records we are updating and the information we are adding to the individual's records. That is why virtually all of these changes are made during a face-to-face interview in our field offices.

One way we provide individuals the opportunity to review and, if necessary, correct their wage records is the annual Social Security Statement that goes to each worker 25 years or older. The Statement provides individuals with an annual report of wages recorded. In FY 2006, SSA mailed approximately 145 million Statements.

Our current experience with voluntary EEVS shows that for every 100 queries submitted to the System, SSA field offices or phone representatives are contacted three times. As the number of participating employers increases, the number of related contacts with SSA will also increase. We anticipate that in a mandatory system the percentage of individuals coming to us will be higher than in the current voluntary system.

As you know, the Agency is currently facing substantial challenges in meeting the workloads of our core programs. With timely and adequate funding, we will be able to meet the demands of a phased-in approach to mandatory participation. We are grateful for your ongoing efforts to ensure the Agency has the funding it needs to accomplish its missions.

Conclusion

At SSA, we have a proven performance record and can and will do what we are called upon to do. The Administration supports a strong employer verification system as a critical element of a successful and comprehensive approach to immigration reform. As increasing numbers of employers participate in the current voluntary EEVS, and considering the even greater number that will participate if mandated by Congress, it is crucial that the tools and resources be in place to ensure that the system works efficiently and effectively and that the proper safeguards are built in to guarantee that United States citizens and work authorized noncitizens receive prompt confirmation of their work authorization status.

I want to thank the Chairman and members of the Subcommittee for inviting me here today. On behalf of SSA, I want to thank the Subcommittee for its continuing support for the Agency, for our mission, and for our dedicated workforce.

I will be happy to answer any questions you might have.

Mr. Schaeffer.

STATEMENT OF STEVEN L. SCHAEFFER, ASSISTANT INSPECTOR GENERAL FOR THE OFFICE OF AUDIT, SOCIAL SECURITY ADMINISTRATION OFFICE OF THE INSPECTOR GENERAL

Mr. SCHAEFFER. Good morning, Chairman McNulty, Mr. Johnson, and Members of the Subcommittee. It is a pleasure to be here today to provide the Social Security Administration's Office of Inspector General's perspective on Employment Eligibility Verification Systems, or EEVS.

Each agency involved in EEVS has its own contribution to make to the system's success. The SSA OIG's role is to evaluate the use of SSA data within the EEVS process and recommend improvements with respect to the accuracy and the security of such data.

SSA's information constitutes the foundation of EEVS. The purpose of our evaluations and reviews is to assist SSA in improving

the accuracy of the employer wage reporting and reducing SSN misuse and identity theft.

In 2006, the former Chairman of this Subcommittee, Mr. McCrery, asked us to conduct several reviews relative to EEVS. First, to assess the accuracy of the data used by EEVS, we turned to SSA's Numident file. This file contains relevant information about Social Security number holders, including name, date of birth, place of birth, and citizenship status, and these data are used in the EEVS.

Although we found SSA's information to be generally accurate, we identified discrepancies in an estimated 18 million, or 4 percent, of the Numident records that could result in incorrect feedback to employers attempting to determine the employment eligibility of their workers.

This incorrect feedback could lead to both false positives and false negatives for employees. In addition, verification problems may delay the hiring process and lead to an increase in visits to SSA's field offices.

In our second review, to assess the functionality of EEVS, we gathered information on the experience of employers who had used EEVS, as well as those who had used SSA's Social Security number verification service or SSNVS. We found that 100 percent of the EEVS users interviewed rated the programs as excellent, very good, or good. In addition, at least 98 percent of the users indicated that their employers were very likely to continue to use the programs.

About 10 percent of the EEVS users reported that they experienced minor problems using the two programs. In most of the cases, the user reported that SSA and/or DHS staff were able to resolve their problems timely.

We also found, however, that approximately 42 percent of EEVS users were not using the program as intended. While the program is intended to verify the work authorization of newly hired employees within 3 days after they are hired, some employers conducted verifications for longstanding employees or individuals who were not yet hired. Monitoring appropriate use should be part of any enhanced system.

In the third review conducted at the Subcommittee's request, we assessed controls over EEVS and SSA's SSNVS to monitor potential abuse by employers, as well as SSA and DHS's experience to date with this monitoring. We found that SSA had established effective controls over access and use of sensitive data in its SSNVS program, as well as effective controls to detect anomalies in SSNVS usage and potential misuse of the program.

While we found that EEVS did not have the same level of controls, we reported that DHS officials were meeting with counterparts from SSA and the IRS to discuss potential enhancements to EEVS, avenues for greater cooperation, and the potential for adopting some of the monitoring and applicant verification activities already being performed under SSNVS.

We are now completing a fourth review where we are assessing controls over all of SSA's employee verification programs as well as EEVS. This review will also highlight best practices, and as a part of the audit, we will determine whether employers are receiving a

consistent reply from all of these services. We expect to issue this report in the next few months, and as always, will share a copy with the Committee.

Through reports such as these, our efforts to ensure the reliability of the data used by EEVS and the functionality and security of EEVS helps employers report accurate wages to SSA and minimize the improper use of SSNs.

Thank you, and I will be happy to answer any questions.

Chairman MCNULTY. Thank you, Mr. Schaeffer.

Mr. Stana.

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

Mr. STANA. Thank you, Chairman McNulty, Mr. Johnson, Members of the Subcommittee. I appreciate the opportunity to participate in today's hearing on EEVS. As we and others have reported in the past, the opportunity for employment is a key magnet attracting illegal aliens to the United States. In 1986, Congress passed the Immigration Reform and Control Act, which established an employment verification process for employers to verify all new hired employees' work eligibility, and a sanctions program for fining employers who do not comply with the Act. The availability and use of counterfeit documents, and the fraudulent use of valid documents belonging to others, have made it difficult for employers who want to comply with current employment verification processes to ensure that they hire only authorized workers. Counterfeit documents have also made it easier for employers who don't want to comply and knowingly hire unauthorized workers to do so without fear of sanction.

Over the years, immigration experts have said that the single most important step that could be taken to manage lawful immigration and reduce unlawful migration is to develop an effective system for verifying work authorization. DHS and SSA currently operate the EEVS program, which is a voluntary automated system authorized by the 1996 Immigration Act, for employers to electronically check employees' work eligibility information against information in DHS and SSA databases. Of the 5.9 million employers in the U.S., about 17,000 employers are now registered to use the program, and only about half of these are active users. This program shows promise to help identify the use of counterfeit documents and assist U.S. Immigration and Customs Enforcement in better targeting its worksite enforcement efforts, but the following areas would need to be addressed before it is expanded to all employers and is effectively implemented as envisioned in various immigration reform proposals.

First, program capacity would need to be expanded. DHS estimated that increasing EEVS capacity could cost it $70 million annually for program management and $300 million to $400 million annually for compliance activities and staff. SSA officials estimated that expansion of the EEVS program to 100,000 participants from the current 17,000 would cost $5 to $6 million, and noted that the cost of a mandatory EEVS would be much higher and driven by in-

creased workload of its field office staff who resolve queries that SSA cannot immediately confirm.

Second, data reliability issues would need to be addressed. The majority of EEVS queries entered by employers, about 92 percent, are confirmed within seconds that the employee is work-authorized. About 7 percent of the queries cannot be immediately confirmed by SSA, and about 1 percent cannot be immediately confirmed by DHS. Resolving these nonconfirmations can take several days, or in a few cases even weeks. DHS and SSA are considering options for using additional automated checks to immediately confirm work authorization, which may be important should EEVS be made mandatory for all employers.

Third, while EEVS may help to reduce document fraud, it cannot yet fully address identity fraud issues, for example, when employees present borrowed or stolen genuine documents. The current EEVS program is piloting a photograph screening tool, whereby an employer can more easily identify fraudulent documentation. DHS expects to expand the use of this tool to all participating employers by September 2007. Although mandatory EEVS and the associated use of the photograph screening tool offer some remedy, limiting the number of acceptable work authorization documents and making them more secure would help to better address identity fraud issues.

Finally, EEVS is vulnerable to employer fraud, such as entering the same identity information to authorize multiple workers. EEVS is also vulnerable to employer misuse that adversely affects employees, such as employers limiting work assignments or pay while employees are undergoing the verification process. Currently there is no formal mechanism for sharing compliance data with ICE agents. DHS is establishing a new compliance and monitoring program to help reduce employer fraud and misuse by, for example, identifying patterns in employer noncompliance with program requirements. Information suggesting employers' fraud and misuse of the system could be useful in targeting limited worksite enforcement resources and promoting employer compliance with employment laws.

As an aside, our report last summer on selected countries' experiences with foreign worker programs found that while different approaches were used, and no country we studied did everything perfectly or effectively, many of the same issues existed in these countries as exist here. These include ensuring only that those authorized to work could obtain employment; that employers comply with laws governing worksite conditions; that taxes and social insurance payments are collected; and that appropriate mechanisms are available, including data matching and sharing among agencies, to help reduce immigration and labor law violations.

In closing, both DHS and SSA have taken a number of steps to address weaknesses in the current EEVS program, but much more needs to be done if this is going to be expanded to all employers. This will require a substantial investment in staff and other resources, at least in the near term, in both agencies. Implementing an EEV program that ensures that all individuals working in the country are doing so legally, and that undue burdens are not

placed on employers or employees, will not be an easy task within the timelines suggested in immigration reform proposals.

This concludes my oral statement, and I would be happy to answer any questions that Members of the Subcommittee may have.

[The prepared statement of Mr. Stana follows:]

Prepared Statement of Richard Stana, Director of Homeland Security and Justice, Government Accountability Office

Mr. Chairman and Members of the Subcommittee:

I appreciate the opportunity to be here today to participate in this hearing on electronic employment verification. As we and others have reported in the past, the opportunity for employment is one of the most powerful magnets attracting unauthorized immigrants to the United States. To help address this issue, in 1986 Congress passed the Immigration Reform and Control Act (IRCA),[1] which made it illegal for individuals and entities to knowingly hire, continue to employ, or recruit or refer for a fee unauthorized workers. The act established a two-pronged approach for helping to limit the employment of unauthorized workers: (1) an employment verification process through which employers verify all newly hired employees' work eligibility and (2) a sanctions program for fining employers who do not comply with the act.[2]

Following the passage of IRCA, the U.S. Commission on Immigration Reform and various immigration experts indicated a number of problems with the implementation of immigration policies and concluded that deterring illegal immigration requires, among other things, strategies that focus on disrupting the ability of illegal immigrants to gain employment through a more reliable employment eligibility verification process. In particular, the commission report and other studies found that the single most important step that could be taken to reduce unlawful migration is the development of a more effective system for verifying work authorization. In the over 20 years since passage of IRCA, the employment eligibility verification process has remained largely unchanged. The House and Senate are considering legislation to reform immigration laws and strengthen electronic employment verification. Some of this legislation includes proposals that would require implementing a mandatory, functional electronic employment verification program for all employers before other immigration-related reforms could be initiated. Currently, the U.S. Citizenship and Immigration Services (USCIS) administers, and Social Security Administration (SSA) supports, a voluntary electronic employment verification program, called the Employment Eligibility Verification (EEV) program.

My testimony today is an update of our prior work regarding employment verification and worksite enforcement. Specifically, I will discuss our observations on the current electronic employment verification program and challenges to making the program mandatory for all employers.

In preparing this testimony, we reviewed our past work on employment verification and worksite enforcement efforts.[3] We analyzed updated information provided by U.S. Immigration and Customs Enforcement (ICE), USCIS, and SSA officials on steps they are taking to address weaknesses identified in our prior work, as well as challenges their agencies may face if an electronic employment verification program were made mandatory. We examined regulations, guidance, and other studies on the employment verification process. We also analyzed a report on the results of an independent evaluation of the electronic employment eligibility verification program, then known as the Basic Pilot program, conducted by the Institute for Survey Research at Temple University and Westat in June 2004.[4] Fur-

---

[1] Pub. L. No. 99–603, 8 U.S.C. § 1324a.

[2] IRCA provided for sanctions against employers who do not follow the employment verification (Form I–9) process. Employers who fail to properly complete, retain, or present for inspection a Form I–9 may face civil or administrative fines ranging from $110 to $1,100 for each employee for whom the form was not properly completed, retained, or presented. Employers who knowingly hire or continue to employ unauthorized aliens may be fined from $275 to $11,000 for each employee, depending on whether the violation is a first or subsequent offense. Employers who engage in a pattern or practice of knowingly hiring or continuing to employ unauthorized aliens are subject to criminal penalties consisting of fines up to $3,000 per unauthorized employee and up to 6 months' imprisonment for the entire pattern or practice.

[3] GAO, *Immigration Enforcement: Weaknesses Hinder Employment Verification and Worksite Enforcement Efforts*, GAO–05–813 (Washington, D.C.: Aug. 31, 2005).

[4] Institute for Survey Research and Westat, Findings of the Basic Pilot Program Evaluation (Washington, D.C.: June 2004).

thermore, we received updated data on employer use of the current electronic employment eligibility verification system. We reviewed these data for accuracy and completeness and determined that these data were sufficiently reliable for the purposes of our review. We conducted the work reflected in this statement from September 2004 through July 2005 and updated this information in May and June 2007 in accordance with generally accepted government auditing standards.

Summary

A mandatory EEV would necessitate an increased capacity at both USCIS and SSA to accommodate the estimated 5.9 million employers in the United States.[5] As of May 2007, about 17,000 employers have registered for the EEV program, about half of which are active users. USCIS has estimated that a mandatory EEV could cost USCIS $70 million annually for program management and $300 million to $400 million annually for compliance activities and staff, depending on the method for implementing the program. The costs associated with other programmatic and system enhancements are currently unknown. SSA is currently refining its estimates and was not yet able to provide estimates for the cost of a mandatory EEV. According to SSA officials, the cost of a mandatory EEV would be driven by the field offices' increased workload required to resolve queries that SSA cannot immediately confirm.

USCIS and SSA are exploring options to reduce delays in the EEV process. According to USCIS, the majority of EEV queries entered by employers—about 92 percent—confirm within seconds that the employee is authorized to work. About 7 percent of the queries cannot be immediately confirmed by SSA, and about 1 percent cannot be immediately confirmed by USCIS. With regard to the SSA-issued tentative nonconfirmations,[6] USCIS and SSA officials told us that the majority occur because employees' citizenship or other information, such as name changes, is not up to date in the SSA database. Resolving some DHS nonconfirmations can take several days, or in a few cases even weeks. USCIS and SSA are examining ways to improve the system's ability to use additional automated checks to immediately confirm work authorization.

EEV may help reduce document fraud, but it cannot yet fully address identity fraud issues, for example, when employees present borrowed or stolen genuine documents. The current EEV program is piloting a photograph screening tool, whereby an employer can more easily identify fraudulent documentation. This tool is currently being used by over 70 employers, and USCIS expects to expand the use of the tool to all participating employers by the end of summer 2007. Although mandatory EEV and the associated use of the photograph screening tool offer some remedy, further actions, such as limiting the number of acceptable work authorization documents and making them more secure, may be required to more fully address identity fraud.

EEV is vulnerable to employer fraud that diminishes its effectiveness and misuse that adversely affects employees. ICE officials stated that EEV program data could indicate cases in which employers may be fraudulently using the system and therefore would help the agency better target its limited worksite enforcement resources toward those employers. EEV is also vulnerable to employer misuse that adversely affects employees, such as limiting work assignments or pay while employees are undergoing the verification process. USCIS is establishing a new Compliance and Monitoring program to help reduce employer fraud and misuse by, for example, identifying patterns in employer compliance with program requirements. Information suggesting employers' fraud or misuse of the system could be useful to other DHS components in targeting limited worksite enforcement resources and promoting employer compliance with employment laws.

Background

In 1986, IRCA established the employment verification process based on employers' review of documents presented by employees to prove identity and work eligibility. On the Form I–9, employees must attest that they are U.S. citizens, lawfully

---

[5] In 2004, the most recent year for which data are available, there were approximately 5.9 million firms in the United States. A firm is a business organization consisting of one or more domestic establishments in the same state and industry that were specified under common ownership or control. Under EEV, one employer may have multiple worksites that use the system. For example, a hotel chain could have multiple individual hotels using EEV. This hotel chain would represent one employer using the pilot program.

[6] In general, in cases when the EEV system cannot confirm an employee's work authorization status through the initial automatic check, the system issues the employer either an SSA or a DHS tentative nonconfirmation of the employee's work authorization status, which requires the employee to resolve any data inaccuracies if he or she is able or chooses to do so.

admitted permanent residents, or aliens authorized to work in the United States. Employers must then certify that they have reviewed the documents presented by their employees to establish identity and work eligibility and that the documents appear genuine and relate to the individual presenting them. In making their certifications, employers are expected to judge whether the documents presented are obviously counterfeit or fraudulent. Employers generally are deemed in compliance with IRCA if they have followed the Form I–9 process in good faith, including when an unauthorized alien presents fraudulent documents that appear genuine. Following the passage of IRCA in 1986, employees could present 29 different documents to establish their identity and/or work eligibility. In a 1997 interim rule, the former U.S. Immigration and Naturalization Service (INS) reduced the number of acceptable work eligibility documents from 29 to 27.[7]

The Illegal Immigration Reform and Immigrant Responsibility Act (IIRIRA)[8] of 1996 required the former INS and SSA to operate three voluntary pilot programs to test electronic means for employers to verify an employee's eligibility to work, one of which was the Basic Pilot Program.[9] The Basic Pilot Program was designed to test whether pilot verification procedures could improve the existing employment verification process by reducing (1) false claims of U.S. citizenship and document fraud, (2) discrimination against employees, (3) violations of civil liberties and privacy, and (4) the burden on employers to verify employees' work eligibility.

In 2007, USCIS renamed the Basic Pilot Program the Employment Eligibility Verification (EEV) program. EEV provides participating employers with an electronic method to verify their employees' work eligibility. Employers may participate voluntarily in EEV, but are still required to complete Forms I–9 for all newly hired employees in accordance with IRCA. After completing the forms, these employers query EEV's automated system by entering employee information provided on the forms, such as name and Social Security number, into the EEV Web site within 3 working days of the employees' hire date. The program then electronically matches that information against information in SSA's NUMIDENT database and, for noncitizens, DHS databases to determine whether the employee is eligible to work. EEV electronically notifies employers whether their employees' work authorization was confirmed. Those queries that the DHS automated check cannot confirm are referred to DHS immigration status verifiers, who check employee information against information in other DHS databases. The EEV process is shown in figure 1.

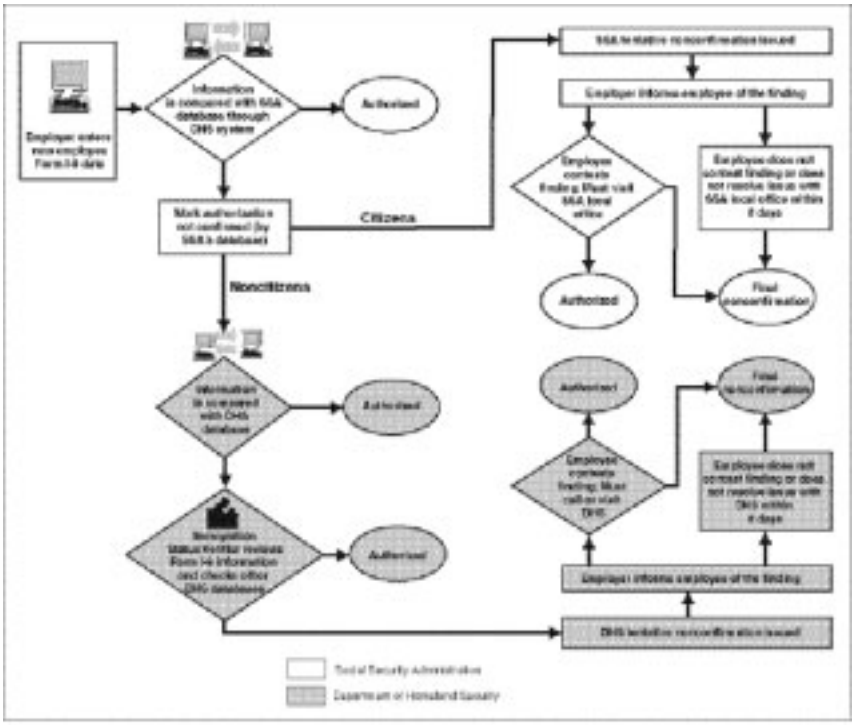
---

[7] Eight of these documents establish both identity and employment eligibility (e.g., U.S. passport or permanent resident card); 12 documents establish identity only (e.g., driver's license); and 7 documents establish employment eligibility only (e.g., Social Security card).

[8] U.S.C. 1324a(b). IIRIRA was enacted within a larger piece of legislation, the Omnibus Consolidated Appropriations Act, 1997, Pub. L. No. 104–208, 110 Stat. 3009.

[9] The other two pilot programs mandated by IIRIRA—the Citizen Attestation Verification Pilot Program and the Machine-Readable Document Pilot Program—were discontinued in 2003 due to technical difficulties and unintended consequences identified in evaluations of the programs. See Institute for Survey Research and Westat, *Findings of the Citizen Attestation Verification Pilot Program Evaluation* (Washington, D.C.: April 2003) and Institute for Survey Research and Westat, *Findings of the Machine-Readable Document Pilot Program Evaluation* (Washington, D.C.: May 2003).

Figure 1: Electronic Employment Verification Program Verification Process



In cases when EEV cannot confirm an employee's work authorization status either through the automatic check or the check by an immigration status verifier, the system issues the employer a tentative nonconfirmation of the employee's work authorization status. In this case, the employers must notify the affected employees of the finding, and the employees have the right to contest their tentative nonconfirmations by contacting SSA or USCIS to resolve any inaccuracies in their records within 8 days. During this time, employers may not take any adverse actions against those employees, such as limiting their work assignments or pay. After 10 days, employers are required to either immediately terminate the employment or notify DHS of the continued employment of workers who do not successfully contest the tentative nonconfirmation and those who the pilot program finds are not work-authorized.

The EEV program is a part of USCIS's Systematic Alien Verification for Entitlements Program, which provides a variety of verification services for federal, state, and local government agencies. USCIS estimates that there are more than 150,000 federal, state, and local agency users that verify immigration status through the Systematic Alien Verification for Entitlements Program. SSA also operates various verification services. Among these are the Employee Verification Service (EVS) and the Web-based SSN Verification Service (SSNVS), which can be used to provide verification that employees' names and Social Security numbers match SSA's records. These services, designed to ensure accurate employer wage reporting, are offered free of charge. Employer use is voluntary, and the services are not widely used.

EEV Would Require An Increase in Capacity at USCIS and SSA

Mandatory electronic employment verification would substantially increase the number of employers using the EEV system, which would place greater demands on USCIS and SSA resources. As of May 2007, about 17,000 employers have registered to use the program, 8,863 of which were active users,[10] and USCIS has esti-

[10] Active users are those employers who have run at least one query in fiscal year 2007.

mated that employer registration is expected to greatly increase by the end of fiscal year 2007. If participation in the EEV program were made mandatory, the program may have to accommodate all of the estimated 5.9 million employers in the United States. USCIS officials estimate that to meet a December 2008 implementation date, this could require about of 30,000 employers to register with the system per day. The mandatory use EEV can affect the capacity of the system because of the increased number of employer queries.

USCIS has estimated that a mandatory EEV could cost USCIS $70 million annually for program management and $300 million to $400 million annually for compliance activities and staff. The costs associated with other programmatic and system enhancements are currently unknown. According to USCIS, cost estimates will rise if the number of queries rises, although officials noted that the estimates may depend on the method for implementing a mandatory program. SSA officials told us they have estimated that expansion of the EEV program to levels predicted by the end of fiscal year 2007 would cost $5 to $6 million, but SSA was not yet able to provide us estimates for the cost of a mandatory EEV. According to SSA officials, the cost of a mandatory EEV would be driven by the increased workload of its field office staff due to resolving SSA tentative nonconfirmations.[11]

A mandatory EEV would require an increase in the number of USCIS and SSA staff to operate the program. For example, USCIS had 13 headquarters staff members in 2005 to run the program and 38 immigration status verifiers available for secondary verification.[12] USCIS plans to increase staff levels to 255 to manage a mandatory program, which includes increasing the number of immigration status verifiers who conduct secondary verifications.[13] USCIS officials expressed concern about the difficulty in hiring these staff due to lengthy hiring processes, which may include government background checks. In addition, according to SSA officials, a mandatory EEV program would require additional staff at SSA field offices to accommodate an increase in the number of individuals visiting SSA field offices to resolve tentative nonconfirmations. According to SSA officials, the number of new staff required would depend on both the legislative requirements for implementing mandatory EEV and the effectiveness of efforts USCIS has under way to decrease the need for individuals to visit SSA field offices. For this reason, SSA officials told us they have not yet estimated how many additional staff they would need for a mandatory EEV.

USCIS and SSA Are Exploring Options to Reduce Delays in the EEV Process

In prior work, we reported that secondary verifications lengthen the time needed to complete the employment verification process. The majority of EEV queries entered by employers—about 92 percent—confirm within seconds that the employee is authorized to work. About 7 percent of the queries are not confirmed by the initial automated check and result in SSA-issued tentative nonconfirmations, while about 1 percent result in DHS-issued tentative nonconfirmations. With regard to the SSA-issued tentative nonconfirmations, USCIS and SSA officials told us that the majority occur because employees' citizenship status or other information, such as name changes, is not up to date in the SSA database. SSA does not update records unless an individual requests the update in person and submits the required evidence to support the change in its records. USCIS officials stated that, for example, when aliens become naturalized citizens, their citizenship status is often not updated in the SSA database. In addition, individuals who have changed their names for various reasons, such as marriage, without notifying SSA in person may also be issued an SSA tentative nonconfirmation. According to SSA officials, although SSA instructs individuals to report any changes in name, citizenship, or immigration status, many do not do so. When these individuals' information is queried through EEV, a tentative nonconfirmation would be issued, requiring them to go to an SSA field office to show proof of the change and to correct their records in SSA's database.

USCIS and SSA are exploring some options to improve the efficiency of the verification process. For example, USCIS is exploring ways to automatically check

[11] In general, in cases when the EEV system cannot confirm an employee's work authorization status through the initial automatic check, the system issues the employer a tentative nonconfirmation of the employee's work authorization status.

[12] Thirty-eight immigration status verifiers were available for completing secondary verifications. According to USCIS, at any one time about 3 to 5 immigration status verifiers work to resolve tentative nonconfirmations. The other immigration status verifiers work on other verification programs, such as the Systematic Alien Verification for Entitlements Program.

[13] USCIS officials noted that this does not include staff for monitoring and compliance functions.

for naturalized citizens' work authorization using DHS databases before the EEV system issues a tentative nonconfirmation. Furthermore, USCIS is planning to provide naturalized citizens with the option, on a voluntary basis, to provide their Alien Number or Naturalization Certification Number so that employers can query that information through the EEV system before referring the employees to SSA to resolve tentative nonconfirmations.[14] SSA is also coordinating with USCIS to develop an automated secondary verification capability, which may reduce the need for employers to take additional steps after the employee resolves the SSA tentative nonconfirmation.[15] USCIS and SSA officials told us that the agencies are planning to provide SSA field office staff with access to the EEV system so that field office staff can resolve the SSA tentative nonconfirmation directly in the system at the time the employee's record is updated at the field office. According to SSA officials, the automated secondary verification capability is tentatively scheduled to be implemented by October 2007. While these steps may help improve the efficiency of the verification process, including eliminating some SSA tentative nonconfirmations, they will not entirely eliminate the need for some individuals to visit SSA field offices to update records when individuals' status or other information changes.

USCIS and SSA officials noted that because the current EEV program is voluntary, the percentage of individuals who are referred to SSA field offices to resolve tentative nonconfirmations may not accurately indicate the number of individuals who would be required to do so under a mandatory program. SSA and USCIS officials expressed concern about the effect on SSA field offices' workload of the number of individuals who would be required to physically visit a field office if EEV were made mandatory.

May Help Reduce Employee Document Fraud, but Cannot Yet Fully Address Identity Fraud Issues

In our prior work, we reported that EEV enhances the ability of participating employers to reliably verify their employees' work eligibility and assists participating employers with identification of false documents used to obtain employment.[16] If newly hired employees present false information, EEV would not confirm the employees' work eligibility because their information, such as a false name or social security number, would not match SSA and DHS database information. However, the current EEV program is limited in its ability to help employers detect identity fraud, such as cases in which an individual presents borrowed or stolen genuine documents.

USCIS has taken steps to reduce fraud associated with the use of documents containing valid information on which another photograph has been substituted for the document's original photograph. In March 2007, USCIS began piloting a photograph screening tool as an addition to the current EEV system. According to USCIS officials, the photograph screening tool is intended to allow an employer to verify the authenticity of a Lawful Permanent Resident card (green card) or Employment Authorization Document that contain photographs of the document holder by comparing individuals' photographs on the documents presented during the I–9 process to those maintained in DHS databases. As of May 2007, about 70 employers have been participating during the pilot phase of the photograph screening tool, and EEV has processed about 400 queries through the tool. USCIS expects to expand the program to all employers participating in EEV by the end of summer 2007.

The use of the photograph screening tool is currently limited because newly hired citizens and noncitizens presenting forms of documentation other than green cards or Employment Authorization Documents to verify work eligibility are not subject to the tool. Expansion of the pilot photograph screening tool would require incorporating other forms of documentation with related databases. In addition, efforts to expand the tool are still in the initial planning stages. For example, according to USCIS officials, USCIS and the Department of State have begun exploring ways to include visa and U.S. passport documents in the tool, but these agencies have not yet reached agreement regarding the use of these documents. USCIS is also exploring a possible pilot program with state Departments of Motor Vehicles.

In prior work we reported that although not specifically or comprehensively quantifiable, the prevalence of identity fraud seemed to be 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 authoriza-

---

[14] According to USCIS, providing these data to employers would be voluntary to help ensure that naturalized citizens are not subject to discrimination.

[15] Currently, once an individual resolves the reason for the SSA tentative nonconfirmation, the employer must then re-query the EEV system in order to finalize the verification.

[16] GAO–05–813.

tion documents—27 under the current employment verification process—along with inherent vulnerabilities to counterfeiting of some of these documents, may complicate efforts to address identity fraud. Although mandatory EEV and the associated use of the photograph screening tool offers some remedy, further actions, such as reducing the number of acceptable work eligibility documents and making them more secure, may be required to more fully address identity fraud.

Most Employers Complied with EEV Procedures, the Program Is Vulnerable to Employer Fraud That Diminishes Its Effectiveness and Misuse That Adversely Affects Employees

While Most Employers Complied with EEV Procedures, the Program Is Vulnerable to Employer Fraud That Diminishes Its Effectiveness and Misuse That Adversely Affects Employees.

EEV is vulnerable to acts of employer fraud, such as entering the same identity information to authorize multiple workers. Although ICE has no direct role in monitoring employer use of EEV and does not have direct access to program information, which is maintained by USCIS, ICE officials told us that program data could indicate cases in which employers may be fraudulently using the system and therefore would help the agency better target its limited worksite enforcement resources toward those employers. ICE officials noted that, in a few cases, they have requested and received EEV data from USCIS on specific employers who participate in the program and are under ICE investigation. USCIS is planning to use its newly created Compliance and Monitoring program to refer information on employers who may be fraudulently using the EEV system, although USCIS and ICE are still determining what information is appropriate to share.

Employees queried through EEV may be adversely affected if employers violate program obligations designed to protect the employees, by taking actions such as limiting work assignments or pay while employees are undergoing the verification process. The 2004 Temple University Institute for Survey Research and Westat evaluation of EEV concluded that the majority of employers surveyed appeared to be in compliance with EEV procedures. However, the evaluation and our prior review found evidence of some noncompliance with these procedures. In 2005, we reported that EEV provided a variety of reports that could help USCIS determine whether employers followed program requirements, but that USCIS lacked sufficient staff to do so. Since then, USCIS has added staff to its verification office and created a Compliance and Monitoring program to review employers' use of the EEV system. However, while USCIS has hired directors for these functions, the program is not yet fully staffed. According to USCIS officials, USCIS is still in the process of determining how this program will carry out compliance and monitoring functions, but its activities may include sampling employer usage data for evidence of noncompliant practices, such as identifying employers who do not appear to refer employees contesting tentative nonconfirmations to SSA or USCIS. USCIS estimates that the Compliance and Monitoring program will be sufficiently staffed to begin identifying employer noncompliance by late summer 2007.

USCIS's newly created Compliance and Monitoring program could help ICE better target its worksite enforcement efforts by indicating cases of employers' egregious misuse of the system. Currently, there is no formal mechanism for sharing compliance data between USCIS and ICE. ICE officials noted that proactive reduction of illegal employment through the use of functional, mandatory EEV may help reduce the need for and better focus worksite enforcement efforts. Moreover, these officials told us that mandatory use of an automated system like EEV could limit the ability of employers who knowingly hired unauthorized workers to claim that the workers presented false documents to obtain employment, which could assist ICE agents in proving employer violations of IRCA.

Concluding Observations

Although efforts to reduce the employment of unauthorized workers in the United States necessitate a strong employment eligibility verification process and a credible worksite enforcement program and other immigration reforms may be dependent on it, a number of challenges face its successful implementation. The EEV program shows promise for enhancing the employment verification process and reducing document fraud if implemented on a much larger scale, and USCIS and SSA have undertaken a number of steps to address many of the weaknesses we identified in the EEV program. USCIS has also spent the last several years planning for an expanded or mandatory program, and has made progress in several areas, but it is unclear at this time the extent to which USCIC's efforts will be successful under mandatory EEV. It is clear, however, that a mandatory EEV system will require a substantial investment in staff and other resources, at least in the near term, in

both agencies. There are also issues, such as identity fraud and intentional misuse, that will remain a challenge to the system. Implementing an EEV system to ensure that all individuals working in this country are doing so legally and that undue burdens are not placed on employers or employees will not be an easy task within the timelines suggested in reform proposals.

This concludes my prepared statement. I would be pleased to answer any questions you and the subcommittee members may have.

Chairman MCNULTY. We thank all of the witnesses for their testimony. Let me just begin by generally framing the issue, and then we will go to some of my colleagues for questions.

This Committee has been working for some time, and as a matter of fact for some years, on the whole issue of the backlog in the disability claims and so on, and all of the problems related to that. And the situation as it exists right now I believe is a national embarrassment. When people are legitimately entitled to a government benefit and come to the government to apply for that benefit, and are told, you have to wait a year and a half or two years just to get an answer, I think that is a disgrace.

So we are working on that as a separate issue, and we made some progress in the budget resolution this year, and we hope to have some results during the appropriations process.

With that as a backdrop, when I look at this issue I see a massive new undertaking here that is going to cost an awful lot of money and require an awful lot of additional backup. I just want to elicit from you your views as to how effective you think we can be in a reasonable timeframe in setting up such a new system.

Now, Mr. Schaeffer, you mentioned additional visits to field offices. If we were to expand this program to the estimated 60 million new hires this year, how many additional field office visits do you think that would entail?

Mr. SCHAEFFER. I would hesitate to put an exact number, but it would be a substantial increase on the visits that are now taking place, and without increased staff, would obviously lead to the disability backlog problem probably being exacerbated as opposed to being addressed timely.

Chairman MCNULTY. Based upon how past Administrations and Congresses have addressed the backlog issue, how confident are you that the resources would be there?

Mr. SCHAEFFER. I would refer to Mr. Streckewald to answer that question.

Chairman MCNULTY. That is fine.

Mr. STRECKEWALD. I really can't hazard a guess, but our position is that we can do whatever Congress asks us. We always have, but need to be funded for it. This, as you said, Mr. Chairman, is a huge new workload for us if we go to mandatory EEVS. I think the estimate of 2 or 3,000 more work years, more people, hundreds of millions of dollars of more money each year, is in the ballpark.

We need time to hire, equip and train new people so that they can do this. We don't know if we would expand our field offices. We would probably try to fit them into the existing field offices and tele-service centers. Our position is we hope Congress does see the need to fund us for this workload so that it doesn't disrupt our

other critical workloads. As you mentioned, one of them is a top priority—the disability hearings.

Chairman MCNULTY. Could you be any more specific with regard to the additional number of work years that would be involved?

Mr. STRECKEWALD. We are still working on our final figures. We are looking at a couple of key elements that get us to that figure. One critical element is the fallout rate. Right now, for every 100 queries, we have three contacts to the field office or the teleservice centers.

So, we are trying to use these key elements as a base and think through what a mandatory system would look like instead of a voluntary system because our assumption is that companies that volunteer for EEVS probably have fewer people trying to pass off as legal workers.

So, we have roughly, in our estimates for mandatory EEVS that we are working on now, doubled the full-out rate. So, we figured it may be as high as 6 percent fallout rate. That fallout rate means that 6 percent of, let's say, 60 million new hires per year will be 3.6 million extra visits or phone calls to our field offices.

Each one of those takes 15 to 20 minutes to resolve, and most of them will be resolved, as my colleague said, in probably just a short period of time. Some of them may take a little longer if we have to go through some additional verification processes.

That is the business process that we already are set up to do. It would just greatly increase the volume of that business process. That is why the funding is so critical.

Chairman MCNULTY. As we move along further in this process and you do your additional analysis, can you give us more specific information?

Mr. STRECKEWALD. I would be glad to do that, and work with the Committee to do that.

Chairman MCNULTY. Great.

Mr. Johnson.

Mr. JOHNSON. Thank you, Mr. Chairman.

I would like to follow up on that, Mr. Streckewald. Why do you need more money and employees if it is all computerized? Theoretically, according to the way I am told it operates, you punch a button and a guy gets an instant response. You just said that.

Mr. STRECKEWALD. Now, 92 percent of the time, you are right. Employers get an instant response. What we are looking at is the ones that don't have an instant response, the ones that don't match our records. It is about 7 percent for our records, I think 1 percent for DHS records.

So, if you look at 7 percent, out of that, some people would never contact SSA because they are illegal workers. A lot of them are legal workers, are citizens, where their records just don't match our records. So, they come into our offices. They show us the proofs that they need to show. We change our records to make sure that they are up to date and then they fit what the employer has. Then employees are authorized to work, and life goes on.

There is a lot of work, depending on the volume, if we go to a mandatory EEVS.

Mr. JOHNSON. How do you report the ones that don't check out? Do you report them to——

Mr. STRECKEWALD. The ones that come through the system and are verified?

Mr. JOHNSON. That aren't verified.

Mr. STRECKEWALD. Well, we do have a system for reporting those, and we are working on a system that allows us to report back to the employer to tell them the status of the resolution of the mis-match. So, we are building that system so that the employers will know and we will know and DHS will know how many cases we get and what the resolution of each case is.

Mr. JOHNSON. Thank you. It is amazing to me that MasterCard and Visa can do it instantly all over the world, and you can't do it here.

Mr. Stana, Mr. Rotenberg, a witness on our next panel, tells us last month the Department of Homeland Security lost the employment records of 100,000 Federal employees containing names, Social Security numbers, dates of birth, and bank account information.

At a time when we are considering a massive expansion of the collection of personal information by DHS, how can we be sure that DHS can adequately safeguard workers' personal information?

Mr. STANA. Well, let me say right up front that GAO has not done a stress test, a privacy test, or we haven't done any penetration testing of the system. We have spoken with DHS about their system, and they capture this sensitive information on an Oracle database. They have done privacy testing, and they are of the opinion that they can safeguard the records. They have done the privacy checks in accordance with law.

Now, having said that, any time you collect data on hundreds of thousands or millions of people, there is always the chance that something may go awry. By the way, the 100,000 example you used, I believe, was a TSA laptop. This is a little bit different. This is a mainframe application, mainly.

Now, we have watched—as Members of the Subcommittee may have—watched USCIS test the EEVS system using a phony name to see what happens. The EEVS system is password protected, and it does have the certain kinds of protections that you would expect to see in remote applications.

So, I guess it would remain to be seen exactly how safe it is. They do need to keep information in these databases because they do want to do pattern testing over time. So, another issue is how long do they keep the information? and DHS hasn't really resolved that yet, either.

Mr. JOHNSON. Well, thank you. According to what I understand, less than 1 percent of the employers are participating in that program now. On page 8 of your testimony, you say that according to DHS, in order to begin implementation for all employers beginning in December 2008, you need 30,000—or 30,000 employers would be required to register with the system per day.

With that, substantial investment will be needed in staffs, systems, resources. Can you assure the Congress that such an enormous data collection processing system can be established?

Mr. STANA. If you ask them to put something in place, something will be in place. Something is in place right now, and it has 17,000 registrants, and 8800 consistent users.

Mr. JOHNSON. Is the "something" going to work? Is that system going to work?

Mr. STANA. They are trying to expand EEVS to about 6 million businesses. It is a very hard thing to do. If I could just put it into perspective, everyone on the dais is working on a two-year term, and there are approximately 18 months left in your term.

So, if you figure it that way, by the end of your term of office for this term—whether you go on to the next term is another thing—DHS has to hire 255 program staff, 1800 monitoring staff, procure office space, develop operating procedures, inform employers how to work the system, support worksite enforcement areas, register approximately 30,000 businesses per day starting now. The longer you wait——

Mr. JOHNSON. Well, how did you get those figures? You said GAO hasn't even looked at it yet.

Mr. STANA. Oh, no. We looked at the program. We did not look at the stress testing on the computer system. These are all things that would have to be done so that by December 2008, it is ready to service 5.9 million employers.

Now, there are ways to manage that. You can phase it in, or you could enroll certain industries first, perhaps those involving critical infrastructure. That is what it would take.

Mr. JOHNSON. I am over my time. Thank you, Mr. Chairman.

Chairman MCNULTY. Thank you, Mr. Johnson.

Mr. Levin may inquire.

Mr. LEVIN. So, what would be the cost of what you just read?

Mr. STANA. What USCIS estimated for the first year of operation, I believe, was $70 million in management costs and about $300 to $400 million for compliance and investigative staff. That doesn't include computer upgrades that would be necessary. It doesn't include ICE investigators that follow up on any leads of employer abuse of employees or misuse. It is going to be substantial.

Now, having said that, any immigration expert would probably tell you that of the handful of things that are must-haves in an immigration reform proposal, this would be one of them. So, it is probably more a question of what type of a verification program you have, not whether you would have one.

Mr. LEVIN. I think the Senate is going to be acting. They may act this week. And the odds seem to be that they are going to pass a bill. And so the odds are that we are going to need to address this in the House. And so we need to begin to prepare for the possibility, if not the probability.

To pick up what the Chairman said, who is doing the hard work of itemizing the costs of this? Who is doing that?

Mr. STRECKEWALD. In Social Security, we have a budget shop that works with the systems people and the programs people, and our field office people, everybody that has a role in this. They have a process they go through for any new workload. They try to budget it and figure what the total cost would be. They are just now revising those figures, so we don't have them here today. We will be happy to, again, submit them when they are available.

Mr. LEVIN. When is that going to be?

Mr. STRECKEWALD. When is that going to be?

Mr. LEVIN. More or less?

Mr. STRECKEWALD. More or less, it should be shortly. I don't know exactly when, but in the next few weeks or shorter, I would guess.

Mr. LEVIN. No. I think if it is a few weeks, it will be before we pass the bill.

Mr. STRECKEWALD. What has been very helpful to us in getting ready for this has been the expansion of the system that DHS and SSA have partnered in. DHS is registering more employers onto the system, which means we both have to build greater capacity, and we have to make sure our business processes are sound, and we have to move forward on building additional functionality into the system.

So, that is in essence preparing us for great expansion, just by preparing for moderate expansion.

Mr. LEVIN. Yes, but there is a cost to that, too. Right?

Mr. STRECKEWALD. Yes, there is. We have a reimbursable agreement that we have developed between DHS and SSA that is not yet signed, but at this point I think it is with the lawyers from each agency, looking to make sure everything is right from their agency's perspective.

Mr. LEVIN. And it has a cost estimate?

Mr. STRECKEWALD. It has a cost estimate in there for this year. It is based upon——

Mr. LEVIN. When you say for this year, you mean——

Mr. STRECKEWALD. 2007.

Mr. LEVIN. This fiscal year?

Mr. STRECKEWALD. Right.

Mr. LEVIN. And who is making the projection for next fiscal year?

Mr. STRECKEWALD. Well, that is the budget shop that I was talking about a little bit earlier. They are waiting to see what the exact elements of a bill will be, and then they will plug in those provisions and do the math and come up with an estimate.

Mr. LEVIN. So, you would expect that there will be available to the Congress within the next short period a detailed itemization of what this would cost, assuming there is complete coverage. What kind of timeline is being assumed, and which bill?

Mr. STRECKEWALD. For getting it implemented, from our perspective? I think the timeline—the ramp-up approach—that is in the current bill is probably sufficient for us. It kind of starts slowly, then builds up.

Mr. LEVIN. When you say the current bill, you mean?

Mr. STRECKEWALD. The Senate bill.

Mr. LEVIN. The Senate bill.

Mr. STRECKEWALD. It starts over a several-year period, starts with critical infrastructure, moves to new hires, and then moves to everybody, your whole payroll. So, that allows us—as long as we get the money early in the fiscal year—it allows us to hire, train, and equip new employees to deal with the increased business and increased workload.

As that ramps up, so will our efforts to hire, train, and equip new employees. So, we think that that is very doable with the appropriate funding at the beginning of each year.

Mr. LEVIN. The appropriate funding is going to be major, is it not?

Mr. STRECKEWALD. Well, as I mentioned, in the neighborhood, if you will, without giving any specific figures yet because they are not done with our estimates, it could be in the peak years as much as 2 to 3,000 work years or, as I say, people, extra people, new hires, and up to $300 million a year during the peak years. So, that is significant for us.

Mr. LEVIN. Two to 3,000? That is included in the figure you gave?

Mr. STRECKEWALD. Yes. I tried to convert it to millions of dollars. Basically—the major cost of that is people.

Mr. LEVIN. As I close, Mr. Chairman, I think that underlines the need for this Congress and the Administration to face up to the additional costs, because we do not want it to deter the effort to get hold of the disability issue. You are going to be very blunt and direct about what is needed, right?

Mr. STRECKEWALD. We are going to have our estimates shortly, and I will make sure that everybody is aware of them.

Mr. LEVIN. Thank you.

Chairman MCNULTY. Mr. Streckewald, what about the old estimate I saw here of the agency estimating that it would cost approximately $10 billion to issue these new cards?

Mr. STRECKEWALD. That estimate——

Chairman MCNULTY. That estimate is in the budget of Social Security.

Mr. STRECKEWALD. Yes. We were talking about a different process here. If we are talking about issuing new cards—I think the $10 billion was reference to new cards——

Chairman MCNULTY. Right.

Mr. STRECKEWALD [continuing]. What we had been talking about was the fallout from the employer verification system. If we go to issuing new cards to all new workers of all people in the United States over 14 years of age. Yes, that figure is still approximately right. If you did it over 2 years or 5 years, it is going to take about $10 billion to issue new cards to most of the people in the United States. I don't think it is much different today. It might be a little higher today than when that was estimated a year ago.

Chairman MCNULTY. And I would again state for the record that is more than the entire SSA operating budget right now.

Mr. STRECKEWALD. That is right.

Chairman MCNULTY. Mr. Lewis may inquire.

Mr. LEWIS. Thank you, Mr. Chairman.

I just want to go back to the privacy issue just for a minute here. Mr. Schaeffer, your office supports data sharing and disclosure restrictions between the Social Security Administration and the Department of Homeland Security. At the same time, I am sure you would agree that the importance of protecting the privacy of taxpayers is important.

So, what information should be shared with the Department of Homeland Security?

Mr. SCHAEFFER. Well, currently there is a limit on the information that we can share because of IRS rules and regulations. Some of the information that may be useful to share if you really want to get a handle on people working in the country illegally would be to focus on the employers that consistently have a large number of items going into the earnings suspense file, which means that the name and the Social Security number could not match up within SSA's records to a legitimate number holder; and then have the appropriate enforcement action take place.

It is really difficult to try to go after the individuals because you are really talking about millions of items that are going into the ESF. So, the number of employers are much more finite, and that is where it starts with. These employers are giving individuals a job where their name and Social Security number do not match up to SSA's records.

Mr. LEWIS. Mr. Stana, would you like to comment?

Mr. STANA. You know, I would be a little cautious about sharing a lot of data quickly with DHS if I were in SSA's shoes. The reasons are that, first, we haven't had the full certification testing of the databases, and we'd just want to make sure that they are in good shape security-wise.

Second, the data that has been available to DHS in the past, hasn't been used. So, why would you want to release a lot of information that they are not likely to use? Certainly SSA would want to, on a case by case basis, at least, start out and to DHS say, what is most useful to you, how can we help you, and let's limit it to that initially.

Once, DHS ramps up its compliance units, maybe there will be opportunities for more broadly sharing information. I think the kind of information that would be most useful to them, knowing how their worksite and employer/employee compliance efforts work, the kind of information that would be most useful would be information dealing with Social Security numbers over time that keep being used again and again by workers or employers.

Information about patterns over 10 years of noncompliance might be in the earnings suspense file, maybe in other documents or databases. I would be very carefully initially about opening it up wholesale until we really had a better sense of what is useful.

Mr. LEWIS. Very good. Thank you.

Chairman MCNULTY. Thank you.

Mr. Becerra may inquire.

Mr. BECERRA. Thank you, Mr. Chairman. Thank you to all of you for your testimony. And Mr. Chairman, thank you for this timely hearing. I think it is important for us to move on this as quickly as we can in the event there is comprehensive immigration reform.

Gentlemen, let me ask a question, and first focus on the cost of the current EEVS system. I suspect I should probably first ask Mr. Streckewald this: How much did the EEVS system cost the SSA to administer or to conduct last year, in 2006?

Mr. STRECKEWALD. It cost us $891,000.

Mr. BECERRA. Under an agreement you have with DHS, Homeland Security, you are to be reimbursed for those costs of doing those inquiries?

Mr. STRECKEWALD. Yes.
Mr. BECERRA. Have you yet been reimbursed?
Mr. STRECKEWALD. No. Not for that money.
Mr. BECERRA. Are you expecting to be reimbursed?
Mr. STRECKEWALD. We hope to be reimbursed.
[Laughter.]
Mr. STRECKEWALD. I assume our lawyers are still working to resolve it, but that is almost a million dollars. That is a lot of money. Actually, it is a million if you count a little bit of money left over from 2005 that they weren't able to pay us. So, approximately a million dollars, and to us every million counts. So, we do hope to get that money reimbursed.
Mr. BECERRA. You mentioned a scary word, lawyers. Is there a reason why a Federal Government agency, SSA, is having to employ its lawyers to talk to another Federal Government agency, the Department of Homeland Security, when it has an agreement, a document, that says that it is to be reimbursed?
Mr. STRECKEWALD. I can't speak to that. I know that DHS felt that it didn't get the funding in order to be able to reimburse us, and we said, well, we are doing work here. So there has been a friendly, so far, exchange of arguments. I hope that it does get resolved where we are reimbursed for the money. I don't disagree with the point you are making.
Mr. BECERRA. Mr. Chairman, we may want to inquire of DHS when we have that opportunity.
My understanding is, and you can correct me, Mr. Streckewald, if I am wrong, but that for every million dollars, you could conduct some 565 additional disability hearings to help reduce that backlog of over 1.3 million cases of Americans waiting to have their disability claim processed through SSA.
Mr. STRECKEWALD. That is true.
Mr. BECERRA. So for every million dollars that DHS doesn't reimburse you, under which they have an agreement to do so, then you have to either cut back on services or allow those individuals to wait even longer as they wait for their hearing to determine if they should be receiving disability benefits.
Mr. STRECKEWALD. You are right.
Mr. BECERRA. How much have you spent so far to date doing the inquiries that are required under the EEVS system, the employment verification system, for DHS?
Mr. STRECKEWALD. This year?
Mr. BECERRA. Yes.
Mr. STRECKEWALD. We have had 1.8 million inquiries, or queries. So, what we are doing is setting up a reimbursable agreement for the rest of the year because this was——
Mr. BECERRA. If you could try to just give me the answer. I apologize. It is just that I am going to run out of time. How much do you estimate you have spent to date conducting EEVS services for DHS?
Mr. STRECKEWALD. Well, I think it would be in the neighborhood of $2 million that SSA has not been reimbursed because last year it was nearly a million. This year, so far, we are about the pace of last year. So, approximately $2 million. We could probably submit the exact number for the record. [INSERT]

Mr. BECERRA. Could you do that? My understanding from some of the information we received from Committee staff was that it was now exceeding $5 million.

Mr. STRECKEWALD. $5.9 million is the amount for all of FY 2007. We have a reimbursable agreement that we are working on with DHS. They say they are going to sign it and that they have the money this year. So, for FY 2007, it is about $5.9 million, and that would cover us.

Mr. BECERRA. I see. So, that is the projection for the entire year 2007?

Mr. STRECKEWALD. Yes. Yes.

Mr. BECERRA. Maybe we can help because I think it is outrageous that you are conducting a service that is outside the core mission of your work for an agency under which you have an agreement to do this, which is essential work, yet you are having to underfund your programs that are helping lots of Americans who are in desperate need in some cases of this assistance.

So, perhaps, Mr. Chairman, we can try to lend a hand to SSA to try to get reimbursed for the monies it is due for the work that it is done.

Let me ask a question with regard to error rates. I know this has always been an issue with regard to the SSA and the Social Security card because the Social Security number was never meant to be a data-confirming number other than for purposes of Social Security benefits.

Tell me when I am wrong. I understand from an inspector general report that was done back in December 2006—and Mr. Schaeffer, please tell me if I am incorrect on this—I understand that there are about 17.8 million employees who are erroneously categorized as nonconfirmed in these checks that are done simply as a result of discrepancies that are related to their name, birth date, or citizenship status.

So, if someone gets married, the current file doesn't reflect that that individual has changed his or her her name as a result of marriage. There are 17.8 million employees who don't check out. That is about 4.1 percent.

Mr. SCHAEFFER. That is basically correct. I wouldn't say they are all employees. That is of the active Social Security numbers in SSA's database, which theoretically they all could be employees, but they all may not be employees.

Mr. BECERRA. Thank you for that correction. There are approximately about 5 million new hires per month in this country, more or less?

Mr. SCHAEFFER. Right.

Mr. BECERRA. So, if you take that 4 percent error rate and apply it to the 5 million or so new hires that occur every year, and you are talking about somewhere close to—or over 200,000 Americans on a monthly basis, about 2.5 million people on a yearly basis, who could, based on discrepancies, be misidentified as not eligible to work using the current Social Security database with its current list of errors. Have I said anything wrong here?

Mr. SCHAEFFER. No. That is theoretically possible. One would hope that things would get better over time.

Mr. BECERRA. And, of course the error rate is higher, my understanding is, for foreign-born U.S. citizens. So, if you happen to be born in another country but you have citizenship by birthright, by your parentage, or for individuals who have come to this country and have since become citizens, the error rates are even higher for them.

Mr. SCHAEFFER. That is correct.

Mr. BECERRA. Mr. Streckewald, you wanted to say something?

Mr. STRECKEWALD. Yes. I don't disagree with your figures. I would maybe just clarify by saying that it is tentative nonconfirmation. You are right, they are going to be told tentatively it looks like you don't have authorization to work. They come in to us, we straighten it out, and then they are authorized to work.

So, it is not pleasant to have to do that, but it gets updated and they get to work.

Mr. BECERRA. Mr. Chairman, I know my time has expired so I won't ask any more questions other than to just make the following point. My understanding is that your field offices serve some 42 million visitors a year. You have lost—Social Security Administration has lost—some 2,400 positions in the past 19 months, and you are at your lowest staffing level now that you have been since the 1970s.

Your processing time in most cases in most offices takes over 900 days. You requested a budget of President Bush totaling $10.4 billion. The President's budget allotted Social Security Administration $9.6 million. That is an $800 million loss right there.

With all of these tasks that are placed upon you and with the burdens fiscally that you have, Mr. Chairman, I think it becomes very obvious that we have to really examine this and try to help make sure that SSA not only gets reimbursed from DHS for money that it is due, but also that we get the resources to the agency to make sure that if we do move forward on immigration reform, they are able to do this, and not at the expense of Social Security applicants for disability benefits or Social Security benefits.

Thank you.

Chairman MCNULTY. Mr. Ryan may inquire.

Mr. RYAN. Thank you. First of all, Mr. Chairman, I want to thank you for having this hearing. Very good timing on this. We need to do this.

As I look at this and I see this immigration bill most likely passing the Senate, it seems, and probably next week, is what we hear, and then coming our way, we really have to get our hands around this. I think most Members of Congress believe we need comprehensive immigration reform.

Then when you look at comprehensive immigration reform, most people conclude a central premise of that is an airtight worker verification system. So, we all kind of agree that that is necessary.

Then when we look at this system, the word fiasco comes to my mind, to be honest with you. I guess here is the couple questions I want to ask. Number one, do you really believe we could get this thing up and running in 18 months and have a minuscule error rate? Do you really believe that?

Mr. STRECKEWALD. From Social Security's perspective, I think we will. Again, the funding is critical, but we have risen to challenges that we have been faced with. We will get it done.

I can't speak to what the error rate will be, but right now it is at about three contacts for every hundred queries. We would like to get that down, but it is unknown in the future what that will be if all employees must go through the system. We can get it done with the proper funding.

Mr. RYAN. Then what pieces of personal information does Homeland Security think they are going to need at the end of the day to make this work?

Mr. STANA. First, if I might address the question this way.

Mr. RYAN. Sure. I would appreciate that.

Mr. STANA. To say the least, this is going to be a tremendous challenge. You are talking about signing up 30,000 employers per day from now until December 2008. What if employers wait until fall 2008 to enroll? Then there's the need to hire staff. Do background checks. Get office space. Procure new computer equipment. You never say never, and something will probably be available in December 2008. Is it going to be something that 5.9 million employers can use? It is going to be a challenge for DHS.

Now, your other question was dealing with the——

Mr. RYAN. The pieces of information, all the pieces you think they need.

Mr. STANA. The information that goes to Social Security for EEVS, I believe, are name, Social Security number, and date of birth. That is what goes, and it is checked against the Numident database. The information for checking against DHS databases include the name and the A number, alien number, or the employment authorization number. That is the extent of the information used. They get either a confirm or nonconfirm.

Mr. RYAN. The goal of the system is twofold. Right? You are who you say you are, and you are eligible to work in this country.

Mr. STANA. Also you are work-authorized.

Mr. RYAN. Right?

Mr. STANA. Yes.

Mr. RYAN. Have you ever considered the idea of maybe having a private-based identity system for identifying who you are, and then referencing the Social Security database to see if you are eligible to work or not? Have you ever considered those kinds of ideas, those kinds of systems?

Mr. STANA. GAO hasn't seen those kinds of things being seriously considered. I have heard discussions of using other means. Mr. Johnson mentioned, swiping a credit card, and why can't you get the verification done quicker?

Mr. RYAN. Yes. Right.

Mr. STANA. I have heard of using private sector facilities like credit card terminals but one of the stoppers, frankly, is getting the right equipment out to the employers to use for this quick verification. Right now it just requires a computer and Internet access. If you want to do something more with biometrics, it may require something more sophisticated. I have heard the "credit card" solution tossed around, but not seriously considered.

Mr. RYAN. So, $370 million is the number I just heard when I added up all that you said you think you need, Mr. Streckewald. So, $370 million I am taking as sort of the minimum up-front cost annually to get a system like this going. You are going to give us——

Mr. STRECKEWALD. We don't have the exact figures yet, but——

Mr. RYAN. But you are going to give us a budget estimate in about three or four weeks, you told Mr. Levin?

Mr. STRECKEWALD. I hope to be able to. We will get it to you as soon as it is done.

Mr. RYAN. So, that number will probably go up to half a billion?

Mr. STRECKEWALD. That was the figure for DHS. Three to $400 million for compliance staff, and another $70 million for program management. So, it could be $370 to $470 million.

Mr. RYAN. By the end of our terms, we are going to be—I don't see a clock so I don't know what my time is—but by the end of our terms here, by 18 months, we are expecting every employer to verify every—actually, it is a four-year staggered process. Correct? So, can you walk me through that? I am not precisely familiar with the Senate bill, but it is—how do they roll in who all is checked?

Mr. STRECKEWALD. If I recall——

Mr. STANA. I have got that.

Mr. STRECKEWALD. Why don't you go ahead. It does ramp up.

Mr. STANA. There are two——

Mr. RYAN. What is the ramp-up?

Mr. STANA. Gutierrez-Flake is a different version, but I can give you both, if you like. The Senate version is in six months you want all new employees hired after the act is passed in critical infrastructure and government to be verified. By 18 months, you want new employees in all sectors to be verified. After three years, you want all employees, old and new to be verified. That is the Senate proposal.

Mr. RYAN. Three years? Okay.

Mr. STANA. On the Gutierrez-Flake proposal, the STRIVE Act, it is in year one, all employees working in critical infrastructure are to be verified. In year two, all large firms with 5,000 or more employees would have their employees verified. In the third year, mid-size firms would be added. In the fourth year, employees in small firms would be verified. Those criteria could probably be adjusted if need be.

This gets to the stress that is put on the field offices. It depends on how you manage EEVS implementation. Once an employee's data is validated in NUMIDENT, he or she is probably not going to get nonconfirms when seeking employment in the future unless there is a name change due to marriage, for example.

Mr. RYAN. Well, I would simply just say, Mr. Chairman, I think we owe it to our constituents, our colleagues, and our country to try and fix this or figure this out if this train is really coming on the rails as fast as it looks like it might be.

I would like to look into the possibility of not necessarily having a centralized database but a decentralized database, where we can use some of the ingenuity that is going out there in the private sector.

So, with that, I yield. Thanks.

Chairman MCNULTY. Ms. Tubbs Jones may inquire.

Ms. TUBBS JONES. Thank you, Mr. Chairman. Gentlemen, I apologize for being late. In Congress they give us lots of things to do.

I want to speak to Mr. Streckewald. You are real optimistic. You oversee the disability and income security programs. Do you know how many people there are in America that are waiting for a disability determination? We haven't fixed that yet, to then give you a greater responsibility of doing an employment verification system.

How many people do you need to fix that part before you do employment verification?

Mr. STRECKEWALD. Well, we are still looking at what approach will work best. My understanding, we have come up with a multi-faceted approach that not only looks at the old cases to try to get them out and get decisions on them, but also tries to sort through the new ones so that they don't become the old cases. So, I think the Commissioner is coming out with a plan shortly on that.

Ms. TUBBS JONES. Then we are trying to figure out how we hire the employees to do the work that needs to be done. The issue was that there is a 10-year-old list of hearing officers and we have to hire some new ones.

So, in employment verification, it is likely there is going to be a list, that we have to put the list together to hire the people from the list, and on and on and on? Come on. Be real with us. I know the Administration is saying what you can do, but the reality is that this is not going to happen. I know you don't want to say it. I am going to say it for you. This ain't going to happen.

[Laughter.]

Mr. STRECKEWALD. We like to think with proper funding, this particular business process is doable. I apologize for seeming overly optimistic.

Ms. TUBBS JONES. You know, that is what we heard about—and I am not pointing individually at you or any of your colleagues at the table. Realism has to set in somewhere in this process so that there is not an anticipation by the people of America that we can do what people are talking about doing within 18 months.

I am more of a person that would say I love individual ingenuity, and privatization is something that could happen, but I also like people having jobs that are guaranteed and secure. There are people who would love to come and work at the Government till and have an opportunity to pursue this.

So, I would like to encourage you to figure out, if everybody else is doing it, why can't the Federal Government do it? Why can't we come up with a system by which we can do the work of employment verification?

I could ask a lot of questions, but the bottom line for me is, tell me the truth. Don't—and I am not saying you are lying—don't misunderstand me, but don't make me anticipate more than I am really going to get.

Mr. Chairman, Ranking Member, thank you so much for the opportunity to ask the questions. I am running. Thanks.

Chairman MCNULTY. The Ranking Member has an additional question.

Mr. JOHNSON. Mr. Schaeffer and Mr. Stana, I would like to ask you this one question: Is it possible to achieve a tamper-proof, fraud-resistant ID card?

Mr. STANA. Is it possible?

Mr. JOHNSON. Yes. I want to listen to him first.

Mr. SCHAEFFER. I would say anything is possible. However, the probability of achieving that, I think, would be very difficult. Most things that happen in that, once the card is out there and the people that want to circumvent that, once they start reverse engineering, almost always they develop the ability to do so.

So, you may have a tamper-proof card today and it may last for a period of time. It may not be—to me, the probability that the tamper-proof card that you develop today, for it lasting forever, I would say a very small probability, that you would have to continually be revising that card, with the associated cost associated with it, to have to stay one step ahead of those who would be looking at a way to defeat it.

Mr. JOHNSON. Mr. Stana?

Mr. STANA. I would say it is possible. If you put the right security features on an identity card, it might be useful for some time. Those security features would be mainly biometric—retina scans, enhanced fingerprints, other digital information.

I would also note for this purpose of verifying that the person who is sitting in front of you, if you are the employer—is the individual who they say they are—would probably require some expensive equipment for employers to maintain. So, that is the other aspect of it.

There are secure cards that are used to verify identity in top secret locations, and I suppose you could use those kinds of cards. I agree with my friend here that it is a matter of time before secure cards and systems get hacked. You would have to probably renew a card periodically to keep it reliable and secure.

Mr. JOHNSON. Thank you, Mr. Chairman.

Chairman MCNULTY. I thank all of the members of the panel. Members may have additional questions that they want to submit to you in writing, and I would ask that you would reply to them. I would ask you to respond to some staff inquiries that we may have as a result of your testimony at the hearing today, too.

Mr. Streckewald mentioned that the Social Security Administration has risen to past challenges. I believe he is correct, when—and you had that big qualifier there—when the proper resources are made available.

So that is a big qualifier on this whole issue. I would submit to you that the resources have not been made available with regard to the disability backlog. That is why that is an unmitigated disaster.

There is no reason why a citizen of the United States of America should come to the Social Security agency or to a Member of Congress with an application for benefits, and be told, we will get back to you in a year and a half or two years.

That is a disgrace. That is because you don't have the proper resources to do that. So, before we embark on any new big expanded

program, one of my main concerns is going to be to make sure that if we do this, that we do have the proper resources.

We thank all the members of the panel. We will now hear from panel two.

[Pause.]

Chairman MCNULTY. We thank all of the panel members for being here. Let me just begin by introducing the panel members.

Tyler Moran, Employment Policy Director of the National Immigration Law Center.

Angelo Amador, Director of Immigration Policy, U.S. Chamber of Commerce.

Sue Meisinger, President and CEO, Society for Human Resource Management, on behalf of the Human Resource Initiative for Illegal Workforce.

Peter Neumann, Principal Scientist, SRI International, on behalf of U.S. Public Policy Committee of the Association for Computing Machinery.

Marc Rotenberg, Executive Director, Electronic Privacy Information Center.

So, we thank all of you for being here. Your entire testimony will be included in the official record. We ask that you summarize your comments to stay within 5 minutes. You see the little prompter in front of you; when the amber light comes on, we ask you to try to wrap up and conclude when the red light appears.

Again, we thank you for taking time out of your busy schedules to help us address this issue. We will start with Ms. Moran.

STATEMENT OF TYLER MORAN, EMPLOYMENT POLICY DIRECTOR, NATIONAL IMMIGRATION LAW CENTER, BOISE, IDAHO

Ms. MORAN. Good morning, Chairman and Mr. Johnson, Members of the Committee. Thank you for the opportunity to allow me to address the critical issue of EEVS, or EEVS. This issue has not received the attention it deserves, and so it is critical that this Committee is holding a hearing today.

My name is Tyler Moran. I am the Employment Policy Director for the National Immigration Law Center. NILC is a nonpartisan national legal advocacy organization that works to promote and advance the rights of low-income immigrants and their families.

NILC has tracked the Basic Pilot Program since it was implemented in 1997, and we have extensive experience assisting immigrant advocates in responding to problems with the program, including the way in which it has been used to adversely affect workers.

Because of this experience, we do not support a mandatory EEVS. However, because it enjoys almost universal support in Congress, we want to work with you all to ensure that a system is implemented that is accurate and that avoids negative consequences for workers, both U.S.-born and immigrant.

While the focus of the Basic Pilot and the immigration reform debate has largely focused on DHS, as you heard this morning, SSA plays an integral role in its functionality. If it were to become mandatory, SSA would have to process 60 million queries per year versus the 1.8 it currently does.

So, a number of studies have found that the Basic Pilot Program has significant weaknesses, including its reliance on government databases that have unacceptably high error rates, and employer misuse of the program to take adverse action against workers. The significant weaknesses that exist in the current program, which serves approximately 17,000 employers, would be greatly exacerbated if the program were to surge to over six million.

Improvements to the Basic Pilot have been made in the past 10 years, but they are not sufficient enough for a mandatory program that, because of database errors, could take away people's livelihood. Additionally, if the current flaws are not addressed before it is made mandatory, it could lead to noncompliance, which would result in certain businesses and workers moving into the underground, unregulated cash economy, which could result in billion-dollar losses in Federal, state, and local tax revenues. A similar situation would occur if an EEVS were to be implemented outside the context of comprehensive immigration reform.

So, the database errors: As you heard this morning, we have got a 4.1 percent error rate. The error rate affects all workers, but it disproportionately affects immigrants. The impact is the most on foreign-born naturalized citizens.

Most people don't know when you naturalize to tell SSA that they changed their status. So, there are over three million records that have incorrect information on those folks. So they are going to have to go into SSA field offices to correct the information. So, the burden on your constituents could be enormous.

When workers receive a tentative nonconfirmation, they can't call the SSA field office. They actually have to physically go into the SSA field office. Right now, one-third of people simply applying for an SSN have to go back to the office with additional documentation. They have to make two trips.

From testimony from the National Council of Social Security Management Associations, wait times in field offices are running 2 to 3 hours, with some over 4 hours. So, if you think you are getting calls on disability right now, just wait until this is implemented.

So, the independent evaluation also found that employers misuse the Basic Pilot. For example, the law requires that you first extend a job offer and then you put the person's information through the system. In violation of this requirement, 42 percent of employers put workers through Basic Pilot before extending a job offer.

Why is this a problem? It is a problem because, because of these high error rates, most people who get tentative nonconfirmations are actually authorized to work. So, if they are not hired because of a tentative nonconfirmation, they never know that there is a problem, they are never hired, and then they can't go and fix the database errors. It might happen again at their next job.

Employers also penalize workers who receive tentative nonconfirmations, and 45 percent of employers subject people to pay cuts, delays in job training, and other restrictions on working.

So, what do we need to do to have a workable system? First, I want to start out and say the STRIVE Act in the House is what we consider the best effort at addressing an EEVS in a meaningful and thoughtful way. I do want to mention, too, that there is an independent evaluation commissioned by USCIS that has not been

released to the public, and I would urge you all to get a copy of that report before you move forward. It is by the Westat Corporation.

So, one, we need to phase in the system at a reasonable rate, and we need to have objective benchmarks. So, SSA and DHS have to prove to us they can meet certain levels of database accuracy, privacy, employer compliance with the system, and low error rates before the system is implemented. It is simple: Prove the system works before you implement it.

Two, include meaningful due process protections because for the first time in the history of this country, your constituents are going to have to ask the Federal Government for permission to work. If they are wrongly denied, they are going to be mad, and there should be a way for them to correct those errors.

Last, include workable documentation requirements that do not require a real ID license or a hardened SSN card, neither of which exist. Fifteen states thus far have said they will not implement the REAL ID Act.

Last, I forgot, strong anti-discrimination protections that prohibit employers from misusing the EEVS to penalize workers.

So, I just want to conclude by saying the House of Representatives is going to move forward on a immigration bill after the Senate finishes up this week. It is critical that it be guided by the lessons learned of the last 10 years of Basic Pilot. Since so much of the focus is on DHS, it will be critical for this Committee to work with the Judiciary Committee to help inform them about the impact of the system on SSA, and what resources will be needed to fix those database errors, and also how the agency can work with DHS to make sure that employers are following the rules and not taking adverse action against workers.

So, I would be happy to answer any questions, particularly about any of the proposals before Congress right now.

[The prepared statement of Ms. Moran follows:]

Prepared Statement of Tyler Moran, Employment Policy Director, National Immigration Law Center, Boise, Idaho

Members of the Committee, thank you for the opportunity to address the critical issue of current and proposed electronic employment verification systems (EEVS). My name is Tyler Moran, and I am the Employment 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 national advocacy groups, policymakers, attorneys and legal aid groups, workers' rights advocates, labor unions, government agencies, and the media.

Overview

My testimony today will focus on (1) the limitations of the current electronic employment verification system—the Basic Pilot program—upon which most proposed EEVS are based; (2) a summary of the impact of a flawed EEVS on the Social Security Administration (SSA) and on foreign-born workers; (3) an explanation of what provisions must be included in any mandatory EEVS; and (4) an analysis of the EEVS proposed in the 2007 House and Senate comprehensive immigration reform bills.

NILC has tracked the Basic Pilot program since it was implemented in 1997 and has extensive experience assisting immigrant advocates, attorneys, unions and other worker advocates in responding to problems with the program, including the way in which it has adversely affected workers. Because of this experience, we do not support expansion of a mandatory EEVS. However, because the concept enjoys almost universal support in Congress, and therefore will almost certainly be incorporated into any comprehensive immigration reform bill, we want to ensure that any proposed system be designed so as to avoid negative consequences for workers—both immigrant and U.S.-born.

While the focus of Basic Pilot has largely been on the Department of Homeland Security (DHS) and its agency that administers the program—the U.S. Citizenship and Immigration Services (USCIS)—the SSA also plays an integral role in ensuring its functionality. In fact, SSA 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 the Basic Pilot. If Basic Pilot were to become mandatory (and apply only to new hires), this would mean that SSA would need to process 50–60 million queries per year, versus the 1.8 million queries that the agency processed in 2006.[1]

It is therefore essential that this Committee understand what it will take to create a system that functions with a high level of data accuracy, is properly monitored, and does not unintentionally promote employment discrimination. If implemented using the existing technology, procedures, and databases, the financial costs would be high and the inaccurate results would have a human cost borne by U.S.-born and immigrant workers. In addition, an expanded system would result in dangerous privacy breaches and increased discrimination against individuals who look or sound foreign.

The Social Security Administration's Role in the Basic Pilot Program

The Basic Pilot Program is an Internet-based program that allows employers to electronically verify new workers' employment eligibility by directly checking the records maintained by SSA and DHS. The program is one of the three pilots created by the Illegal Immigration Reform and Immigrant Responsibility Act of 1996, which began operating in six states in 1997. The other two pilot programs were discontinued. However, in December 2004 Congress extended the Basic Pilot to all 50 states, and it is now available to employers who voluntarily choose to participate in the program, although certain employers who have been found to unlawfully hire unauthorized workers or who have discriminated against workers on the basis of national origin or citizenship status may be required to participate. According to DHS, 16,000 employers are currently enrolled in the program.[2]

How the Verification Process Works at SSA[3]

Before employers can use the Basic Pilot program, they must first sign a memorandum of understanding (MOU), which sets forth the points of agreement between SSA, DHS, and the employer regarding the employer's participation in the program. Employers must also complete an online training and display a notice at the workplace from DHS indicating the employer's participation in the program, and an anti-discrimination notice from the Office of Special Council for Immigration-Related Unfair Employment Practices, Department of Justice.

1. Step 1: Employer completes I–9 form.

Employers participating in the Basic Pilot must still complete an I–9 employment eligibility verification form for each new employee hired as is required of all employers, but with one change to those procedures: Basic Pilot employers can accept a document as proof of a worker's identity only if the document includes a photograph. It is still the employee's choice, however, which documents to present to establish identity and employment eligibility.

---

[1] According to former Commissioner Barnhart, SSA averaged 150,000 queries per month in 2006. *See* Jo Anne B. Barnhart, Testimony before the House Committee on Ways and Means (Social Security Administration, July 26, 2006), http://waysandmeans.house.gov/hearings.asp?formmode=printfriendly&id=5172.

[2] Jock Scharfen, Testimony before the Subcommittee on Immigration, Citizenship, Refugees, Border Security, and International Law, Committee on the Judiciary, U.S. House of Representatives: Problems in The Current Employment Verification and Worksite Enforcement System (USCIS, U.S. Dept. of Homeland Security, April 24, 2007), http://judiciary.house.gov/media/pdfs/Scharfen070424.pdf.

[3] For more information on the entire Basic Pilot process, see Basic Information Brief: DHS Basic Pilot Program (National Immigration Law Center, March 2007), www.nilc.org/immsemplymnt/ircaempverif/basicpilot_infobrief_brief_2007-03-21.pdf.

2. Step 2: Employer verifies identity and employment eligibility using the Basic Pilot.

For each newly hired worker, the employer must enter the worker's information provided on the I–9 form—such as name, SSN, and citizenship status or alien number—into a form on the Basic Pilot website within three days of the worker's hire date. If a worker has not yet been assigned an SSN (as can be the case with newly-arrived immigrants), however, the employer has to wait to enter that person's information into the Basic Pilot form *after* the SSN is obtained. This procedure is in conflict with the requirements outlined in the MOU stating that the employer will put the worker's information into the Basic Pilot within three days of hire. There continue to be delays in issuing SSNs at field offices—delays that can last for months. According to the American Immigration Lawyers Association, some of the delays arise from "front desk" errors, where an application is rejected for lack of a document that is not required.[4]

The information that is entered on the Basic Pilot website is first checked against information contained in SSA's database, the Numerical Identification File ("Numident"). SSA verifies that the name, SSN, and date of birth are correct, regardless of the worker's immigration status. SSA also confirms whether, if the employee has stated that he or she is a U.S. citizen, this is in fact the case; if it is, this establishes that the employee is employment-eligible. In the cases of naturalized citizens, however, SSA is sometimes unable to confirm their U.S. citizenship and must forward the inquiry to USCIS.

For any non-U.S. citizen employee, USCIS verifies that the worker currently has employment-authorization. If the information provided by the worker matches the information in the SSA and USCIS records, the employer will receive a "confirmation" and no further action will generally be required, and the worker may continue employment.

If SSA is unable to verify information presented by the worker, the employer will receive an "SSA tentative nonconfirmation" notice. Employers can receive an SSA tentative nonconfirmation notice for a variety of reasons, including lags in data entry in SSA's database, inaccurate entry of information into the form on the Basic Pilot website, or name changes or changes in immigration status that are not reflected in SSA's database. An SSA tentative nonconfirmation is also issued when the person attests to being a U.S. citizen but SSA records indicate that the person is a noncitizen with unknown work-authorization status. For example, a foreign-born U.S. citizen may have naturalized, but if the person does not inform SSA of this fact, SSA records will reflect his or her former immigration status.

3. Step 3: Employee can challenge a "tentative nonconfirmation."

If the individual's information initially does not match SSA's records, the employer must first double-check that the information was entered correctly into the system. If the employer did not make an error, the employer must give the employee written notice of that fact, called a "Notice to Employee of Tentative Nonconfirmation." The worker must then check a box on the notice stating that he/she contests or does not contest the tentative nonconfirmation notice, and both the worker and employer must sign the notice. If the worker chooses to contest the tentative nonconfirmation notice, the employer must print a second notice, called a "Referral Letter," which contains information about resolving the tentative nonconfirmation notice, as well as the contact information for SSA. The worker then has eight Federal Government work days to visit an SSA office to try to resolve the discrepancy. SSA then has 10 Federal Government work days after the worker receives the referral notice to resolve the case.

Under the MOU, if the worker contacts SSA (or USCIS) to resolve the tentative nonconfirmation, the employer is prohibited from terminating or otherwise taking adverse action against the worker while he/she awaits a final resolution from the Government agency—even if it takes more than 10 Federal Government work days for SSA to resolve the matter. In the case of an SSA tentative nonconfirmation notice, the employer must wait 24 hours after the worker visits SSA to resubmit the inquiry to the Basic Pilot program, and no later than 10 Federal Government work days after the date that the worker was referred to SSA. If the worker does *not* contest the tentative nonconfirmation notice, it automatically becomes a "final nonconfirmation" and the employer is required to fire the worker.

---

[4] Minutes of the Social Security Administration and CIS AILA Liaison Meeting on SSA Related Issues (American Immigration Lawyers Association, May 8, 2006).

Concerns about Expanding the Basic Pilot Program

Numerous entities, including those that researched and wrote an independent report commissioned by the former Immigration and Naturalization Service, the Government Accountability Office, and the Social Security Administration's Office of the Inspector General (SSA–OIG), have found that the Basic Pilot program has significant weaknesses, including (1) its reliance on government databases that have unacceptably high error rates and (2) employer misuse of the program to take adverse action against workers.[5] It is our understanding that the research corporation, Westat, has recently concluded another evaluation of the Basic Pilot for USCIS, though the results of that study have yet to be released to the public. It is critical that Congress review this evaluation before proceeding with any proposal to create a mandatory EEVS.

The significant weaknesses that exist in the current program, which serves approximately 16,000 employers, would be greatly exacerbated if the program were to surge to over 7 million. In Fiscal Year 2005, when the latest evaluation took place, only half as many employers used the program as use it now. While improvements to the Basic Pilot have been made since its inception, they are not sufficient for a mandatory program that, because of inaccurate nonconfirmations, could cause workers and businesses irreparable harm. Additionally, if the current flaws in the Basic Pilot are not addressed before it is made mandatory, it will lead to flawed implementation, frustration, and even noncompliance, which will result in certain businesses and industries moving into the unregulated underground cash economy.

When employers and workers move into the underground economy, the societal and economic costs are enormous. If enough of them abandon the "above-ground" economy, it could result in billion-dollar losses in federal, state, and local tax revenues, unfair competition, and further exploitation and abuse of all workers by unscrupulous employers. The similar situation would result if a mandatory EEVS were to be implemented outside the context of comprehensive immigration reform. In that case, the new system would start out with the insurmountable handicap of 8 million unauthorized workers and their employers seeking to uncover and exploit the weaknesses inherent in any system.

Database inaccuracies

One of the most significant problems identified in independent evaluations of the Basic Pilot program is that it is seriously hindered by inaccuracies and outdated information in SSA and DHS databases. For example, a sizeable number of workers who are identified as not having work authorization are in fact authorized, but for a variety of reasons the databases do not have up-to-date information on them. The SSA database used for the Basic Pilot program is the Numident file, which contains information on 435 million SSN holders, including name, date of birth, and place of birth, parents' names, citizenship status, date of death (if applicable), and the office where the SSN application was processed and approved.[6] As referenced earlier in this testimony, the Numident file is the first point of verification in the Basic Pilot process.

According to a December 2006 report by SSA–OIG, 17.8 million (or 4.1 percent) of SSA's records in the Numident file contain discrepancies related to name, date of birth, or citizenship status that could result in tentative nonconfirmation notices from Basic Pilot.[7] Any time that SSA's database conflicts with information presented by a worker, that worker must follow up with one of SSA's field offices. According to the Bureau of Labor Statistics, there are 4.9 million new hires per month

---

[5] *See* Findings of the Basic Pilot Program Evaluation (Temple University Institute for Survey Research and Westat, June, 2002), www.uscis.gov/portal/site/uscis/menuitem.5af9bb95919f35e66f614176543f6d1a/?vgnextoid=9cc5d0676988d010VgnVCM10000048f3d6a1RCRD&vgnextchannel=2c039c7755cb9010VgnVCM10000045f3d6a1RCRD; Immigration Enforcement: Weaknesses Hinder Employer Verification and Worksite Enforcement Efforts (Government Accountability Office, Aug. 2005) (hereafter "GAO"), www.gao.gov/new.items/d05813.pdf; and Congressional Response Report: Accuracy of the Social Security Administration's Numident File (Office of the Inspector General, Social Security Administration, Dec. 2006), (hereafter "SSA"), www.socialsecurity.gov/oig/ADOBEPDF/audittxt/A-08-06-26100.htm; Congressional Response Report: Employer Feedback on the Social Security Administration's Verification Programs (Office of the Inspector General, Social Security Administration, Dec. 2006), www.ssa.gov/oig/ADOBEPDF/A-03-06-26106.pdf; and Congressional Response Report: Monitoring the Use of Employee Verification Programs (Office of the Inspector General, Social Security Administration, Sept. 2006), www.ssa.gov/oig/ADOBEPDF/A-03-06-36122.pdf.

[6] SSA, Accuracy of the Social Security Administration's Numident File, *supra* note 5.

[7] *Id.*

in the U.S.[8] If 4.1 percent of these new hires received a tentative nonconfirmation notice from SSA, field offices could potentially see 100,900 additional citizens and lawful immigrants per month seeking assistance with these alleged discrepancies.

In 2006 testimony before the Senate Finance Committee, the Inspector General of Social Security expressed concerns about an "increased workload in the field offices and teleservice centers" that would result from workers challenging erroneous database findings.[9] At a recent Senate Finance hearing, the President of the National Council of Social Security Management Associations, Inc., testified that if a mandatory EEVS and hardened SSN card are instituted as part of an immigration reform bill without necessary funding, "it could cripple SSA's service capabilities."[10] This problem is compounded by the fact that the agency is at its lowest staffing level since the early 1970s, and SSA field offices have lost 2,400 positions in the past 19 months.[11] As noted in the December 2006 OIG report, "[I]f use of an employment verification service such as the Basic Pilot becomes mandatory, the workload of SSA and DHS may significantly increase—even if only a portion of these 17.8 million numberholders need to correct their records with one of these agencies."[12] Already, SSA field offices serve 42 million visitors per year.[13]

The cost and burden of SSA tentative nonconfirmation notices not only affects local SSA offices, but also workers. Although U.S. citizens' records do have discrepancies, a disproportionate number of the database errors affect foreign-born U.S. citizens and work-authorized noncitizens. According to the December 2006 OIG report, approximately 4.8 million noncitizen records and 8 million foreign-born U.S. citizen records contain discrepancies that may result in a tentative nonconfirmation notice from the Basic Pilot.[14] And, 3.3 million of foreign-born U.S. citizen records do not contain updated information on their citizenship status, so when they claim U.S. citizenship on their I–9 employment eligibility verification form, these workers receive a tentative nonconfirmation notice because their information does not match that in the SSA database.

When workers receive a tentative nonconfirmation notice, they often have to take unpaid time off from work to follow up with SSA, which may take more than one trip. Waiting time at field offices are running two to three hours, with some visits lasting over four hours.[15] According to the National Council of Social Security Management Associations, Inc., nearly one-third of the people currently coming into SSA Field Offices to apply for an original or duplicate SSN have to return with additional documentation.[16] Additionally, an unknown number of work-authorized job applicants are not notified of tentative nonconfirmations by their employer or are wrongfully terminated by their employer before they even have the opportunity to prove that they are indeed authorized to work in the U.S. (For more information on this problem, see the section below regarding employer misuse of the program).

Equally concerning is the fact that when workers do go to an SSA field office to correct their records, their information is sometimes not updated in a timely manner. Additionally, Basic Pilot rules instruct employers to wait 24 hours after a worker has updated his or her records to re-query the system; however, many times the employer will re-query the system before the 24-hour period has passed, or check before the employee visits SSA. In these instances, the employer will receive a default *final* nonconfirmation. According to Basic Pilot rules, the employer is then required to fire the worker.

---

[8] Job Openings and Labor Turnover: February 2007 (U.S. Dept. of Labor, Bureau of Labor Statistics, February 2007), www.bls.gov/news.release/pdf/jolts.pdf.

[9] Patrick P. O'Carroll Jr., Testimony before the U.S. Senate Committee on Finance: Administrative Challenges Facing the Social Security Administration (Office of the Inspector General, Social Security Administration, March 14, 2006), http://finance.senate.gov/hearings/31699.pdf.

[10] 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.

[11] *Id.*

[12] SSA, Accuracy of the Social Security Administration's Numident File, *supra* note 5.

[13] Barnhart, *supra* note 1.

[14] SSA, Accuracy of the Social Security Administration's Numident File, *supra* note 5.

[15] Warsinskey *supra* note 10.

[16] Richard Warsinskey, Testimony before the U.S. Senate Committee on Finance: Administrative Challenges Facing the Social Security Administration (National Council of Social Security Management Associations, Inc., March 14, 2006), http://finance.senate.gov/hearings/31699.pdf.

Employer misuse of the program

The independent evaluations of Basic Pilot have also revealed that employers use the Basic Pilot program to engage in prohibited employment practices.[17] According to the SSA–OIG, "We learned that a significant number of the Basic Pilot employers in our sample verified individuals outside the scope of the signed agreement between the employer, SSA and DHS."[18] For example, the law requires that employers first extend a job offer to a worker and then complete the employment eligibility verification process, including the Basic Pilot procedure. In violation of this requirement, many employers put workers through Basic Pilot *before* extending the job offer, to avoid the potential costs of hiring and training employees who are not eligible to work (a practice known as "pre-screening"). This practice is a problem because most workers who receive a tentative nonconfirmation are, in fact, authorized to work. If workers are not hired because of a tentative nonconfirmation and are never informed that there is a problem with their records, they not only are denied a job but also the opportunity to contest database inaccuracies. Moreover, pre-screening increases the likelihood that an employer may be discriminatorily selecting foreign-looking or foreign-sounding individuals for such screening, resulting in increased discrimination without the person even knowing he or she has been subjected to this unlawful practice.

- In 2002, among employees who received a tentative nonconfirmation from the Basic Pilot, 23 percent said that they were *not* offered a job.[19]
- Four years later, in 2006, 42 percent of employees surveyed reported that employers used the Basic Pilot to verify their employment authorization *before* hire.[20]
- The 2002 evaluation found that 73 percent of employees who should have been informed of work authorization problems were not notified.[21]

Employers also illegally use the Basic Pilot to verify the employment eligibility of their existing workforce. The immigration regulations require employers to reverify workers' employment authorization in very limited circumstances (including when their work authorization expires). This has helped minimize the potential discrimination that may ensue from employers constantly reverifying only noncitizens or from using the reverification system in a retaliatory manner. According to the September 2006 SSA–OIG report, 30 percent of Basic Pilot users admitted they had verified the employment authorization of existing employees.[22]

Employers also take adverse employment action based on tentative nonconfirmation notices, which penalizes workers while they and the appropriate agency (SSA or DHS) work to resolve database errors. For example, the 2002 independent evaluation found that 45 percent of employees surveyed who contested a tentative nonconfirmation were subject to pay cuts, delayed job training, and other restrictions on working.[23] Some employers also compromised the privacy of workers in various ways, such as by failing to safeguard access to the computer used to maintain the pilot system, e.g., leaving passwords and instructions in plain view for other personnel to potentially access the system and employees' private information.

Although employers are prohibited from engaging in these practices under the MOU they sign, USCIS officials have told the GAO that their efforts to review and oversee employers' use of the Basic Pilot program have been limited by lack of staff.[24]

Provisions That Must Accompany Any Nationwide, Mandatory Employment Eligibility Verification System

After nearly a decade of experience with the Basic Pilot Program, it is clear that the existing program has significant flaws that must be addressed if Congress is to pursue the creation of a new EEVS. The creation of such a system without addressing the fundamental flaws in the current program is inadvisable and will result in

---

[17] GAO, SSA, and Temple University Institute for Survey Research and Westat, *supra* note 5.

[18] SSA, Employer Feedback on the Social Security Administration's Verification Programs, *supra* note 5.

[19] Temple University Institute for Survey Research and Westat, *supra* note 5.

[20] SSA, Employer Feedback on the Social Security Administration's Verification Programs, *supra* note 5.

[21] Temple University Institute for Survey Research and Westat, *supra* note 5.

[22] SSA, Monitoring the Use of Employee Verification Programs, *supra* note 5.

[23] Temple University Institute for Survey Research and Westat, *supra* note 5.

[24] Richard M. Stana, Testimony before the Subcommittee on Immigration, Border Security, and Citizenship, Committee on the Judiciary, U.S. Senate, Immigration Enforcement: Weaknesses Hinder Worksite Enforcement Efforts (Government Accountability Office, June 2006), www.gao.gov/new.items/d06895t.pdf.

severe negative consequences for immigrants and U.S. workers on a much larger scale than they currently experience.

The following features would address the flaws in the existing Basic Pilot program.

- **Phase-in with objective benchmarks.**

The best way to ensure implementation of an EEVS that is accurate and implemented in a nondiscriminatory manner is to set standards and expectations for system performance up front and to hold DHS and SSA accountable for meeting those standards. Experience confirms that federal agencies do not meet expectations if the standards they are given are vague and optional. Therefore, the EEVS should be phased in at a reasonable rate, by size of employer, and provide for certification by the Comptroller General that it meets benchmarks regarding database accuracy, low error rates, privacy, and measurable employer compliance with system requirements before implementation and each phase of expansion.

The EEVS program is particularly vulnerable to poor planning because of its unprecedented scope and the disconnect between the agency mandate to get something up and running quickly and the requirements that would ultimately determine whether it is successful, such as the need for speed, efficiency, reliability, and information security. It is much easier to make design changes in a system before it goes fully online than afterwards. That is why software manufacturers produce "beta" versions of their programs to be tested in the real world before mass public marketing distribution. Once a system is designed and put in place for all employers and workers in our economy, it will be costly and difficult to implement needed changes.

- **Antidiscrimination protections.**

Experience has taught us that unscrupulous employers will use the system to unlawfully pre-screen potential employees, reverify work authorization, and engage in other unlawful activities when an employee lodges a complaint or engages in collective organizing. It has also demonstrated that DHS has not prioritized monitoring of employer misuse of the system, since 10 years after it was first implemented there is still no system in place for monitoring it. Thus, stronger enforcement and monitoring efforts and higher penalties for noncompliance are necessary to compel reluctant employers to comply with the law.

Employers also must be explicitly prohibited from (1) conducting employment eligibility verification before offering employment; (2) unlawfully reverifying workers' employment eligibility; (3) using the system to deny workers' employment benefits or otherwise interfere with their labor rights, or to engage in any other unlawful employment practice; (4) taking adverse action against workers whose status cannot initially be confirmed by the EEVS; or (5) selectively excluding certain people from consideration for employment due to the perceived likelihood that additional employment eligibility verification might be required, beyond what is required for other job applicants.

- **Due process protections against erroneous determinations.**

For the first time in the history of this country, workers will need to seek approval from the federal government to secure their livelihood. If the database errors are not improved before the EEVS is implemented, it is likely that millions of workers could be wrongly identified as not authorized for employment. It is therefore critical that workers have access to a *meaningful* administrative and judicial review process that provides for remedies such as back pay and attorney's fees if it is determined that a worker was terminated due to SSA or DHS error. Additionally, the EEVS must allow individuals to view their own records and correct any errors through an expedited process established by SSA and DHS.

- **Privacy and identity theft protections.**

The EEVS must protect information in the database from unauthorized use or disclosure. It is critical that privacy protections be included so that the information contained in the databases is not used for nonemployment eligibility verification purposes. The 2002 evaluation found several instances where employers or other unauthorized individuals gained access to the Basic Pilot program for uses other than the designated purpose. Civil and criminal penalties for unlawful use of information in the EEVS should also be included.

- **Studies of and reports on EEVS performance.**

Any EEVS should be independently evaluated to ensure that the program is meeting the needs of both employers and employees. Reports should specifically evaluate

the accuracy of DHS and SSA databases, the privacy and confidentiality of information in the databases, EEVS's impact on workers, and whether the program has been implemented in a nondiscriminatory manner.

• **Workable documentation requirements.**

Proposals to further limit which documents are acceptable to establish employees' identity must be flexible enough to recognize the fact that not all work-authorized individuals have the same documents. Under no circumstances should a REAL ID-compliant driver's license or ID card be required. No state is currently in compliance with REAL ID, and indeed 11 states thus far have decided not to implement the law or have placed significant conditions on their participation.[25] In eleven additional states, legislation opposing REAL ID has passed one or more chambers of the state's legislature.

Employment Eligibility Verification Systems in the Context of Comprehensive Immigration Reform

The two most significant immigration reform bills introduced in the House and Senate in 2007 include the "Security Through Regularized Immigration and a Vibrant Economy (STRIVE) Act of 2007" (H.R. 1645), introduced by Representatives Gutierrez and Flake, and the "Secure Borders, Economic Opportunity and Immigration Reform Act of 2007" (S. 1348) currently being negotiated in the Senate. Both bills include a mandatory EEVS, but there are *significant* differences between these two proposals. Most notably, the STRIVE Act makes a real attempt to address the shortcomings of the Basic Pilot program by including benchmarks, as well as privacy, antidiscrimination, and due process protections. Although it is unlikely that the STRIVE Act will be the immigration bill taken up by the House Judiciary Committee, it is helpful to analyze its EEVS provisions through the lens of accuracy, workability, and minimizing the harm to *all* workers.

The "Security Through Regularized Immigration and a Vibrant Economy (STRIVE) Act of 2007"

The STRIVE Act represents the best legislative effort to date to address the shortcomings of the Basic Pilot program.[26] Unfortunately, the bill contains a couple of provisions that would limit its workability. First, the STRIVE Act significantly limits the documents that individuals can present to prove their identity when seeking employment. Most concerning is the requirement that workers present documents that do not exist, such as a REAL ID-compliant driver's license and a biometric, machine-readable, tamper-resistant Social Security card. Former Commissioner Barnhart testified in July 2006 that the cost of issuing new cards with enhanced security features could cost approximately $9.5 billion and require 67,000 work years.[27] This means that if U.S. citizens, including foreign-born U.S. citizens, do not have a REAL ID license or hardened SSN, they will have to present either a passport (passports are held by only approximately 20 percent of the U.S. population[28]) or a passport card, which is not yet available. The Brennan Center for Justice estimates that as many as 13 million U.S. citizens do not have ready access to citizenship documents, such as U.S. passports, naturalization papers, or birth certificates.[29]

Second, the STRIVE Act requires SSA to disclose private taxpayer identity information of employers and employees to DHS when DHS requests this information. Use of confidential tax information to enforce immigration law can have a negative affect on tax compliance and has the potential to increase discrimination against foreign-looking or -sounding workers.

Provisions in the STRIVE Act that should be included in any EEVS proposal:

• **Benchmarks for system performance.** Before the EEVS is implemented (and before any subsequent phase-in), the Comptroller General must study and certify that certain standards have been met, including database accuracy, measurable employer compliance with the EEVS requirements, protection of workers' privacy,

---

[25] States include Arkansas, Colorado, Georgia, Hawaii, Idaho, Maine, Missouri, Montana, Nevada, North Dakota, and Washington.

[26] For a summary of the EEVS provisions in the STRIVE Act, *see* Employment Eligibility Verification System in the STRIVE Act of 2007 (National Immigration Law Center, April 2007), www.nilc.org/immsemplymnt/cir/strive_eevs_2007-04-02.pdf.

[27] Barnhart, *supra* note 1.

[28] Phil Gyford, "How Many Americans Own Passports?," www.gyford.com/phil/writing/2003/01/31/how_many_america.php.

[29] Citizens Without Proof: A Survey of Americans' Possession Of Documentary Proof of Citizenship and Photo Identification (Brennan Center for Justice at NYU School of Law, November 2006), www.brennancenter.org/dynamic/subpages/download_file_39242.pdf.

and adequate agency staffing and funding. In conducting the studies, the Comptroller General must consult with representatives from immigrant communities, among others. The Comptroller General is also required to submit reports to DHS and Congress on the impact of the EEVS on employers and employees.

• **Protections against discrimination.** The STRIVE Act amends section 274B of the Immigration and Nationality Act (INA), relating to unfair immigration-related employment practices, to explicitly apply to employment decisions related to the new EEVS. Additionally, it prohibits employers from misusing the EEVS, increases fines for violations, brings the INA into line with other civil rights laws, such as Title VII of the Civil Rights Act, and provides funding to educate employers and employees about antidiscrimination policies.

• **Privacy protections. The STRIVE Act requires that information in the EEVS be safeguarded and that only minimum data elements be stored. It creates penalties for unlawfully accessing the EEVS and for using information in the EEVS to commit** identity theft for financial gain.

• **Due process provisions. The** STRIVE Act requires that workers can view their own records and correct or update information in the EEVS. DHS also must establish a 24-hour hotline to receive inquiries from workers and employers concerning determinations made by the EEVS. **The STRIVE Act** also **creates an administrative and judicial review process to challenge a finding that a worker is not authorized for employment (a "final nonconfirmation"). If, after the process, the worker is found to be authorized for employment and the error was DHS's, the worker is entitled to back wages (although not during any period that the worker was not authorized for employment). However,** attorney's fees and costs are not included—even though employers can recover up to $50,000 in attorney's fees when they challenge a finding that they violated immigrant law. Low-income workers are far less equipped than better-off workers to represent themselves or hire counsel, and the availability of fees is critical to their ability to pursue their rights. STRIVE also prohibits a private right of action, which also would drastically limit workers' ability to correct abuses and errors of the system.

• **Annual study and report.** The STRIVE Act requires the Comptroller General to conduct annual studies to be submitted to Congress that determine whether the EEVS meets the following requirements: demonstrated accuracy of the databases; low error rates and incidences of delays in verification; measurable employer compliance with EEVS requirements; protection of workers' private information; adequate agency staffing and funding for SSA and DHS.

The "Secure Borders, Economic Opportunity and Immigration Reform Act of 2007" (S. 1348) [30]

S. 1348 falls well short of creating a workable system. Its most troubling provision is the requirement that the guest worker and legalization programs for which it provides may not be implemented until the EEVS (including the use of "secure" documentation and digitized photographs that do not currently exist) is implemented. Because of this pressure, the focus will be on getting the EEVS up and running as quickly as possible, rather than on implementing an accurate system that actually works without adversely impacting authorized workers.

It is expected that an amendment will be introduced this week (to amendment 1150; see footnote 30) that will improve the EEVS provisions in S. 1348. Although the amendment will significantly improve the underlying bill, it will not address the database inaccuracies and will fall short on due process protections. Concerns with S. 1348 as introduced include the following:

• **The implementation timeline is unreasonable and unworkable.** All employers must participate in the EEVS within 18 months of enactment, with respect to new hires and those with expiring work authorization documents or immigration status; and within 3 years, all employers must use the EEVS for all new and continuing employees, including those in "Z" status who have not previously presented secure documentation. DHS is also given the sole discretion to require employers to participate at an earlier date than outlined. This rigid timetable must be met regardless of whether the EEVS actually works and whether the technology exists to implement it; nor is the timetable subject to performance benchmarks.

• **The antidiscrimination protections are weaker than current law.** Current law regarding "impermissible" uses of the EEVS would be weakened under the

[30] Amendment 1150 to S. 1348 is the actual text of the bill being debated; however, there has not yet been a vote on the amendment, so S. 1348 still stands. This analysis refers to amendment 1150.

Senate bill (existing requirements are outlined in the MOU that employers sign under the Basic Pilot) because the bill specifically prohibits these "impermissible" practices from being covered under the antidiscrimination protections in the INA by giving DHS exclusive enforcement authority and funding. Section 274B of the INA prohibits discrimination based on national origin and citizenship status, and provides a process for complaints, investigations, administrative and judicial review, and remedies. It is unlikely that DHS's policy will include such procedures, since DHS has no expertise in this area.

• **The due process protections are insufficient.** Under the administrative review provisions, a final nonconfirmation is stayed pending the administrative review decision unless SSA or DHS decides that the "petition for review is frivolous, unlikely to succeed on the merits, or filed for purposes of delay." This means that the agency whose administrative decision is being appealed has sole authority to issue or deny a stay of a nonconfirmation notice while an appeal is pending. The employee appealing the decision faces irreparable harm through loss of employment if a stay is denied, and the legislation does not provide a method for recovery of back pay, costs or attorney's fees for those who are wrongfully terminated due to SSA or DHS database errors, including where the agency fails to issue a stay during the appeal process.

Workers have 30 days from the completion of the administrative appeal to file for judicial review in the U.S. Court of Appeals. However, the court can decide the petition based only on the administrative record, which may be limited. The burden is on the worker to demonstrate that the agency decision was "arbitrary, capricious, not supported by substantial evidence, or otherwise not in accordance with law." Moreover, "findings of fact are conclusive unless any reasonable adjudicator would be compelled to conclude to the contrary." That deferential review standard for factual findings is unwarranted. As with the administrative review process, the court must stay the final nonconfirmation notice, unless it determines that the "petition for review is frivolous, unlikely to succeed on the merits, or filed for purposes of delay."

• **The documentation requirements are unattainable.** Like the STRIVE Act, the documentation requirements are heavily focused on state compliance with the REAL ID Act and a biometrically-enhanced Social Security card.

• **Employers, state and federal government agencies, and SSA are required to turn over to DHS confidential information about workers.** The bill permits data mining of SSA files, tax records, and other federal, state, and territorial databases covering everyone in the U.S. Multiple provisions requiring information-sharing give DHS expansive access to (a) personal employee information held by employers; (b) birth and death records maintained by states, passport and visa records, and state driver's license or identity card information; and (c) as an exception to tax code confidentiality provisions, SSA records of taxpayers when the taxpayer's SSN or name or address (for whatever reason) does not match SSA records, or when just two taxpayers have the same SSN. It also allows DHS to access "information" from SSA that DHS "may require." The provisions do not require independent review, monitoring of disclosure, privacy protections, notice to workers that their private information or records have been disclosed, or recourse if overbroad information is sought or misused.

Conclusion

As stated in the first part of this testimony, based on our experience, NILC does not support the creation of a mandatory EEVS. However, when the House of Representatives moves forward with its immigration reform bill, which will inevitably include a mandatory EEVS, it is critical that it be guided by the lessons learned from ten years of experience with the Basic Pilot program. Put simply, if the shortcomings of the Basic Pilot are not addressed before it is expanded into a mandatory program, it will be a disaster for workers and employers, and will put an enormous strain on already overburdened SSA field offices. Because so much of the focus of EEVS proposals is on DHS, it will be important for this committee to work closely with the Judiciary Committee on any comprehensive immigration reform bill that creates a mandatory EEVS to ensure that SSA has the necessary funding and resources to carry out its duties. It will also be critical to ensure that the weaknesses of the Basic Pilot are addressed before it is expanded, including correcting SSA's database errors, and implementing a monitoring system so employers do not use the system to take adverse action against workers.

Chairman MCNULTY. Thank you.
Mr. Amador.

STATEMENT OF ANGELO I. AMADOR, DIRECTOR OF IMMIGRATION POLICY, U.S. CHAMBER OF COMMERCE

Mr. AMADOR. Thank you. Good morning, Chairman McNulty, Ranking Member Johnson, and distinguished Members of the Committee. Thank you for inviting me to testify on EEVS today. My name is Angelo Amador. I am the Director of Immigration Policy for the Chamber.

We also chair the Essential Workers Immigration Coalition, and are on the executive Committee of the Electronic Employment Verification System working group. That is a business group, but actually, as Tyler knows, we work very closely with groups on the left, unions, and this is a system that really is going to affect everyone, and we really need to work together to make sure that all of the main issues are addressed.

The concerns of the business community about how this new mandate is going to affect us cannot be overstated. The Government Accountability Office, as was said earlier, estimate that the cost of a new EEVS system that would apply to all employees would cost about $11.7 billion per year, with employers bearing most of the cost. Still, the Chamber is willing to support a new EEVS as a necessary part of comprehensive immigration reform.

While most of the press has concentrated on the issues of the undocumented and the new worker programs with regards to comprehensive reform, employers view the employer verification system provisions as equally important. In fact, some of my members view it as the most important part of comprehensive reform.

As stated in my written testimony, the three issues are interrelated, and comprehensive reform remains crucial to both economic and national security for our country. Noted national security experts have also reinforced that enforcement alone at any level is not sufficient, and it would not be the solution.

Everyone agrees that the current immigration system is broken and the status quo is unacceptable. But agreement on a solution has been harder to find. States and localities have responded to the lack of action at the Federal level with a patchwork of immigration laws and enforcement, exposing employers most deal with a broken legal structure of unfair liability.

Many states and local governments are attempting to either force employers and retailers to bear the costs of helping shield undocumented workers, or are attempting to impose additional worksite enforcement provisions. must know what their responsibilities are, and having one Federal law with strong state law preemption language will help alleviate any confusion about employers' role under the law.

There are things that can be done immediately without legislation, such as limiting the number of documents accepted for verification under the I–9 system. Also, current documents should be retooled so as to provide employers with a clear and functional way to verify that they are accurate and relate to the prospective employee.

As you know, there are more than 27 documents and combinations of documents that you can use to prove your employment eligibility. Some of them don't even have pictures. So, you could technically get a job without showing an ID that has a picture, and the employer is forbidden, because of the current anti-discrimination provisions, from asking for other pieces of ID.

In addition, I would like to mention seven other critical things that are very crucial for the employer community. There are some others that are in my testimony, and actually some are addressed by Tyler as well, that I think are very important.

Just for the time being, I want to mention that, first, enforcement of employment verification law resides properly within the Federal Government. Accordingly, the Chamber maintains that DHS, as the Federal enforcement authority with responsibility in enforcement of section 274A, which is the one that we are talking about, should remain.

You may be aware that the Federal RICO statute has recently been used by private attorneys seeking to enforce immigration law. Not only does this invade the province of the Federal Government as sole enforcer of Federal immigration policy, it also perverts the Federal RICO statute into a use that is contrary to the intent of the statute. We do not want to create a trial attorneys relief act.

Second, the power to investigate labor and employment violations should be kept out a system created exclusively for the purpose of verifying employment eligibility. The system needs to be implemented with full acknowledgment that employers already have to comply with a variety of employment laws. The Code of Federal Regulations—actually, I looked at it this morning—is more than 5,000 pages long.

Third, a new verification system should only apply to new hires. Trying to re-verify the entire existing workforce of over 140 million employees is a burden that is too high. Again, I will be happy to talk about the different versions, but the version of the Senate requires that you re-verify more than 140 million employees.

What we hear from our members, especially those that are large, is that that is a monumental task. And there are other ways of doing this. Again, with the turnover today, everybody will be verified under the system in a couple of years.

Fourth, an employer should also be responsible only to verify the work authorization of its own employees.

Fifth, an employer needs to be able to affirmatively rely on the response as soon as possible. We think that 30 days should be more than enough for DHS or Social Security or somebody to tell us whether this person is authorized to work or not.

There are concerns, as you might have heard, and it is in the testimony, of the cuts that are implied when you have a tentative nonconfirmation. For one, you cannot fire the worker. Second, DHS wants to use the fact that this individual that they told you not to fire to come and investigate and do raids and other things.

Sixth, penalties must be tailored to the offense, and the system must be fair. Automatic debarment from Federal contract is not an authority that should be given to DHS. Indeed, a work in process already exists in current law under the Federal Acquisition Regulations.

Finally, let me know that we are concerned about undue expansion of liability and new causes of actions which we have seen in some formulations of electronic employer verification systems. For example, the STRIVE Act, which I agree with Tyler is probably the best effort right now at trying to address a workable EEVS, but it still has—it would even make it illegal for an employer to hire an American or a legal permanent resident over a temporary worker that should be in the United States only when employers cannot find enough of the first two.

Discrimination protections should be retained, as in current law, to comport with the purposes of the program, monitoring the hiring and firing process, not other terms and conditions of employment.

Thank you for giving me the opportunity to come before you today, and I look forward to your questions.

[The prepared statement of Mr. Amador follows:]

Statement of the U.S. Chamber of Commerce

ON: ELECTRONIC EMPLOYMENT VERIFICATION SYSTEMS (EEVS)

TO: THE HOUSE SUBCOMMITTEE ON SOCIAL SECURITY OF THE COMMITTEE ON WAYS AND MEANS

BY: ANGELO I. AMADOR

DATE: JUNE 7, 2007

The U.S. Chamber of Commerce is the world's largest business federation, representing more than three million businesses and organizations of every size, sector, and region.

More than 96 percent of the Chamber's members are small businesses with 100 or fewer employees, 70 percent of which have 10 or fewer employees. Yet, virtually all of the nation's largest companies are also active members. We are particularly cognizant of the problems of smaller businesses, as well as issues facing the business community at large.

Besides representing a cross-section of the American business community in terms of number of employees, the Chamber represents a wide management spectrum by type of business and location. Each major classification of American business— manufacturing, retailing, services, construction, wholesaling, and finance—is represented. Also, the Chamber has substantial membership in all 50 states.

The Chamber's international reach is substantial as well. It believes that global interdependence provides an opportunity, not a threat. In addition to the U.S. Chamber of Commerce's 96 American Chambers of Commerce abroad, an increasing number of members are engaged in the export and import of both goods and services and have ongoing investment activities. The Chamber favors strengthened international competitiveness and opposes artificial U.S. and foreign barriers to international business.

Positions on national issues are developed by a cross-section of Chamber members serving on committees, subcommittees, and task forces. More than 1,000 business people participate in this process.

Statement on

"Electronic Employment Verification Systems (EEVS)"

Before

The House Subcommittee on Social Security of the Committee on Ways and Means

Angelo I. Amador

Director of Immigration Policy

U.S. Chamber of Commerce

June 5, 2007

Good Morning Chairman McNulty, Ranking Member Johnson, and distinguished members of the Subcommittee. Thank you for inviting me to testify on the subject of employment eligibility verification systems. My name is Angelo Amador and I am director of immigration policy for the U.S. Chamber of Commerce. I am encouraged that the Subcommittee is examining the potential impact that a new electronic employment verification system (EEVS) would have on workers and employers.

The Chamber is the world's largest business federation, representing more than three million businesses and organizations of every size, sector, and region. The Chamber co-chairs the Essential Worker Immigration Coalition (EWIC), a coalition of businesses, trade associations, and other organizations from across the industry spectrum that support reform of U.S. immigration policy to facilitate a sustainable workforce for the American economy while ensuring our national security and prosperity.

The Chamber is also on the executive committee of the Employment Eligibility Verification System Working Group, or EEVS Working Group. This group was formed to serve as the voice of business exclusively on the issue of a new employment verification system and it is now made up of companies and trade associations from across the industry spectrum. The reason is simple:

there are over seven million employers and this will affect all of them, whether or not they hire immigrants.[1]

The stakes are extremely high, and the concerns of the business community of how a new system will be constructed cannot be overstated. While much of the press has been focused on the issues of the undocumented and new worker programs, we certainly view the employer verification system provisions as equally important. After all, a new EEVS will have an impact in the day-to-day activities, obligations, responsibilities, and exposure to liability of every U.S. employer.

I. Overview

The Chamber supports a new EEVS within the context of comprehensive immigration reform because employers want the tools to ensure that their workforce is in fact authorized to work. Currently, each new employee must be verified as eligible to work under the paper-based I-9 system and we expect that new employees would have to be verified under any future EEVS. All the proposals under consideration by Congress require employers to bear a greater share of the burden of enforcing the nation's employment eligibility policies. The new EEVS must recognize that the over seven million employers in the U.S. are extremely different in both size and levels of sophistication and, accordingly, the system should accommodate these differences. If the system is not constructed and implemented properly, there is great risk of very real confusion among employers and employees alike, which could have significant consequences for every individual worker, as well as the employer community.

There are common concerns across the business, labor, and ethnic groups' advocates because of the broad reach of any new program. However, the Chamber believes that a new law should not be used to open the door to a barrage of new causes of action unrelated to the hiring or firing of employees based on their work authorization status and should, instead, clarify that only the Department of Homeland Security has enforcement jurisdiction over this issue. Likewise, employment verification, as discussed below, should not be combined with the enforcement of labor laws. Before concentrating on the specifics of a future system, I will briefly address why this issue should be dealt with only within the context of comprehensive immigration reform.

II. New EEVS Within the Context of Comprehensive Immigration Reform

Current immigration laws are severely flawed and have failed to curb the flow of undocumented workers into the U.S. It has been more more than 20 years since the passage of the Immigration Reform and Control Act of 1986 (IRCA), and we are still experiencing the entry of undocumented workers into the U.S. at a rate of about 500,000 per year.[2] IRCA's goal was to address the undocumented in the country and create a worksite enforcement regime that deterred the employment of the undocumented, but it did not address the future need for workers in the

[1] U.S. Census Bureau "Number of Firms, Number of Establishments, Employment, and Annual Payroll" http://www.census.gov/csd/susb/susb04.sh.
[2] Passel, Jeffrey, "The Size and Characteristics of the Unauthorized Migrant Population in the U.S." *Pew Hispanic Center Report*, March 2006. http://pewhispanic.org/files/reports/61.pdf

U.S. economy. There was no provision for the legal flow of lesser skilled or semi-skilled ("essential") workers when there was a shortage of U.S. workers.

Studies have shown that the principal element in determining the level of immigration into the U.S., both legal and illegal, in the last decade is the strength or weakness in our economy, while enforcement has had only a "small" effect.[3] "The single macroeconomic/demographic variable most highly correlated with the annual flows is the U.S. unemployment rate."[4] Therefore, any new earned legalization program with a new worksite enforcement regime must be promulgated together with a new essential workers program. This new essential workers program must have the flexibility to respond to the needs of our vibrant and diverse economy.

There have been recent attempts to revamp the current worksite enforcement regiment in isolation at the federal legislative level and through the administrative process. Although the goal of fixing the worksite enforcement program is admirable, such attempts, outside comprehensive reform, could be severely detrimental to the economic security of the country. Noted national security experts have also reinforced that enforcement alone at any level is not the solution.[5]

III. The Current Employment Verification System

IRCA created the current paper-based employment verification system in the U.S. An employer must wait for a newly hired employee to start work before attempting to verify work eligibility in the U.S. Within the first three days, the employee shows the employer a document or combination of documents to prove identity and eligibility to work from a list of 27 possible options. The employer must fill out the Form I-9 and retain it. The process is susceptible to fraudulent documents, as well as identity fraud. Employers are not document experts. If a document looks valid on its face, an employer may not legally ask questions without the risk of violating anti-discrimination laws.

The current system has made it impossible for employers to really know who is actually authorized to work and who is not. It is important to note that often, when the Department of Homeland Security (DHS) conducts an audit or raid of an employer, the employer is generally not found at fault because it has followed the law, filled out the proper forms and documents, and could not have known that its employees were not authorized to work. While the company might not suffer any legal action or fines, losing valuable members of the workforce and possibly closing down for even a short amount of time can often add up to significant financial losses, not including the less quantifiable harm such as negative publicity.

In 1998, DHS rolled out an electronic employment eligibility system, the Basic Pilot Program. The Basic Pilot Program is a strictly voluntary, internet based, automated system where an

---

[3] Passel, Jeffrey, "U.S. Immigration: Numbers, Trends, and Outlook." *Pew Hispanic Center Report*, March 26, 2007, pages 12-13.
[4] Id. at 13.
[5] Coalition for Immigration Security, composed of numerous former DHS officials, stated in their April 2006 letter that there is a relationship between adequate legal channels of immigration and enhanced border security. See also Stuart Anderson "Making the Transition from Illegal to Legal Migration" *National Foundation for American Policy*, November 2003.

employer checks a new hire's name and social security number against a government-run database to make sure the name and number matches those on record. As numerous studies and reports have shown, the databases maintained at DHS and the Social Security Administration are not always up-to-date, there is a high error rate in determining work authorization, and the program is incapable of capturing identity fraud.[6] It is worth noting that in its current form, it would be problematic to expand it to all existing employers and employees. A future EEVS will need to take into account the failures and successes of the Basic Pilot Program to ensure that it is workable.

IV. Potential Costs and Increased Workloads

In your invitation, I was asked to address the potential costs and increased workloads that would be faced by the Social Security Administration (SSA). The Chamber would like to point out that in addition to the government cost of hiring more verifiers, modernizing the system, and purchasing and monitoring additional equipment, the Government Accountability Office (GAO), relying on independent studies, estimated "that a mandatory dial-up version of the pilot program for all employers would cost the federal government, employers, and employees about **$11.7 billion total per year, with employers bearing most of the costs**."[7] (Emphasis added.)

Employers would also need to train employees to comply with the new law's requirements and devote a great deal of human resources staff time to verifying and re-verifying work eligibility, resolving data errors, and dealing with wrongful denials of eligibility.[8] In particular, data errors and technological problems would lead many employees to start work as "would-be employees."[9] This could lead to a substantial decrease in productivity, especially when the work to be done is seasonal or time-sensitive.[10] Employers would also have to deal with the possibility of another level of government bureaucracy with random "on-site auditing" powers.[11] Finally, employers who already will incur many internal costs of meeting the requirements of a new EEVS, should not be subject to a fee to pay for the cost of building the system itself—that is a government function and should be paid for by the government.

V. Principles for a New Employment Eligibility Verification System

Businesses want a reliable, streamlined, and easy to use method to verify the employment eligibility of their workforce. To start, it is imperative that adequate funds and resources be allocated to develop and implement the program to accommodate the over seven million

---

[6] Government Accountability Office, "Immigration Enforcement: Weaknesses Hinder Employment Verification and Worksite Enforcement Efforts," June 19, 2006, http://www.gao.gov/new.items/d06895t.pdf. Even an error rate of one percent of applicants would put at risk over a million workers in losing their job or perspective employment. The stakes could not be higher. For more detail on error rates see testimony from Angelo I. Amador, U.S. Chamber of Commerce before the House Subcommittee on Workforce, Empowerment, and Government Programs of the Committee on Small Business, June 27, 2006, http://www.uschamber.com/issues/testimony/2006/060627_testimony_immigrant_employment.htm.

[7] GAO, Immigration Enforcement: Weaknesses Hinder Employment Verification and Worksite Enforcement Efforts, at 29.

[8] Sparapani, Memorandum on Problems with Employment Eligibility.

[9] *Id.*

[10] *Id.*

[11] DHS, Report to Congress on the Basic Pilot Program, at 8, July 2004.

employers in the U.S. This will be a significant expansion of the less than one percent of the employer community that currently uses the Basic Pilot Program on a voluntary basis.[12] The Chamber has testified many times during the immigration reform debate and has consistently called for the development of an EEVS that carefully addresses: who is to be verified; what documents will be accepted; how the system will be phased in; how the system will function and who will certify functionality; how the system will be enforced; and, how DHS will protect good faith actors.

The Chamber's foremost concern is to ensure that any new system does not become too costly or burdensome for employers. Businesses already spend approximately 12 million hours each year documenting the legal status of the nation's 50 to 60 million new hires.[13] This new system will not only be used by companies with large Human Resources departments and in-house legal counsel, but also by employers operating in the field out of the back of a pickup truck. These small employers create millions of jobs in the U.S. economy, and the burdens placed upon these entrepreneurs must be considered.

A. Preemption of State Laws and Local Ordinances

The current immigration system is clearly broken and states and localities have responded to the lack of action at the federal level with a patchwork of immigration laws and enforcement—exposing employers who must deal with a broken legal structure to unfair liability. Many states and local governments are attempting to either force employers/retailers to bear the cost of helping shield undocumented workers or are attempting to impose additional worksite enforcement provisions. These attempts run the risk of undermining the ability of the federal government to oversee and enforce national immigration laws and also put undue burden on businesses attempting to deal with the current broken system.

A new worksite enforcement regime needs to address specifically these attempts to preempt jurisdiction of federal immigration law.[14] Employers must know what their responsibilities are under immigration law, and having one federal law will help alleviate any confusion about employers' role under the law.

B. Fair Enforcement Provisions

Full and fair enforcement of a new, functional verification system coupled with comprehensive immigration reform will be more feasible and more likely to focus on the true egregious violators than is currently the case. Enforcement should take into account transition times for the new system and should protect employers acting in good faith.

---

[12] As of December 2006, over 12,000 employers were registered with the Basic Pilot Program, approximately 0.2 percent of all employers, http://www.uscis.gov/files/nativedocuments/EEV_FS.pdf.
[13] Jacoby, Tamar. "An Idea Whose Time Has Finally Come? The Case for Employment Verification." *Migration Policy Institute*, 2005, www.migrationpolicy.org.
[14] A record number of immigration-related bills are under consideration, or have been enacted, in all 50 states. Nationwide, 1,169 immigration bills are in the works, and at least 57 bills in 18 states have been enacted, according to the National Conference of State Legislatures, http://www.ncsl.org/.

Furthermore, DHS should have primary authority over the enforcement provisions of any new system.

Enforcement of employment verification laws resides properly with the federal government. Accordingly, the Chamber maintains that DHS, as the federal agency tasked with responsibility for immigration enforcement, should have sole enforcement authority over prosecutions for violations of section 274A of the immigration code, and this should also be the case for all other enforcement provisions in any new employment verification system.

You may be aware that the federal RICO statute has recently been used by private attorneys seeking to enforce immigration law. Not only does this invade the province of the federal government as sole enforcer of federal immigration policy, it also perverts the federal RICO statute into a use that is contrary to the intent of the statute.

Thus, there should be language prohibiting private rights of action against employers for matters that should be enforced by DHS. Furthermore, the power to investigate any labor or employment violations should be kept out of a system created exclusively for the purpose of verifying employment eligibility. The Chamber continues to call for a simple and reliable system, which includes reasonable penalties for bad actor violators.

C. Liability Standards and Penalties

The Chamber agrees that employers who knowingly employ illegal aliens ought to be prosecuted under the law. This current "knowing" legal standard for liability is fair and objective and gives employers some degree of certainty regarding their responsibilities under the law and should, therefore, be maintained. Lowering this test to a subjective standard would open the process to different judicial interpretations as to what an employer is expected to do. Presumptions of guilt without proof of intent are unwarranted. Furthermore, while the government should punish intentional violators, those employers whose only error was a simple oversight or mistake should be given an opportunity to rectify such error.

We do not oppose efforts to increase penalties. However, the penalties need to be proportionate to the offense and comparable to other penalties in existence in the employment law arena. If penalties are too high, and too unyielding, an employer who is assessed a penalty, but believes that they did not violate the law, will be forced into an unnecessary settlement because they cannot afford to pay both the legal fees necessary to fight the citation, and gamble that they might end up with a penalty that is so high that it devastates their business. Penalties should not be inflexible, and we urge you to incorporate statutory language that allows enforcement agencies to mitigate penalties, rather than tying them to a specific, non-negotiable, dollar amount.

It is also critical to the employer community that it does not bear vicarious liability for subcontractor actions unless the contractor knew of the actions of the subcontractor. In other words, the contractor should not be held liable for undocumented workers hired by

a subcontractor, both of which would be required to independently participate in the new EEVS for their own employees, without evidence of direct knowledge of the general contractor. Without such protection, an employer could be open to liability even for the violations of its peripheral contractors – e.g. a water delivery company or landscaping contractor.

A number of additional penalties and causes of action have been suggested as proper penalties in a new verification system. These range from debarring employers from federal government contracts to expansion of the current antidiscrimination protections. Penalties must be tailored to the offense and the system must be fair. Automatic debarment from federal contracts is not an authority that should be given to DHS. Indeed a working process already exists in current law under the Federal Acquisition Regulations (FAR).

Additionally, the Chamber objects to expansion of antidiscrimination provisions found in current law. As stated above, a new, functional system coupled with comprehensive immigration reform should provide adequate assurances that it will not be used to discriminate against workers. Employers should not be put in a "catch-22" position in which attempting to abide by one law would lead to liability under another one.

D. Employee Population to be Covered

Pursuant to IRCA, each new employee hired after November 6, 1986 must be verified as eligible to work under the current paper-based I-9 system. IRCA grandfathered employees hired prior to November 6, 1986 so as not to cause undue disruption of businesses. It is critical that any new process only mandate that new hires need to be verified under any future electronic employment verification system. Employers should only be required to verify new employees, as existing employees have already been verified under the applicable legal procedures in place when they were hired. Re-verifying an entire workforce is an unduly burdensome, costly proposition, and unnecessary given how often workers change jobs in the United States.

E. Acceptable Documents for Proof of Identity and Employment Authorization

The issues of document fraud and identity theft have been exacerbated under the current paper-based I-9 system because of the lack of reliable and secure documents. Documents should be re-tooled and limited so as to provide employers with a clear and functional way to verify that they are accurate and relate to the prospective employee. There are two ways by which this can be done, either by issuing a new tamper and counterfeit resistant work authorization card or by limiting the number of acceptable work authorization documents to, for example, social security cards, driver's licenses, passports, and alien registration cards (green cards). All of these documents could be made more tamper and counterfeit resistant. In fact, in 1998, the federal government began issuing green cards with a hologram, a digital photograph and fingerprint images and by 2010 all green cards currently in existence should have these features.

With fewer acceptable work authorization documents, the issue of identity theft can more readily be addressed. The new verification process will need to require a certain degree of inter-agency information sharing. When an employer sends a telephonic or internet based inquiry, the government must not only be able to respond as to whether an employee's name and social security number matches, but also whether they are being used in multiple places of employment by persons who may have assumed the identity of other legitimate workers. In the long run, as the verification system is developed and perfected, it should move closer towards the use of biometric technology that can detect whether the person presenting the document relates to the actual person to whom the card relates.[15]

F. Fair and Reasonable Roll Out of New System

The Government Accountability Office (GAO) reported last year that there are still some unresolved issues with the Basic Pilot Program, including delays in updating immigration records, false-negatives, and program software that is not user friendly.[16] Specifically, GAO has reported additional problems and emphasizes, "the capacity constraints of the system [and] its inability to detect identity fraud."[17] Given these and other concerns, the new system should be phased in and tested at each stage, and expanded to the next phase only when identified problems have been resolved. The best approach would be for the program to move from one phase to the next only when the system has been improved to take care of inaccuracies and other inefficiencies ascertained through the earlier phase. This would also allow DHS to properly prepare for the new influx of participants. In addition, if industry sectors are carved out, these need to be delineated and defined. For example, there needs to be clear guidelines of what exactly falls within the broad term of "critical infrastructure" if that is used as one benchmark.

G. Response Times

The employer needs to be able to affirmatively rely on the responses to inquiries into the system. Either a response informs the employer that the employee is authorized and can be retained, or that the employee is not and must be discharged. Employers would like to have 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 Social Security Administration must be given the resources to ensure that work authorization status changes are current to 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.

The Chamber understands that due process concerns must allow the employee to know of an inquiry and to then have the ability to challenge a government determination. Thus, at

---

[15] Obviously, as biometric technology is rolled out, it is important to address who would actually pay for the readers and the implementation of the technology. Further, there will be legitimate issues of practicality in implementing biometrics in many workplaces.

[16] Bovbjerg, Barbara D., Director, Education, Workforce, and Income Security Issues at GAO, Testimony before the Subcommittee on Oversight of the House Committee on Ways and Means, February 16, 2006.

[17] Id.

the very least, employers should be able to submit an initial inquiry into the system after an offer of employment has been made and accepted. Presumably this could be done two weeks before the first day of employment so the clock starts running earlier. The start date should not be affected by an initial tentative nonconfirmation. Of course, for employers that need someone immediately, the option of submitting the initial inquiry shortly after the new employee shows up for his or her first day at work should continue to be available. In the case of staffing agencies, current law allowing for submission of the inquiry when the original contract with the agency is signed should be kept in future laws. A maximum of 30 days, regardless of when or how the inquiry is made, and taking into consideration time to submit additional information and manual review, should be the outer limit that the system should take from the date of initial inquiry until a final determination is issued by the government.

H. Government Accountability

The government must also be held accountable for the proper administration of the new system. There must be an administrative and judicial review process that would allow employers and workers to contest findings. Through the review process, workers could seek compensation for lost wages due to a DHS agency error. Meanwhile, if an employer is fined by the government due to unfounded allegations, the employer should be able to recover some attorneys' fees and costs—capped at perhaps $50,000—if they substantially prevailed in an appeal of the determination. Additionally, workers should have access to review and request changes to their own records to avoid issues when changing jobs.

I. Limited Bureaucracy and Additional Cost Concerns

It is imperative that the new system be workable, simple, easy to use, and not be costly or burdensome to employers. DHS will need adequate funding to create, maintain and implement the new system. This cost should not be passed on to the employer with fees for inquiries or through other mechanisms. Additionally, there should not be overly burdensome document retention requirements. The more copies of official documents are kept in someone's desk drawer, the increased likelihood of identity theft. Under current law, an employer does not need to keep copies of driver licenses, social security cards, birth certificates, or any other document shown to prove work authorization. The employer must certify under penalty of perjury that those documents were presented. The requirement to copy and store copies of this sensitive documentation in any new program should be carefully analyzed not only from the cost perspective to employers, but also from the privacy perspective of workers.

J. No Further Expansion of Employment Law

Finally, the new system needs to be implemented with full acknowledgment that employers already have to comply with a variety of employment laws. Thus, verifying employment authorization, not expansion of employment protections, should be the sole emphasis of a new employment verification system.

In this regard, it should be emphasized that there are already existing laws that govern wage requirements, pensions, health benefits, the interactions between employers and unions, safety and health requirements, hiring and firing practices, and discrimination statutes. The Code of Federal Regulations relating to employment laws alone covers over 5,000 pages of fine print. And of course, formal regulations, often unintelligible to the small business employer, are just the tip of the iceberg. Thousands of court cases provide an interpretive overlay to the statutory and regulatory law, and complex treatises provide their own nuances.[18] A GAO report titled "Workplace Regulations: Information on Selected Employer and Union Experiences" identified concerns regarding workplace regulations that employers continue to have to this very day.[19] The report noted that enforcement of such regulations is inconsistent, and that paperwork requirements could be quite onerous. Most importantly, the report concluded that employers are overburdened by regulatory requirements imposed upon their businesses and many are fearful of being sued for inadequate compliance.

The cost of compliance continues to grow at an alarming pace. A 2005 study by Joseph Johnson of the Mercatus Center[20] estimated the total compliance cost of workplace regulations at $91 billion (in 2000 dollars) and a follow up study by W. Mark Crain for The Office of Advocacy, U.S. Small Business Administration,[21] estimated the total compliance cost of workplace regulations at $106 billion (in 2004 dollars). Within a four year span, the cost grew at a rate of $15 billion, or $3.75 billion per year.

VI. Conclusion

The Chamber urges you to continue to engage the business community to create a workable electronic employment verification system within the context of comprehensive immigration reform. This requires an overall system that is fast, accurate and reliable under practical real world working conditions, and includes:

- Clarification that federal jurisdiction preempts state and local laws with DHS-only enforcement authority;
- An investigative and enforcement system that is fair, with penalties commensurate to the offense;
- Provisions to protect first-time good faith "offenders" caught in the web of ever-changing federal regulations;
- No expansion of liability beyond the knowing standard for contractor/subcontractor relationships;
- No expansion of antidiscrimination laws or debarment outside the FAR system;

[18] For example, one treatise on employment discrimination law alone stretches over 2,000 pages. Barbara Lindemann and Paul Grossman, "Employment Discrimination Law," *ABA Section of Labor and Employment Law*, 3rd Edition, 1996.
[19] U.S. Government Accountability Office Report, "Workplace Regulation: Information on Selected Employer and Union Experiences," GAO-HEHS-94-138, Washington DC, pages, June 30, 1994, pages 25-53.
[20] Johnson, Joseph. "The Cost of Workplace Regulations", *Mercatus Center*, George Mason University, Arlington, Virginia, August 2001.
[21] Crain, Mark W. "The Impact of Regulatory Costs on Small Firms," Report RFP No. SBHQ-03-M-0522, Lafayette College, for the Office of Advocacy, *U.S. Small Business Administration*, September 2005.

- A new verification system that only applies to new hires;
- A reasonable number of reliable documents to reduce fraud;
- A telephone based alternative to accommodate all employers;
- A phase-in with independent certification as to accuracy and workability;
- Congressional oversight authority with independent studies;
- Verification to begin when firm offer of employment is made and accepted, followed by reasonable system response times—at the most 30 days;
- Accountability structures for all involved—including our government;
- Limited bureaucracy and sensible document retention requirements that takes into consideration privacy concerns;
- No artificially created incentives favoring automatic fines or frivolous litigation; and,
- No expansion of labor laws within the electronic employment verification system.

Employers will be required to utilize and comply with the new electronic employment eligibility verification system, and therefore, we should continue to be consulted in shaping such a system. We at the Chamber, EWIC, and the EEVS Working Group, stand by to continue to assist in this process. Thank you again for this opportunity to share the views of the Chamber, and I look forward to your questions.

Committee on Ways and Means
Witness Disclosure Requirement – "Truth in Testimony"
Required by House Rule XI, Clause 2(g)

Your Name: Angelo I. Amador

	Yes	No
1. Are you testifying on behalf of a Federal, State, or Local Government entity?	☐	☒
2. Are you testifying on behalf of an entity other than a Government entity?	☒	☐

3. Please list any Federal grants or contracts (including subgrants or subcontracts) which you have received during the current fiscal year or either of the two previous fiscal years:

n/a

4. Other than yourself, please list what entity or entities you are representing:

U.S. Chamber of Commerce

5. If your answer to question number 2 is yes, please list any offices or elected positions held or briefly describe your representational capacity with the entities disclosed in question number 4:

Director of Immigration Policy

	Yes	No
6. If your answer to question number 2 is yes, does any of the entities disclosed in question number 4 have parent organizations, subsidiaries, or partnerships that you are not representing?	☐	☒

7. If the answer to question number 2 is yes, please list any Federal grants or contracts (including subgrants or subcontracts) which were received by the entities listed under question number 4 during the current fiscal year or either of the two previous fiscal years, which exceed 10 percent of the entity's revenues in the year received, including the source and amount of each grant or contract to be listed:

n/a

Signature: [signature] Date: 6/15/07

Chairman MCNULTY. Thank you.
Ms. Meisinger.

STATEMENT OF SUSAN R. MEISINGER, PRESIDENT AND CEO, SOCIETY FOR HUMAN RESOURCE MANAGEMENT, ALEXANDRIA, VIRGINIA

Ms. MEISINGER. Mr. Chairman, Ranking Member Johnson, Members of the Committee, my name is Sue Meisinger and I am President and CEO of the Society for Human Resource Management. I appear today on behalf of the more than 200,000 members of the society, as well as being co-chair of the HR Initiative for a Legal Workforce. I am grateful for this opportunity.

Our members represent the frontlines on workforce verification, and therefore offer a crucial viewpoint on the matter. We fully support and we are committed to the hiring of only work-authorized individuals through an effective, efficient, electronic employment verification system.

We also recognize that the current employment verification system is in need of real reform. In fact, we believe that verification is the linchpin of really, truly reforming the immigration system.

As the debate on immigration reform continues, we urge Congress to carefully consider the implications of any new employment verification system, keeping in mind that this is not just a debate about immigration reform. This is a debate about workplace management, which impacts all employers and all American workers, not just those who are foreign born.

My remarks will focus on the current employment verification process, as well as our proposal to create a potentially alternative effective employment verification system.

As you know, under IRCA, employers are required to review documents presented by employees, and after review, required to attest on a Form I–9 that they have reviewed the documents and that they appear genuine and authentic.

Even under the best of circumstances, HR professionals encounter numerous challenges with the employment verifications of IRCA. They include maintaining the I–9 records when an employee presents a document that has an expiration date; verifying the authenticity, the quality, the quantity of documents presented by an employee for work authorization and identification purposes; and simply managing the current I–9 system, which is burdensome and time-consuming.

The system is prone to fraud, forgeries, and identity theft. It is difficult if not impossible for an employer to differentiate between the legal and illegal worker in this process. In addition, if an employer questions the validity of documents too much, they are also vulnerable to potential claims of discrimination.

Attempting to address the shortcomings of the paper-based system, Congress created the Basic Pilot Program that we have heard of this morning in great detail. Under this system, employers can voluntarily check each new employee's work eligibility using the electronic verification system, while also having to do the paper check and maintaining the paper records.

The system is supposed to respond to the employer within three days with either a confirmation or a tentative nonconfirmation of the employee's work eligibility. In the cases of tentative nonconfirmation, a secondary verification process lasting 10 days is initiated to confirm the validity of the information provided and to pro-

vide the employer with a confirmation of nonverification of worker eligibility.

Although it has been operational since 1997, and despite the best efforts of the people in the government agencies managing it, we think it is just flat-out inadequate to meet the U.S. employer's needs in a global verification system.

As we heard this morning, over 92 percent of inquiries from employers receive an instantaneous employment authorized response. This means there is a no verification 8 percent of the time. With 60 million new hires each year, this makes mandating the system having an impact on about 5 million people a year, as we have heard as well.

Since a significant percentage of the Basic Pilot queries require human intervention, a lot of resources are going to be needed to purge the various agency databases and improve communication between the agencies. We think this is going to be problematic.

Employers need the right tools to verify a legal workforce, but we cannot have HR, and we should not have HR, be America's surrogate Border Patrol agents. Rather, employers are entitled to a clear answer to the query whether an employee is authorized to work, and be able to reply to that response.

We believe that Congress must transform the current paper-based verification process into a state-of-the-art electronic system. Specifically, we advocate a system that would verify identity through additional background checks and the voluntary use of biometric enrollment conducted by government-certified private vendors.

The system would be built upon background checks currently conducted by many employers. Our own survey shows that 85 percent of our members do employment verification checks, reference checks, to include forensic document examines and tailored data mining in publicly available databases. An individual's identity could be locked to biometric or other secure identifiers through the process. Employees would not need to present an identity card, just themselves.

Under our proposal, employers would be required to participate in one or two electronic employment verification systems. The first would be the current EEVS, but permitting employers to access the system via phone and internet. The second would be SEEVS, a more secure electronic employment verification system. The state-of-the-art system would identify, through additional background checks and voluntary biometric enrollment conducted by private employers.

This system, we think, would answer two important questions: Is the person identified by name, date of birth, and Social Security authorized to work? Is the person actually who he or she claims to be?

In the interests of time, I would like to conclude by encouraging Congress to look at this carefully. We are very concerned that in the rush to deal with immigration reform, which we believe needs to happen, that there is a push to just simply push this verification system through. And the word chaos, I thought, was apt in describing what we think is going to happen when this rolls forward.

Thank you.

[The prepared statement of Ms. Meisinger follows:]

Prepared Statement of Sue Meisinger, The Human Resource Initiative for a Legal Workforce, Society for Human Resource Management, Alexandria, Virginia

Mr. Chairman, Ranking Member Johnson, Members of the Committee. My name is Susan R. Meisinger and I am the President and CEO of the Society for Human Resource Management. I appear today on behalf of the Society for Human Resource Management. I am also the Co-chair of HR Initiative for a Legal Workforce. I am grateful for the opportunity to provide our views on this important issue.

The Society for Human Resource Management (SHRM) is the world's largest association devoted to human resource management. Representing more than 217,000 individual members, the Society's mission is both to serve human resource management professionals and to advance the profession.

The Human Resource Initiative for a Legal Workforce is a coalition of human resource organizations and business groups, representing thousands of small and large U.S. employers from a broad range of sectors. The HR Initiative includes SHRM, the American Council on International Personnel, the College and University Professional Association for Human Resources, the Food Marketing Institute, the HR Policy Association, the International Public Management Association for Human Resources, and the National Association of Manufacturers. Our objective is to improve the current employment verification process by creating a secure, efficient and reliable system that will ensure a legal workforce and help prevent unauthorized employment.

Our collective members represent the front lines on workforce verification, and therefore offer a crucial viewpoint on the matter. We fully support and are committed to the hiring of only work-authorized individuals through an effective, efficient electronic employment verification system.

We also recognize that the current employment verification system is in need of real reform. In fact, we believe verification is the lynchpin for true immigration reform. Unfortunately, the current paper-based employment verification system is inadequate to meet current and future demands, and current proposals before Congress fall far short of what is needed.

As the debate on immigration reform continues, we urge Congress to carefully consider the implications of any new employment verification system, keeping in mind that this is not just a debate about immigration reform, it is a debate about workplace management, which impacts all U.S. employers and all American workers, not just those who are foreign born.

My remarks will focus on the employment verification process established in the Immigration Reform and Control Act (IRCA) of 1986, the state of the current electronic verification system, the Basic Pilot Program that was enacted in The Illegal Immigration Reform and Immigrant Responsibility Act (IIRIRA) of 1996, as well as our proposal to create an effective electronic employment verification system in the effort to ensure compliance with immigration laws at the worksite, and to protect the civil rights and privacy of employees.

Mr. Chairman, under IRCA employers are required to review documents presented by employees within three business days of hire demonstrating identity and authorization to work in the United States. After reviewing these documents, employers are required to attest on Form I–9 that they have reviewed the documents and that they appear genuine and authentic. Under current law, 27 paper-based documents are available to employees to demonstrate work eligibility, with 12 different documents authorized under law to prove identity.

Even under the best of circumstances, HR professionals encounter numerous challenges with the employment verification requirements under IRCA. These include: maintaining the I–9 records when an employee presents a document that has an expiration date; verifying the authenticity, quality, and quantity of documents presented by an employee for work authorization and identification purposes; and managing the current I–9 process, which is burdensome and time-consuming.

According to *SHRM's 2006 Access to Human Capital and Employment Verification* survey, 60 percent of responding HR professionals indicated that they continue to experience problems with the current verification requirements of IRCA 20 years after its enactment. The most common challenge cited is ascertaining the authenticity of documents presented for employment (40 percent).

The current document-based system is prone to fraud, forgeries and identity theft, making it difficult, if not impossible, for an employer to differentiate between the legal and illegal worker in this process.

U.S. employers, whether large or small, cannot be expected to consistently identify unauthorized workers using the existing system, but they are liable for severe sanctions if these workers find their way onto the payroll. Conversely, they are subject to claims of discrimination if they question the validity of documents too much.

The proliferation of false or stolen documents can and does cause reputable employers to mistakenly hire individuals who are not eligible to work. At the same time, the lack of certainty and threat of government-imposed penalties may lead some employers to delay or forego hiring legal workers who are eligible. In either case, the costs are high for both U.S. employers and legal workers.

In an attempt to address the shortcoming of the paper-based system, Congress created the Basic Pilot program for employers to voluntarily confirm an employee's eligibility to work using an electronic verification system. Under the Basic Pilot program, employers are required to review an employee's identity and work authorization documents consistent with IRCA requirements, including completing all Form I–9 paperwork. Employers are then required to check each new employee's work eligibility using the electronic verification system.

The Basic Pilot system is supposed to respond to the employer within three days with either a confirmation or a tentative non-confirmation of the employee's work eligibility. In the cases of a tentative non-confirmation, a secondary verification process lasting ten days is initiated to confirm the validity of the information provided and to provide the employer with a confirmation or non-verification of work eligibility. Employers are not permitted to terminate individuals that have received a tentative non-confirmation until the employer has received a final non-verification or the ten-day period has elapsed.

Although the Basic Pilot has been operational since 1997, and despite the best efforts of the men and women who administer this program in the USCIS, we believe it is inadequate to meet the needs of all U.S. employers in the employment verification process. According to the Government Accountability Office (GAO), in June of 2005, only 2,300 out of 5.6 million U.S. employers participated in the Basic Pilot in 2004. Even with the relatively low participation rate, the GAO found that about 15 percent of all queries required additional verification because the automated system was unable to provide confirmation responses on the initial attempt.

In April 2007, the United States Citizen Immigration Services (USCIS) testified before the House Judiciary Subcommittee that that the total number of participating employers has risen to about 16,000 employers and that "over 92 percent of inquiries from employers receive an instantaneous employment authorized response."

However, these numbers represent only a fraction of the nearly 6 million employers in the United States. According to USCIS, if all employers were required to enroll in the Basic Pilot within 18 months, as called for by some proposals in Congress, USCIS would need to enroll approximately 20,000 employers a day. Expanding this system to cover all employers as proposed—absent federal certification that the system is adequately staffed and prepared to handle the increased workload—will undoubtedly cause confusion, harm productivity, and deny eligible workers employment opportunities.

Since a significant percentage of the Basic Pilot queries require human intervention, substantial resources will be needed to purge the various agency databases and improve communication between agencies. This problem is likely to be exacerbated if participation increases from 16,000 to all 6 million-plus employers. As we have seen in other aspects of immigration adjudication, a substantial increase in immigration-related caseload without corresponding increases in resources can lead to major processing delays. Using USCIS's own numbers of a 92 percent verification rate, millions of authorized employees' verification for employment could be in jeopardy.

As evidenced in several recent high profile situations, there are major concerns that the Basic Pilot's accuracy is severely limited by the proliferation of fraudulent identity documents. This is because the Basic Pilot system does not verify the authenticity of the identity being presented for employment purposes, only that the identity presented matches information in the Social Security and DHS databases.

In testimony to House Judiciary Subcommittee in April, Jack Shadley, Senior Vice President for Human Resources for Swift & Company detailed the shortcomings of the "Basic Pilot" employment verification system. Despite the company's hiring processes, which included participation in Basic Pilot, the government raided six Swift production facilities on the morning of December 12th, 2006, and detained 1,282 employees. Many were using stolen identities that could not be detected by Basic Pilot. This event cost the company more than $30 million and disrupted communities that Swift has worked hard to enrich. As Mr. Shadley stated in his testimony:

"It is particularly galling to us that an employer who played by all the rules and used the only available government tool to screen employee eligibility would be subjected to adversarial treatment by our government. These ICE raids once again highlight significant weaknesses in the Basic Pilot program."

In addition to concerns with premature expansion of the Basic Pilot, several Congressional proposals also expose employers to liability for actions beyond their control, such as the actions of subcontractors. We strongly believe that U.S. employers should be liable for their own hiring decisions, not those made outside their control. Enforcement needs to be vigorous and fair, and should focus on employers that blatantly ignore the law as opposed to employers who commit paperwork or technical violations in their attempt to comply.

Employers need the right tools to verify a legal workforce. However, HR cannot—and should not—be America's surrogate border patrol agents. Rather, employers are entitled to an unambiguous answer to the query whether an employee is authorized to accept an offer of employment. Unfortunately, mandating the current Basic Pilot system will not meet the needs of employers or employees.

We believe that Congress must transform the current paper-based verification process into a state-of-the-art electronic system that is accurate, reliable, cost-efficient, easy-to-use, and shares responsibility among government, employers and employees. Specifically, we advocate a system that would verify identity through additional background checks and the voluntary use of biometric enrollment conducted by government certified private vendors. According to *SHRM's 2006 Weapons in the Workplace*, 85 percent of responding HR professionals indicated their organizations conduct background checks of potential employees.

This system would build upon background checks currently conducted by many employers, to include forensic document examination and tailored data mining in publicly available databases. An individual's identity could be "locked" to biometric or other secure identifiers through this process. Employees would not need to present a card as some have advocated, just themselves.

Under our proposal, employers would be required to participate in one of two electronic employment verification systems:

> EEVS—A completely electronic employment verification system (EEVS) which improves upon the current Basic Pilot system and permits employers to access the system via phone and internet. Employers would verify identity by visually examining a limited number of documents presented by the employee. Employers would verify work authorization by submitting employee data to the SAVE system. The verification process can be initiated either post offer or acceptance of a job by an employee but prior to the commencement of work or within the first 3 days after work commences. The databases feeding into the SAVE system must be upgraded to ensure all information is accurate and updated and that secondary verifications are completed within 10 days. Employers would continue to make subjective determinations that the person presenting the documents is who he claims to be and that the documents are valid on their face. The current I–9 form would be eliminated. Employers in this system would be subject to the current range of enforcement efforts and penalties.
>
> SEEVS—A more secure electronic employment verification system (SEEVS) that guard against identity theft would be available to employers on a voluntary basis. This state-of-the-art system would verify identity through additional background checks and voluntary biometric enrollment conducted by private vendors. The employee's work authorization would continue to be verified through the SAVE databases. By eliminating subjective determinations of work authorization documents, this system will eliminate discrimination and simplify enforcement. There will be only two enforcement questions for the government: 1) Did you check every employee through the system in a fair and equal manner? 2) Did the employer make his/her hiring decisions consistent with information they received through the system? Employers participating in this system would be deemed to be in compliance absent a showing of bad faith.

The proposed SEEVS system would prevent identity fraud by automatically recognizing an individual based on measurable biological (anatomical and physiological) and behavioral characteristics. The new system would be able to answer two vital questions:

1. Is the person identified by name, date of birth, and social security number **authorized** to accept the employment being offered?
2. Is the person actually who he or she claims to be?

We also believe that any such secure electronic employment verification system as described above needs to meet standards set by the National Institute of Standards and Technology (NIST) from a technology and a privacy standpoint. The SEEVS model for prevention of identity theft lies in authorizing competing private entities, certified by the Government with the involvement of NIST, to develop and conduct the process necessary to verify the identity. The privately held databases would be protected from disclosure by law and held in a segregated fashion that would prevent linking of identity to biometrics without the enrolled person presenting his or her biometrics as the key.

We do not believe a biometric card is necessary to have an effective employment verification system. A new biometric card, such as a Social Security card, would cost billions of dollars to create, foster visions of a national ID card, and would tax the current capabilities of the Social Security system. Finally, as we have discussed and has been demonstrated before through cases such as the Swift, government-issued identity and work authorization cards eventually can be counterfeited by those who want to circumvent the system.

If adequately funded and fairly administered, SHRM and the HR Initiative believe this new system could eradicate virtually all unauthorized employment—thereby eliminating a huge incentive for illegal immigration. It will also eliminate discrimination by taking the subjectivity out of the verification process.

Finally, we strongly recommend that the Federal Government, specifically the Department of Homeland Security, take sole ownership of enforcing immigration laws at the worksite. Recently, partially due to an understandable frustration on the part of state and local governments over the lack of immigration control, many jurisdictions have enacted their own laws on employment eligibility verification. With all due respect to these states and municipalities, it is the U.S. Congress that has plenary authority, and the expertise, to deal with this issue. Moreover, it is extremely hard on employers, especially ones with presence in several states, to keep up with the various requirements. Ironically, while law-abiding employers risk exposure because of inadvertent mistakes or confusion over the different and possibly contradictory requirements, unscrupulous businesses can continue to hire off the books with virtual impunity. We suggest that worksite enforcement must be vigilant, and that the Federal Government must hold all employers to the same standards and same set of requirements.

True employment verification is the only way to ensure fair and equitable treatment for those individuals who should have access to legitimate jobs. It is essential for a legal workforce and for America's national and economic security.

Both SHRM and the HR Initiative coalition look forward to working with the committee on a new verification system that is effective, secure, easy to use, and in which both employees and employers can place their trust.

Chairman MCNULTY. Thank you very much.

We have two votes on the House floor. Since this is a 15-minute vote and we are just at the beginning of it, we are going to try to hear Mr. Neumann's testimony, perhaps Mr. Rotenberg. We will get as far as we can before we have to run over to vote. Then we will do two votes back to back and reconvene here as quickly as possible, hopefully only detaining for a 15-minute break.

So, Mr. Neumann may start.

STATEMENT OF PETER G. NEUMANN, PRINCIPAL SCIENTIST, COMPUTER SCIENCE LABORATORY, SRI INTERNATIONAL, MENLO PARK, CALIFORNIA, ON BEHALF OF THE U.S. PUBLIC POLICY COMMITTEE OF THE ASSOCIATION FOR COMPUTING MACHINERY

Mr. NEUMANN. Thank you very much for the invitation to be here. It is a very important topic, and I hope I can shed some constructive background on it.

I am speaking on behalf of the USACM, the U.S. Public Policy Committee of the Association for Computing Machinery, which is a nonprofit group, over 80,000 people dedicating to constructive use

of computer technology. I also speak as someone who has over 50 years of experience in research and development, and a sideline interest of collecting stories on things that failed.

If you ask me questions about it, I will talk about the IRS failure, the air traffic control modernization failure, the FBI virtual case file problems, the deadbeat dads, and so on. There are just an enormous number of cases in which large systems collapsed. The first two of those were $4 billion efforts that were eventually canceled after it was recognized that they could never succeed.

The task that you are embarking on with a modernization or upgrading of EEVS reminds me of a metaphor, because if you look under the eaves, you typically see rodents and termites and dry rot from roof leaks in a badly built house, or even some of the well-built houses. You also have ongoing maintenance problems of having to clean out the gutters, and the liability lawsuits when the maintenance guy falls off the ladder.

[Laughter.]

Mr. NEUMANN. So it is a much bigger problem than it is normally conceived. When somebody tells you, yes, we can build this system, I will give you hundreds of examples of things that have gone wrong over the years, and reasons why most of the systems don't work.

If Ranking Member Johnson will ask me about tamper-proof systems, there are no such things. There might be some tamper-resistant ones and tamper-evident systems, but some of my colleagues can break just about anything that has ever been built.

I would like to very briefly outline some of the more critical issues. In my written testimony, I go through considerable detail on things that have to be fixed before this could possibly work, assuming that it ever possibly could work.

In particular, the sensitive information needs to be protected. This is an extremely different problem—difficult problem, rather—because many of the privacy problems are extrinsic to the system. They involve insiders who have legitimate access and who can misuse that access, for example. They are based on computer systems that are not secure, which means, since you put it on the Internet, you have a great many problems.

Authentication: Passwords are mentioned. Passwords are an extremely weak form of protection. We need something much greater than that, especially when we start sharing across the Internet.

One of the biggest problems that you are going to face is the scalability problem. I will give you two examples. The simplest example is the man who starts out with a hamburger stand and expands it into a worldwide chain. The logistic problems, the financial problems, the health problems, and so on are orders and orders of magnitude more complex. It does not scale in any reasonable sense.

A more computer-related example is taking MS DOS, which had no security in it whatsoever, and suddenly saying, we are going to build a variant of that that is accessible to everybody in the world over the Internet. There is no security in the Internet. There is very little security in some of the systems that we are dealing with. The result of all of that is that we are living in a world where you cannot really guarantee anything about protection.

Authentication and accountability are absolutely fundamental. Oversight. Audit trails. It represents an enormous problem, but then you have the problem of who can look at the audit trail, who can modify the audit trail. It should never be modifiable, of course.

You then have all of the level playing field issues that smaller organizations may be very seriously disadvantaged, especially by the realtime requirement, where they don't even have access to computers at the time that they need it.

So, I think the bottom line here is that experience has taught us over the years, for those of us who have been deeply involved in building systems and analyzing them and analyzing why they don't work, that systems like EEVS are subject to an enormous number of pitfalls. those are anticipated from the very beginning, they can never be overcome in an incremental way.

I think the real problem here is that we tend not to anticipate all of the problems. We said, oh, let's go and build this thing. We are told that it can work. Our subcontractors are all very happy to take our money and build it. And, in fact, when it doesn't work and it get canceled years later, the same guys go off and build another system.

So, I think the problems here are ones that you really need to look at proactively before you engage in any legislation. So, on one hand, as a technologist, I can say, well, I could build something that might work in the small. However, when you scale it up to the massive number of uses over the Internet, where they are accessible from anywhere in the world, from any hacker, cracker, terrorist, or anybody else who can either bring down the system or access it, you have a totally different ball game than the one that you think you are dealing with.

Thank you very much for inviting me, and I look forward to your questions.

[The prepared statement of Mr. Neumann follows:]

Prepared Statement of Peter Neumann, Principal Scientist, Computer Science Laboratory, SRI International, Menlo Park, California, on behalf of U.S. Public Policy Committee of the Association for Computing Machinery

Security and Privacy in the Employment Eligibility Verification System (EEVS) and Related Systems

This testimony addresses some of the potential pitfalls that should be considered when planning systems with extensive computer database applications containing personal information, such as the Employment Eligibility Verification Systems (EEVS). Many of these concerns are also applicable to related programs such as US–VISIT and REAL–ID and to peripheral systems that may depend on EEVS or result from interconnections among those other systems. Widespread problems have arisen in efforts to develop complex systems that must satisfy critical requirements for security and privacy; these problems are also considered. Furthermore, there is a pervasive tendency to overestimate the benefits of computer-related technologies as would-be solutions to societal problems. We should not expect easy technological answers to inherently difficult problems. People are almost always the weakest links, although in many cases the system design and implementation create further weak links. A deep awareness of the long-term problems is essential before adopting legislation that might promise to help in the short term.

1. Introduction

Thank you, Chairman McNulty and Ranking Member Johnson, for the opportunity to testify at today's hearing exploring issues related to proposed changes to the EEVS. I commend you for exploring the policy and technology issues associated

with current proposals to expand and make this program mandatory. The computing community has often seen problems that resulted from policies established without careful consideration of the inherent limitations of technology. This can result in serious technical and social hurdles, and can lead to problems that are difficult to remediate once they have occurred, but that could have been prevented proactively. We hope that your efforts can help to avoid such difficulties.

As Principal Scientist in the Computer Science Laboratory at SRI International (formerly Stanford Research Institute), where I have been since 1971, and as someone with 54 years of experience related to computer and communication technologies, I have explored the intersection of technology and policy in numerous contexts, with a particular focus on system trustworthiness, security, and privacy issues. These areas are particularly relevant to the technology and policy nexus because privacy and equal treatment under law are fundamental rights; technology can at the same time help secure and also undermine those rights—depending on the policies and practices for its use. Privacy and security are inextricably linked. One cannot ever guarantee complete privacy, but the difficulties are severely complicated by systems that are not adequately secure. Creating complex systems that are dependably trustworthy (secure, reliable, survivable in the face of many adversities, and so on) remains a grand challenge of computer science. As we review a proposed expansion to the EEVS, USACM sees a number of issues that should be explored, debated, and resolved before adopting this massive new system for identity verification.

This statement represents my own personal position as well as that of the Association for Computing Machinery's (ACM) Committee on U.S. Public Policy (USACM). ACM is a non-profit educational and scientific computing society of more than 80,000 computer scientists, educators, senior managers, and other computer professionals in government, industry, and academia, committed to the open interchange of information concerning computing and related disciplines. The Committee on U.S. Public Policy acts as the focal point for ACM's interaction with the U.S. Congress and government organizations. It seeks to educate and assist policy-makers on legislative and regulatory matters of concern to the computing community. (See http://www.acm.org and http://www.acm.org/usacm.) A brief biographical paragraph is appended.

2. Issues of Specific Concern in the EEVS

The information transmitted to and stored in EEVS includes all of the primary personal identifiers in the U.S. As such, any compromise, leak, theft, destruction, or alteration of this data would have severe consequences to the individuals involved, including, but not limited to, identity theft and impersonation. It is thus essential that the system be designed, constructed, and operated with the quality of protection that is essentially that required for classified national security information.

2.1. Transmission of Information

Any legislation requiring the transmission of personal information across the Internet should require secure transmission of this information. Employers and agencies participating in the program should be required to have strong encryption, strong authentication, or even elementary security (such as Secure Socket Layer, SSL) for transmissions to and from employers. Calling out such specific technologies and details would be inappropriate for statutory language; however, the legislation should include performance-based standards for security that limit the exposure of personal information and provide accountability for every step in handling and processing this information. This will make it clear to agencies that implement the system, and employers who use the system, that the security of personal information is as valued by policymakers as the reliability and timeliness of responses. In the case of EEVS and many other important systems, it is much more important to have continuing trust in the security and accuracy of the information rather than to get results in the shortest possible time.

We recommend that legislation require that the system be designed to protect the integrity and confidentiality of information, that an independent security review evaluation be conducted before the system is deployed, and periodically after deployment, and that the results of these evaluations be made public. The systems and their operation should be required to follow Fair Information Practices. See also USACM's recommendations for database design (http://www.acm.org/usacm/Issues/Privacy.htm).

We further recommend that the legislation require security breach notification: if administrators become aware of any breaches that could potentially affect personally identifiable information, then they must publish a disclosure and must notify

all individuals who may be affected. Congress could model this after various state disclosure laws, such as one recently passed in California.

We also recommend that individuals be notified whenever someone accesses their records. The cost would be small, relative to other costs of the system: one letter or e-mail per job application.

2.2. Accountability for Access to Information

Accountability from the end user to the system administrator is vital in a computing system for ensuring the integrity of the system. If people are not held accountable for their actions, then policies intended to curb abuse will be undermined as users circumvent policies to make their jobs easier. One way of improving accountability in any computing system is by requiring strong user authentication and access controls coupled with thorough tamper-resistant and tamper-evident logging of all activity. In addition, all system accesses should log who accessed which records, and individuals whose information is stored should be informed who has accessed their records. This would then allow concerned individuals to detect misfeasance and improper access to their records. Each employer should identify a compliance officer (distinct from EEVS users). The system should automatically detect unusual user behaviors (to the extent technically feasible) and report them to compliance officers.

Some strong controls are clearly needed to explicitly bind the access of a particular request to a specific authorized requestor acting in a specific role for a specific employer. The same controls should be applied to the operators of the system. Names, titles, and SSNs of authorized system users are not enough.

Access controls are also critical if individual employees are going to access the system to check their own information. Procedures and policy need to be in place to restrict employees' access to only their own information. The ability to check the accuracy of one's own information is very important. However, such accesses also need to be controlled and audited, at least as extensively as the accesses on behalf of an employer—particularly to be able to identify systematic misuses.

2.3. Scalability

To date the system has functioned as a pilot program. The pilot has about 8,600 employers (June 2006 number) registered, with about half of those employers considered active users. This is out of about 5.6 million employers (as of 2002) that would eventually use the system once the law is fully implemented. Just because it seems to work for a small number of employers does not imply that it would work for all employers. The scalability of EEVS is a very serious architectural issue, because it will have to handle at least a thousand-fold increase in users, queries, transactions, and communications volumes. As a general rule, each time a system grows even ten times larger, serious new technical issues arise that were not previously significant.

At present, eight percent of confirmation requests cannot be handled immediately. This percentage needs to be reduced significantly as the number of employers increases. This would reduce the frustration with the system as well as the additional time required for manual confirmation for those records that could not be immediately verified. The additional human resources and associated costs necessary to handle this burden must be taken into account and included in budgets.

In general, it is risky to operate a system outside its intended design capacity and rely upon it to work under all circumstances, unless it has been carefully designed and implemented with scalability specifically in mind. Issues relating to inadequate scalability could completely compromise the effectiveness of the resulting system.

2.4. Accuracy of Information

The system has weaknesses about the accuracy of information presented to the system by an employee or employer as well as the accuracy of the underlying databases.

Speaking to the first kind of inaccuracies—fraudulent documents—the GAO has indicated that the Basic Pilot cannot effectively detect identity fraud. Proposals to add a digitized photograph to any employment authorization document would help make sure the employer could confirm that the photograph on the documents matched the employee presenting them. However, it is unclear how much this would reduce identity theft.

The inevitable cat-and-mouse game that always occurs in security (an ever upward escalating spiral in measures and countermeasures) is likely to occur between the security control and those seeking to commit fraud. As it becomes known that photo verification is a security feature, obtaining official documents under false pretenses will become more valuable. This could be done by bribing an insider or providing fraudulent documents to obtain the identification. The fraud is simply moved

to a different part of the system. We also note that requiring REAL–ID, as envisioned by the DHS's rules for implementation of the REAL–ID system, will not solve the insider threat problem. This was pointed out in USACM's comments on the REAL–ID rulemaking. (See the "insider threats" heading in USACM's comments: http://www.acm.org/usacm/PDF/USACM_REAL_ID_Comments_FINAL.pdf)

Carefully developed standards for digital photographs are necessary—much like those for driver's licenses—although they will not be sufficient for the prevention and detection of forgeries.

Serious areas of concern also exist for the second kind of inaccuracies—bad information in the underlying databases, delays in entering or revising information, and inconsistencies and name confusions among different databases. The Social Security database is known to have a high number of errors in name matches, as well as some duplicate numbers. For example, the Social Security Administration's Office of the Inspector General recently estimated that the SSA's 'Numident' file—the data against which Basic Pilot checks worker information—has an error rate of 4.1 percent. If each of 5.6 million employers made a query of a different potential applicant, that percentage suggests that on average more than 200,000 of them might get false responses.

The other databases the system will rely on will have similar issues. We certainly recognize and endorse the importance of provisions that allow individuals to check the correctness of information in the system that relates to them. However, a better defined process of correcting any erroneous information would be the necessary next step in improving the reliability of these databases, and the system as a whole. The risks of incorrect information are considerable, although establishing standards and procedures for accuracy to avoid those risks and to remediate errors and malicious misuse is an extremely difficult task. Numerous potential employees could be wrongly denied employment because of inaccurate records, if this problem is not addressed.

Risks of identity theft and privacy violations are also present—for example, if unauthorized or surreptitious accesses, or even changes, can be made. Explicit provisions are needed to protect employees and potential employees from adverse consequences of database and data entry errors.

Employers should also be held accountable for misuse of their blanket access privileges, such as using the data for running credit and insurance checks, engaging in blackmail, and other inappropriate purposes.

USACM encourages Congress to consider undesirable effects of false-positive and false-negative results. (A false positive is when a response indicates someone may be hired, only to be overturned later. A false negative would be when a response indicates someone has not been confirmed, only to be shown later to be incorrect.) Given the possibilities for error, identity theft, and system failure, employers should be protected from penalties when acting in good faith, and potential employees should be protected against discriminatory behavior. This is a policy issue rather than a technical issue, but directly arises from using an imperfect system as an arbiter.

It must be possible for authorized staff, as well as potential employees, to challenge incorrect EEVS data and determinations.

2.5 National ID System Concerns

Although there is no national ID card requirement attached to the EEVS, the connections to various databases are similar to the REAL–ID system currently proposed by DHS. If the EEVS does store query information or holds duplicates of information gleaned from the databases it interacts with, then it will have the appearance of a national identity system. As the existence of a national ID is not authorized by the proposed Senate immigration reform legislation, the Department will need to take care to avoid even the appearance of providing such documentation. The tradeoffs here are extremely complex, but are probably already being discussed in other testimony and other hearings.

2.6. Accessibility Issues

The potential lack of timely and highly available remote access to EEVS is another concern. Many small employers may not have Internet access or even computers that would allow them to have access. Examples might include small shop owners who want to hire clerks, and farmers who want a few hired hands. Furthermore, access via slow-speed dial-up connections is not likely to encourage consistent system use. Real-time confirmation of employability is less likely to occur consistently in such cases, and in cases of loss of computing or communication connectivity.

Perhaps even worse, poorly protected systems and poorly trained users will probably fall victim to ubiquitous security vulnerabilities and malicious software on the

Internet. Many casual or novice computer system users could become unsuspecting victims of scams, phishing attacks, identity theft, and so on—as a consequence of being forced to add computing and connectivity to support use of EEVS.

It is also a certainty that criminal elements will craft phishing e-mail appearing to originate from the Department of Homeland Security. This would include pointers (URLs) to what appear to be DHS websites with the DHS seal and apparent certificates that are essentially indistinguishable from the real websites. Unsuspecting users who visit these sites might then be victimized, resulting in significant financial losses and other serious consequences that typically result from identity thefts. Skilled identity thieves are likely to be able to scam the system itself more readily than authorized individuals can protect themselves or correct data errors.

A further problem is that many of the computer systems used to access EEVS may not have adequate security, and may have been compromised. Unfortunately, the security of EEVS itself may be subverted by the lack of security in other connected systems (which potentially implies the entire Internet).

For these reasons, despite its possible benefits, EEVS might actually make identity theft easier and at the same time make remediation and recovery more difficult.

3. Broader Concerns

The current state of the art in developing trustworthy systems that can satisfy critical requirements such as security, reliability, survivability, and guaranteed real-time performance is truly very poor. This is not a newly recognized problem, and was well documented in 1990 in a report, Bugs in the Program, by James Paul (Subcommittee on Investigations and Oversight of the U.S. House Committee on Science, Space, and Technology). Subsequently, I presented four testimonies (1997, 1999, 2000, and 2001) for various House committees—each of which suggested that the overall situation had incrementally gotten worse. Of specific relevance to this testimony was my written testimony for the House Subcommittee on Social Security, The Social Security Administration: PEBES, Identity Theft, and Related Risks, on May 13, 1997—now more than 10 years ago. Similar conclusions appear in my testimonies for Senate committees (1996, 1997, 1998). (These testimonies are all online, with links from my website, http://www.csl.sri.com/neumann.)

Software development fiascos abound—including many highly visible projects that have been late, over budget, or indeed abandoned after many years and large expenditures. My Illustrative Risks compendium index (http://www.csl.sri.com/neumann/illustrative.html) cites numerous examples such as the IRS and Air Traffic Control modernization programs and the FBI Virtual Case File, to cite just a few. See also the PITAC report, Cyber Security: A Crisis of Prioritization: http://www.nitrd.gov/pitac/reports/20050301_cybersecurity/cybersecurity.pdf.

Privacy problems are also manifold, and becoming increasingly complex as ubiquitous dependence on computerized databases increases. The extent to which computer systems and databases can enforce privacy policies is severely limited by the absence of meaningfully secure systems, and by the number of privacy violations occurring outside of the confines of the computer systems. Correctness and timeliness of the data are also major concerns.

Several problems with identity management must be addressed. The existing infrastructure is riddled with security and reliability vulnerabilities, and is not sufficiently trustworthy. Because many of the privacy problems are related to total systems (encompassing computers, communications, people, and procedures), they cannot be adequately protected by technological approaches alone. Identities are typically subject to masquerading and spoofing. Name confusions such as alternative spellings and aliases cause major confusions. Authentication is often compromised by ″social engineering″ and other nontechnological bypasses. Authorization is typically inadequately fine-grained (and worse yet, often supposedly all-or-nothing, but bypassable). Blanket authorization should be avoided, observing the Principle of Least Privilege—under which access authorizations should be restricted to just what is needed to accomplish that intended task rather than being overly broad.

It is also worth noting that there are cases where identities need to be masked. Examples include individuals protected under the Federal Witness Protection Program, individuals granted asylum from other countries and given new identities, undercover intelligence agents, undercover law-enforcement agents working criminal cases, and sky marshals. (Note that the Transportation Security Administration somehow lost the employee personnel records for 2003–2005.) All of these people need to have verifiable identities that stand up to any scrutiny, online or otherwise. Exposure of their real identities may result in their violent deaths, compromises of national security, and possible violence to their friends and families. Those individuals will likely need employment under their alternate identities, and it must be ensured that any system implemented for EEVS does not endanger their cover iden-

tities. The more that databases become cross-linked, the more difficult it becomes to prevent errors and leakage of such sensitive information. Furthermore, such linkages make these database systems higher-value targets for criminals.

The requirement of masking, aliasing, or otherwise providing alternative identities seems to create a fundamental conundrum: maintaining the accuracy of a critical database while simultaneously undermining its accuracy may impair the accuracy of other data in the process.

Past legislative efforts for improving accuracy and integrity of public databases have caused serious problems with the viability of other systems. For example, the Help America Vote Act mandated statewide-centralized voter registration databases that must verify the accuracy of records by matching them with drivers' license records. States such as California found that the data-matching requirements in practice led to high rejection rates in some counties, depending on how strictly the data was interpreted across databases. This had the effect of reducing, not improving, voter registration list accuracy, because legitimate voters were removed from the rolls because of address typos and name variants.

4. Conclusions

The problems identified in this testimony are fundamental in the context of EEVS-like systems. There are many risks. Essential concerns for system and data security, system and data integrity, and individual privacy must be anticipated from the beginning and reflected throughout design, implementation, and operation. Many potential slippery slopes must also be anticipated and avoided. Privacy requires a real commitment to creating realistic policies and enforcing them.

Experience has taught us that the design of information systems is subject to many pitfalls that can compromise their effectiveness. If EEVS is not appropriately implemented, it could—like many past systems—be subject to problems that include, but are not limited to, the following:

- Difficulties in maintaining accuracy, correctness, and timeliness of the database
- Inconsistencies among widely distributed systems with distributed data entry
- A popular tendency to place excessive faith in the trustworthiness of the system's responses
- A common tendency to place excessive faith in the infallibility of identification, authentication, and access controls to ensure security and privacy
- The lack of scalability with respect to ever-growing enormous databases, massive numbers of authorized users, and consequent communication and access limitations
- The complexity of requirements imposed by noncompromisible auditing and accountability, both of which introduce further problems with respect to system security and integrity and with respect to data privacy
- The complexity of audit trails and notification of accesses to audit trails themselves
- The risks of exacerbated problems that result from mission creep—as further applications tend to be linked to the originally intended uses, and as control of the above factors becomes less possible
- Similar risks related to feature creep, with or without any oversight and audit mechanisms.
- "Piggybacking" by other agencies—e.g., law enforcement and DHS might want to place silent-hit warnings (as was considered in the late 1980s for the National Crime Information NCIC system) that would inform them who was seeking information for anyone who was under surveillance. Linkages with databases for deadbeat parents, student loan defaulters, and other applications might also be contemplated. Each such connection would expand the exposure of the system and the dangers of incorrect data and data leakage.

Congress should establish clear policies and required outcomes, rather than prescriptive or detailed technical processes or systems. The technical challenges to achieving the policies and outcomes should be fully documented in the Congressional Record of the legislation.

Considerably more focused research is needed on total-system approaches that address identity authentication, authorization, and data protection within the context of overall system architectures for security and privacy. (For example, some promising new developments enable the use of cryptography to enable certain queries to be answered without requiring decryption and release of excessive information in violation of the Principle of Least Privilege. These techniques appear to be significantly less subject to misuse, including insider misuse.) Such approaches may be more effective than trying to rely on biometric and other devices whose effectiveness may be compromised by technological or operational flaws in the systems in which

they are placed and errors in human judgment. Finally, incentives are needed to ensure that research and innovative prototypes are relevant to the real-world problems and to ensure that these advances find their way into the development and operation of practical systems.

Although similar comments can be made about REAL–ID and any other national identification systems, all of these concerns are specifically relevant to systems such as EEVS.

We have not attempted to be complete here, but rather to focus on the main issues. There are many relevant reports of the Government Accountability Office, the National Research Council, and other sources that I hope you have already seen. Whereas USACM and I speak from a technical perspective, we recognize the political imperatives regarding immigration and employment. We urge the Congress to focus on creating the right incentives for operators and employers that maximize achievement of our immigration laws and each citizen's right to work while minimizing privacy invasion, ID theft, and criminal activity. In this effort, technology should be seen as a supporting block, not the keystone of the arch.

We look forward to any further questions that might arise from your reading of this written testimony or from my oral testimony.

Acknowledgments

I am particularly grateful to Cameron Wilson (ACM Director of Public Policy), David Bruggeman (USACM Public Policy Analyst), Eugene Spafford (USACM Chairman, and Professor at Purdue University), Jim Horning, and many other members of USACM for their generous help in my preparing this testimony on rather short notice.

Contact Information

Peter G. Neumann
SRI International, Computer Science Laboratory
Menlo Park CA 94025–3493
Neumann@CSL.sri.com
http://www.csl.sri.com/neumann

Personal Background Information

Peter G. Neumann (Neumann@CSL.sri.com) has doctorates from Harvard and Darmstadt. His first technical employment was working for the U.S. Navy in the summer of 1953. After 10 years at Bell Labs in Murray Hill, New Jersey, in the 1960s, during which he was heavily involved in the Multics development jointly with MIT and Honeywell, he has been in SRI's Computer Science Lab since September 1971. He is concerned with computer systems and networks, trustworthiness/dependability, high assurance, security, reliability, survivability, safety, and many risks-related issues such as voting-system integrity, crypto policy, social implications, and human needs including privacy. He moderates the ACM Risks Forum (comp.risks), edits CACM's monthly Inside Risks column, and is the Chairman of the ACM Committee on Computers and Public Policy (ACM–CCPP), which serves as a review board for RISKS and Inside Risks and is international in scope. He is also a member of USACM, which is independent of ACM–CCPP. He created ACM SIGSOFT's Software Engineering Notes in 1976, was its editor for 19 years, and still contributes the RISKS section. He has participated in four studies for the National Academies of Science: Multilevel Data Management Security (1982), Computers at Risks (1991), Cryptography's Role in Security the Information Society (1996), and Improving Cybersecurity for the 21st Century: Rationalizing the Agenda (2007). His book, Computer-Related Risks (Addison-Wesley and ACM Press, 1995), is still timely—including many of the problems discussed above. He is a Fellow of the ACM, IEEE, and AAAS, and is also an SRI Fellow. He received the National Computer System Security Award in 2002 and the ACM SIGSAC Outstanding Contributions Award in 2005. He is a member of the U.S. Government Accountability Office Executive Council on Information Management and Technology, and the California Office of Privacy Protection advisory council. He has taught courses at Darmstadt, Stanford University, the University of California at Berkeley, and the University of Maryland. Neumann chairs the National Committee for Voting Integrity (http://www.votingintegrity.org). See his website (http://www.csl.sri.com/neumann) for prior testimonies for the U.S. Senate and House and for the California state Senate and Legislature, publications, bibliography, and further background.

Dr. Neumann is Principal Investigator for two SRI projects that are relevant to this testimony:

- Privacy-Preserving Credentials, one of several subcontracts from Dartmouth College, Assessable Identity and Privacy Protection, funded by the Department of Homeland Security, 2006–CS–001–000001–02, FCDA #97.001. The SRI project is part of a collaborative team project jointly with the University of Illinois at Urbana-Champaign, Cornell, Purdue, and Georgia Tech. The project is contributing some highly innovative cryptographic research and extensive system experience to the application of practical techniques for advanced identity management with demonstrations of applications that will include health care and finance but that have significant relevance to identity management generally.
- A Center for Correct, Usable, Reliable, Auditable and Transparent Elections (ACCURATE), NSF Grant number 0524111. ACCURATE is a collaborative effort with colleagues at Johns Hopkins, Rice, the University of California at Berkeley, Stanford, the University of Iowa, and SRI. It is examining techniques and approaches for voting systems, with particular emphasis on security, integrity, and privacy. SRI

Neumann contributes to the following DHS project:

- Cyber Security Research and Development Center (CSRDC), Department of Homeland Security, Science and Technology Directorate, DHS Contract HSHQDC–07–C-0006 to SRI International. CSRDC is providing extensive support for S&T Program Manager Douglas Maughan's R&D program. (http://www.csl.sri.com/projects/csrdc and http://www.cyber.st.dhs.gov)

Chairman MCNULTY. Thank you very much.

The Members will now run over to the House floor to vote. There are 5 minutes left on this vote, and the next vote will be directly afterward, so we should be able to vote and hopefully only be gone for 15 minutes. When we return, we will hear from Mr. Rotenberg, and then allow for questions. Thank you for your patience.

[Recess.]

Chairman MCNULTY. The hearing will come to order. Sorry for the delay. We know that your time is very valuable, and we very much appreciate the fact that you are spending some of it with us here today.

We have heard from the first four witnesses on this panel, and we will now hear Mr. Rotenberg.

STATEMENT OF MARC ROTENBERG, EXECUTIVE DIRECTOR, ELECTRONIC PRIVACY INFORMATION CENTER

Mr. ROTENBERG. Thank you very much, Chairman McNulty and Ranking Member Johnson, Members of the Subcommittee. Thank you for the opportunity to testify today.

My name is Marc Rotenberg. I am Executive Director of the Electronic Privacy Information Center. We are a public interest research organization here in Washington, D.C. We track emerging privacy issues. We have also frequently been before the Subcommittee to discuss the privacy impact of proposals that involve the use of the Social Security number and SSA records.

We recently did a detailed report on the employment verification systems that are contemplated in both the Senate and the House bills. That report is simply titled, "National Employment Database Could Prevent Millions of Citizens from Obtaining Jobs." I would like to add that it be included in the hearing record as part of my statement, if that is okay.

Chairman MCNULTY. No objection.

Mr. ROTENBERG. Thank you. I would like to today highlight the key findings of our report. The central conclusion that we reached is that the employment verification system has significant weaknesses. It will pose enormous burdens for employers, and put the privacy rights of American workers at substantial risk.

It will also give the Federal Government an extraordinary amount of new power over the lives of Americans, as well as greatly expand the role of the Department of Homeland Security in the American labor force.

I want to say a word about the Department of Homeland Security. As Mr. Johnson mentioned earlier, there is, of course, this very significant concern about the misplaced disk drive that contained the employment records of 100,000 TSA employees who had been hired between January 2002 and September 2005. I think it is important to understand the significance of this particular incident.

You have heard a great deal of testimony this morning about the problem of record accuracy. No doubt, if you scale up the Basic Pilot Program, the number of workers who may face determinations that say they may not be eligible to work unless they, in effect, clear their status is going to grow dramatically.

You haven't heard very much about new threats to privacy and security that these proposals raise. I believe that is a key problem that the Department of Homeland Security has helped identify because by misplacing the records that they did on the TSA employees, they have, in effect, brought attention to the problem of identity theft and security breaches, which are significantly increasing in the United States. In fact, the Federal Trade Commission has reported that identity theft is now the number one concern of American consumers. A big contributor to that problem is the extraordinary collection of personal information.

I will say a few words about the current design of this system. As other witnesses have noted earlier, the proposal to consolidate so much personal information in these centralized government databases does significant increase the risks to privacy.

Now, it is our view that the SSA has done a good job over the years trying to narrow the use of the Social Security number and Social Security records for the appropriator legislative purposes. Of course, when another agency comes forward and proposes new expanded uses of the Social Security number, then new privacy issues arise.

Now, both bills state that the database access will be limited to authorized users only. However, it is very easy to understand the circumstances under which others could get access to these record systems. Dr. Neumann has described the various ways under which computer systems can be compromised through weak security. It is also a result of the insider access to the record systems that would result as well.

I would like to say a word about the role that the REAL ID act plays in the legislation that is under consideration in both the Senate and the House. As you know, there is a lot of opposition to the implementation of the REAL ID Act. The statute, which was passed in February of 2005, went forward without a vote, without a public hearing.

Since that time, more than a dozen states have passed bills to oppose the implementation of REAL ID in their states. Four states have actually said that they would not have a REAL ID requirement.

Now, this is a fact worth keeping in mind as you look at these legislative proposals because the Department of Homeland Security is proposing that the REAL ID document be used as one of the ways to establish employment eligibility. In fact, the Senate bill would make non-REAL ID-compliant documents of no use for establishing employment eligibility by the year 2013, which means you could actually have a situation, if the legislation passes and REAL ID is not implemented, that there would be no documents available to authenticate employment eligibility.

Well, let me conclude, Members, if I may briefly with a few key recommendations. I think there are some things that could be done.

Obviously, the data accuracy issue has to be addressed before the system is scaled. I think the systems of accountability for the dramatically expanded role for the Department of Homeland Security, particularly the ability to essentially require biometric identification and perhaps the collection of fingerprints, that needs to be examined. I think the REAL ID provision needs to be revised.

Finally, these proposals, very costly proposals, to try to make the Social Security card tamper-proof, incorporating biometric identity factors—even if those were to go forward, as other witnesses have testified, I think you would be right back in a couple of years trying to design a new card when the flaws in the current card are uncovered.

Thank you very much for your time.

[The prepared statement of Mr. Rotenberg follows:]

Prepared Statement of Marc Rotenberg, Executive Director, Electronic Privacy Information Center

epic.org

ELECTRONIC PRIVACY INFORMATION CENTER

Testimony and Statement for the Record of

Marc Rotenberg
President, EPIC

Hearing on

Employment Eligibility
Verification Systems (EEVS)

Before the

Subcommittee on Social Security
Committee on Ways and Means,
U.S. House of Representatives

June 7, 2007
B-318 Rayburn House Office Building
Washington, DC

Introduction

Chairman McNulty, Ranking Member Johnson, and Members of the Subcommittee, thank you for the opportunity to testify on proposed employment eligibility verification systems (EEVS) and their relationship with the Social Security Administration.

My name is Marc Rotenberg and I am the Executive Director of the Electronic Privacy Information Center (EPIC). EPIC is a non-partisan research organization based in Washington, D.C. Founded in 1994, EPIC has participated in leading cases involving the privacy of the Social Security Number (SSN) and has frequently testified in Congress about the need to establish privacy safeguards for the SSN.[1] Last year, I testified before this Subcommittee on Social Security regarding high-risk issues surrounding SSNs, and I urged the Subcommittee to limit use and disclosure of the SSN in order to reduce error, misuse, and exploitation.[2] In a hearing before the Subcommittee on Immigration of the House Judiciary Committee in 2005, I also described some of the problems that would likely result from a poorly designed employment eligibility system.[3]

Recently, EPIC prepared a detailed report on the legislative proposals to establish the employment eligibility verification systems.[4] We reviewed the bills currently pending in Congress, the recent reports of the Government Accountability Office, and the report of the Inspector General of the Social Security Administration. Our report "National Employment Database Could Prevent Millions of Citizens from Obtaining Jobs" is attached to this statement.

In my testimony today, I will highlight some of our key findings as well as the related privacy and security concerns in the proposed development of the employment eligibility verification systems. Our central conclusion is that the verification systems proposed in H.R. 1645 and S.AMDT. 1150, contain significant weaknesses that should be remedied prior to enactment.[5] As currently planned, these systems greatly diminish

---

[1] EPIC maintains an archive of information about the SSN, including Congressional testimony, *at* http://www.epic.org/privacy/ssn/.

[2] Marc Rotenberg, Exec. Dir., EPIC, *Testimony and Statement for the Record at a Hearing on Social Security Number High Risk Issues Before the Subcomm. on Social Sec., H. Comm on Ways & Means*, 109th Cong. (Mar. 16, 2006) ["EPIC Testimony on SSN"], *available at* http://www.epic.org/privacy/ssn/mar_16test.pdf.

[3] Marc Rotenberg, Exec. Dir., EPIC, *Testimony and Statement for the Record at a Hearing on H.R. 98, the "Illegal Immigration Enforcement and Social Security Protection Act of 2005," Before the Subcomm. on Immigration, Border Sec., and Claims, H. Comm on the Judiciary*, 108th Cong. (May 12, 2005), *available at* http://www.epic.org/privacy/ssn/51205.pdf.

[4] EPIC, Spotlight on Surveillance, *National Employment Database Could Prevent Millions of Citizens From Obtaining Jobs* (May 2007), http://www.epic.org/privacy/surveillance/spotlight/0507.

[5] Security Through Regularized Immigration and a Vibrant Economy Act, of 2007, H.R. 1645, 110th Cong. (2007) ["H.R. 1645"], *available at* http://www.epic.org/privacy/surveillance/spotlight/0507/hr1645.pdf; Secure Borders, Economic Opportunity and Immigration Reform Act of 2007, S.AMDT. 1150 to S. 1348, 110th Cong. (2007) ["S.AMDT. 1150"], *available at* http://www.epic.org/privacy/surveillance/spotlight/0507/samdt1150.pdf.

employee privacy and make personal information vulnerable to theft and misuse. The proposed verification systems would also grant to the federal government unprecedented control over the livelihoods of American citizens and significantly expand the role of the Department of Homeland Security. The Secretary of Homeland Security could create a biometric identity system for all workers in the United States and make determinations about who is allowed to work without providing the basis for a determination.

Giving the Department of Homeland Security the authority to determine employment eligibility for virtually all Americans in the workforce, including those currently employed, raises unprecedented privacy and security concerns. As the Subcommittee must be aware, last month a critical component of the DHS lost the employment records of 100,000 federal employees. That missing data drive contained the names, Social Security numbers, dates of birth, payroll history and detailed bank account information for every person hired by Transportation Security Administration ("TSA") between January 2002 and August 2005, including federal air marshals who fly undercover to help safeguard commercial aviation in the United States. While the privacy office of the TSA responded promptly once the problem was uncovered, the consequences of that data breach are truly staggering.[6]

This loss of 100,000 employment records by the Department of Homeland Security at a time of growing concern about identity theft raises serious questions about the ability of the Department to safeguard the sensitive data of American workers that would be collected under the House and Senate proposals.

I. The Proposed Employment Verification System Will Increase the Likelihood of Inaccurate Employment Determinations

The House and Senate proposals would significantly expand the Basic Pilot employment verification system instituted in 1997. Currently the program is essentially a voluntary program that is used by only one-fifth of one percent of employers.[7] The expansion of Basic Pilot under the House and Senate proposals would require all U.S. employers, approximately 7.4 million employers in the private sector and 90,000 in the public sector, to verify all new hires within 4 years.[8] This will create serious problems for the 143.6 million employees who would be exposed to preexisting data accuracy problems with the Basic Pilot system.

As currently drafted, the House and Senate proposals would cross-reference large volumes of employee information against government databases.[9] If even a small fraction of employee records contained errors, millions of individuals would be prevented from working if the flaws were not corrected. The number of incorrect nonconfirmations may

---

[6] Transp. Sec. Admin., TSA Public Statement on Employee Data Security (May 2007), *available at* http://www.tsa.gov/datasecurity/statement_05-07-2007.shtm.
[7] U.S. Citizenship & Immigration Serv., Dep't of Homeland Sec., *I Am an Employer... How Do I Use the Employment Eligibility Verification/Basic Pilot Program?* 1 (Jan. 2007), *available at* http://www.uscis.gov/files/nativedocuments/EEV_FS.pdf.
[8] S.AMDT. 1150 §302(a) (amending §274A(d)); H.R. 1645 §301(a) (amending §274A(c)).
[9] H.R. 1645 §301(b)(2), §306; S.AMDT. 1150 §302(a) (amending §274A(c)(9)(F)), §304(a)(1), §308.

be significant. A 2002 independent study of Basic Pilot, undertaken by the Immigration and Naturalization Service (INS), determined that 42% of final nonconfirmations were erroneous and the affected individual was eligible for work.[10]

Correcting such inaccuracies would place considerable burdens upon employees. They would have to navigate the appeals process for as long as two and a half months in order to prove their eligibility to work.[11] Some employees will also face hardship from their employers while trying to correct database errors. The INS report found that almost half of employees awaiting appeal had their pay cut, job training delayed, or were prohibited from working altogether.[12]

Recent reports have also determined that employers are using the Basic Pilot to prescreen applicants, in some instances denying them job opportunities because of faulty data maintained by the federal government.[13] Even though the practice of pre-screening is prohibited, it would seem obvious that employers will try to prescreen so as to avoid the additional burden that might result from a "further action" or "tentative nonconfirmation" notification. And the employee may never know the basis for the determination.

Although the House and Senate proposals provide for accuracy and security reviews, these audits take place months after establishment of the program.[14] Any solution adopted after the fact will likely arrive in the midst of an onslaught of verification requests. To minimize the problems that will arise from database inaccuracies, such errors should be corrected prior to enactment of the bills. A comprehensive accuracy and security audit of agency databases to fix existing problems would prevent setbacks if an employee verification system were established in the future.

II. Data Aggregation

Both the House and Senate bills offer government agencies unprecedented power over the means by which an individual may prove identity to gain employment. Both bills greatly expand the federal government's data collection and data sharing roles. Aggregation of large amounts of data increases the possibility that the information could be used for unintended purposes, such as long-term tracking of individuals and identity theft.

An all-inclusive database provides an appealing mark for thieves trying to create false identities for criminal activities. Large centralized databases of sensitive

---

[10] Inst. for Survey Research, Temple Univ., and Westat, *INS Basic Pilot Evaluation Summary Report* 8 (Jan. 29, 2002) ["Summary of Independent Analysis of Basic Pilot"], *available at* http://www.uscis.gov/files/nativedocuments/INSBASICpilot_summ_jan292002.pdf.
[11] H.R. 1645 §301(a) (amending §274A(c)(19)(A); S.AMDT. 1150 §302(a) (amending §274A(d)(5)(C)(iii)(II)).
[12] Summary of Independent Analysis of Basic Pilot at 31, *supra* note 10.
[13] *Id.* at 19-20; Office of Inspector Gen., Soc. Sec. Admin, *Congressional Response Report: Employer Feedback on the Social Security Administration's Verification Programs, A-03-06-26106* 6 (Dec. 18, 2006), *available at* http://www.ssa.gov/oig/ADOBEPDF/A-03-06-26106.pdf.
[14] S.AMDT. 1150 §302(a) (amending §274A(d)(2)(E); H.R. 1645 §301(a) (amending §274A(c)(2)(C)).

information also create the potential for devastating hardships for the millions of Americans who would be affected by identity theft from even a single security breach. In addition to the personal and financial troubles a data breach causes, some individuals would also experience threats to their safety. Privacy is better safeguarded by storing data in multiple, decentralized locations, and only when necessary.

Both the House and Senate proposals require DHS and the Social Security Administration to work together to operate the employment verification system as a fully integrated, cross-agency system.[15] However, the responsibility for data retention is given to DHS exclusively. The Senate bill requires that the Social Security Administration, Internal Revenue Service, and Department of State disclose personal data to DHS, including: driver's license and state identification numbers; tax information; employment data; passport and visa information; and birth and death records.[16] In addition, both bills give the Secretary of DHS the discretion to choose which documents can be required for employment eligibility.[17]

The House bill requires "administrative, technical, and physical safeguards" in order to minimize the unauthorized disclosure of personal information.[18] This includes the use of encryption, security updates, and periodic tests.[19] While these are all necessary and important components to safeguard data privacy, security includes all parts of a system's hardware, software, tapes, disks, and personnel. Although both bills state that database access will be limited to authorized users only, employees with no connection to employment verification could access the database as well. This likelihood is increased by the interlinking nature of the system proposed under both the House and Senate bills.

Both of the proposals require employers to submit employer and employee attestations, names, addresses, birth dates, and Social Security numbers for every employee. The House bill requires that employee information be stored by the employers for three years after the date of hire, or one year after termination for each employee, whereas the Senate bill requires employers to retain records for seven years after the date of hire, or two years after termination.[20] The employee records must be maintained by employers for a significant amount of time, thus increasing the likelihood of security breaches. The Senate proposal also contains a provision allowing employers to require new employees to submit their fingerprints to DHS. However the bill does not require employee notice or consent.[21] While the purpose of the action is to avoid identity theft, the involuntary collection of biometric data for employment verification is expansive and too invasive to adopt at this time. [22]

---

[15] H.R. 1645 §301(a) (amending §274A(c)(2)(B)); S.AMDT. 1150 §302(a) (amending §274A(d)(1)).
[16] S.AMDT. 1150 §302(a) (amending §274A(d)(9)(D)(i)).
[17] H.R. 1645 §301(a) (amending §274A(b)(1)(E); S.AMDT. 1150 §302(a) (amending §274A(c)(1)(E)).
[18] H.R. 1645 §301(a) (amending §274A(c)(4)(F)).
[19] *Id.*
[20] H.R. 1645 §301(a) (amending §274A(b)(3), (b)(4)); S.AMDT. 1150 §302(a) (amending §274A(c)(3), (c)(4)).
[21] S.AMDT. 1150 §307(a).
[22] S.AMDT. 1150 §307(b)(1).

Employers are to submit employment verification requests via the Internet, other electronic media sources, or over phone lines. These systems are vulnerable to interception, but the bills do not specify proper safety protocols for employers. Employers will also be responsible for collecting and storing large quantities of personally identifiable information for their employees seeking verification.[23]

Requiring employers to retain and protect their employees' personal information creates a significant burden. Employers will incur additional costs for storage, training, and necessary safety precautions. In addition, employers also have the added burden of being forced to verify all of their new hires with the federal government. This could lead to lost revenue as well as the difficulty inherent in implementation of the new procedures.

Neither the House nor Senate proposals require employers to retain sensitive employment data in a secure manner. While most employers would undoubtedly engage in safe storage practices, as identity theft becomes more lucrative, and thieves become more sophisticated, the chances of data breaches increase significantly. The Senate bill does contain a provision requiring the Comptroller General to conduct an annual report to ensure 97 percent employer compliance with specified privacy requirements listed in the bill.[24] Although 97 percent compliance is substantial, if even 3 percent of Americans are subjected to the devastation privacy breaches can cause, that would be too many. For this reason, additional federal safety guidelines should be included in both bills. The current proposals require that privacy trainings be conducted for employers; however, grants and other tools would also help employers successfully implement the necessary changes. These tools would be especially helpful for small business owners who may not have sophisticated technology or large budgets at their disposal.

As currently drafted, neither of the bills offers employees a private right of action against employers who negligently retain employee data. This is undesirable because employees must be protected, in the event that overburdened employers take short-cuts that could jeopardize employee data.

The risks of misuse and data breach are very real. Every day new stories surface in which hapless people are the victims of identity theft or security breaches. These events are caused by both unauthorized and authorized users of databases. For example, in 2006 an official of the Maryland Motor Vehicle Administration was one of three people charged with conspiring to sell unlawfully produced identification cards.[25] Similarly, in 2006, a police officer admitted accessing motor vehicle records to gather personal data on a romantic interest and co-workers.[26] Such abuses may increase under a national employment eligibility verification database.

III. REAL ID Requirements

---

[23] H.R. 1645 §301(a) (amending §274A(c)(12)(A)(ii); S.AMDT. 1150 §302(a) (amending §274A(c)(1).
[24] H.R. §301(a) (amending §274A(c)(18)(B)).
[25] *Fake ID Cards*, Wash. Post, Mar. 15, 2006, at B02.
[26] Michael Kiefer, *Officer Admits to Tampering: Databases Used to Check on Women*, Ariz. Republic, Apr. 6, 2006, at B3.

As the Subcommittee is likely aware, there is growing opposition to the implementation of the REAL ID Act. For example, Nevada recently passed a joint resolution urging Congress to repeal the scheme.[27] Fourteen other states have enacted legislation against it as well. In addition, there are bills in both the House and Senate seeking to repeal the Act.[28] During the public comment period on REAL ID draft rule, DHS received over 12,000 comments.[29]

Significantly, it took the Department of Homeland Security two years to issue the draft rule. The delay has raised further questions about the competence of the agency to successfully create a national identification system.

Therefore, it is surprising that the proposals to establish the Employment Eligibility Verification System assume a functioning, reliable REAL ID document and one proposal actual would make REAL ID-compliant identity the only document that could be used to determine employment eligibility. Identification documents listed under both bills include biometric, machine-readable Social Security cards or passports.[30] In addition, the Senate bill also includes REAL ID compliant driver's licenses.[31] Although REAL ID's drafters did not envision it as a national identification system, merely to set federal requirements for driver's licenses, both of the proposed verification systems would obligate individuals to adopt REAL ID as a prerequisite to employment. In fact, the Senate bill stipulates that non-REAL ID compliant cards would not be accepted after 2013.[32] Thus, both bills would help to create a national identification system, and they would move driver's licenses farther from their original use. There is even a scenario under which the Congress would pass legislation that would make employment in this country permissible only upon the presentation of a document that does not exist.

EPIC has previously explained at length that the REAL ID plan is fundamentally problematic.[33] The creation of machine-readable biometric Social Security and REAL ID cards will allow for greater data collection and tracking of individuals. Personal data would be recorded in digital format in many more encounters, leading to greater numbers of information databases and less secure personal information. The most reliable way to protect citizens, and reduce the growing problem of identity theft is by minimizing the collection of data, developing alternative technologies, and utilizing new organizational

---

[27] EPIC, *National ID Cards and REAL ID Act Page*, http://www.epic.org/privacy/id_cards/.
[28] *Id.*
[29] *Id.*
[30] H.R. 1645 §301(a) (amending §274A(b)(1)(B)(i)).
[31] S.AMDT. 1150 §302(a) (amending §274A(c)(1)(C)).
[32] S.AMDT. 1150 §302(a) (amending §274A(c)(1)(F)).
[33] EPIC Testimony on SSN, *supra* note 2; EPIC, *Spotlight on Surveillance, Federal REAL ID Proposal Threatens Privacy and Security* (Mar. 2007), http://www.epic.org/privacy/surveillance/spotlight/0307; EPIC and 24 Experts in Privacy and Technology, *Comments on Docket No. DHS 2006-0030: Notice of Proposed Rulemaking: Minimum Standards for Driver's Licenses and Identification Cards Acceptable by Federal Agencies for Official Purposes* (May 8, 2007) ["EPIC REAL ID Comments"], *available at* http://www.epic.org/privacy/id_cards/epic_realid_comments.pdf.

practices.[34] The REAL ID identification method does not meet these stipulations. Thus, it is an inappropriate requirement of employment verification systems.

But whether or not you accept our assessment of the REAL ID plan, the substantial opposition by the states, the high level of public opposition, as well as the far-reaching engineering problems suggest that employment verification based upon the availability of the REAL ID card is a perilous course.

IV. SSA Responsibilities

As they are currently drafted, the House and Senate proposals make extensive use of SSNs as a means of identity verification. But the number and card were never intended to used be such. The proposed additions to the Social Security card will increase their value to identity thieves and make privacy breaches more serious when they occur. The bills' requirements would also draw Social Security Administration resources away from their core mission.

When Congress passed the Privacy Act of 1974, it recognized the undesirability of using SSNs as universal identifiers. However, as they are currently drafted, the House and Senate proposals reinforce the use of SSNs as identification.[35] The verification system would require the Social Security Administration to cross-reference its information with DHS to help determine identity.[36] The House proposal recognizes that the SSN should not be an identifier: it requires that a disclaimer appear on the Social Security card stating that it is not to be used for identification purposes.[37] Yet that is precisely the practical effect under both bills.

The proposals would transform the Social Security card and include biometric and machine-readable characteristics, such as a digital photograph of the cardholder, for purposes of individual identification.[38] Including machine-readable features on the Social Security card would create a digital record each time the card is used. A widely used machine readable document increases the risk that the number will be compromised through identity theft. And the biometric data on the card would make breaches more serious for cardholders when they occur.

Adding these expensive features to the Social Security card would also divert resources from the original purpose of the Social Security Administration to administer retirement, disability and survivors' benefits. In a 2006 hearing before this Subcommittee, an Assistant Deputy Commissioner of the Social Security Administration testified that issuing Social Security cards with the new features outlined in the House proposal would cost more than $25 per card, with the cost of replacing cards for all

---

[34] EPIC, *Comments to the Federal Identity Theft Task Force, P065410* (Jan. 19, 2007), *available at* http://www.epic.org/privacy/idtheft/EPIC_FTC_ID_Theft_Comments.pdf.
[35] H.R. 1645 §301(a) (amending §274A(b)(1)(B)); S.AMDT. 1150 §302(a) (amending §274A(d)(5)(A)(i)).
[36] H.R. 1645 §301(b)(2) (amending §205(c)(2)).
[37] H.R. 1645 §301(b) (amending §205(c)(2)(G)(iii)(III)).
[38] H.R. 1645 §301(a) (amending §274A(b)(1)(B), (c)(12)(A)(iii)); S.AMDT. 1150 §305(a)(2) (amending §205(c)(2)(G)(4)).

holders approaching $9.5 billion.[39] Likewise, the safeguards the Social Security Administration and DHS must develop to ensure the system runs properly will be substantial. The bills require administrative, technical and physical layers to protect retained information. This includes encryption, an appeals process, periodic system testing and security updates.[40] These components add significantly to the workload of the agency, but are absolutely crucial from a privacy standpoint if the proposed verification system is to go forward.

The SSN is easily used for fraud not because the card lacks tamper-resistant features, but because the number is used as an identifier in so many encounters when it should not be. A more effective and secure verification system might institute a different unique number for the limited purpose of employment eligibility. This would limit the frequency of SSN disclosure and minimize the severity of any privacy breaches associated with the number. This would help curb identity theft and avoid placing increased costs and workload on the Social Security Administration.

V. Recommendations

Mr. Chairman, Members of the Subcommittee, I predict that if these proposals are adopted as currently drafted, there will be unprecedented problems in American labor markets. Employment verification relies upon the accuracy of the underlying data, the ease with which determinations can be made, the establishment of essential safeguards to ensure that the data collected is not subject to misuse, and procedural remedies to guarantee that when problems arise they can be quickly and fairly resolved. There is virtually no indication that any of these issues have been considered.

First, the existing inaccuracies within agency databases ought to be corrected before establishing the verification systems on a nationwide basis. Otherwise there is a strong likelihood that millions of eligible workers face a laborious identity correction process. This would lead to lost productivity and unnecessary expense.

Second, as little sensitive data should be collected as possible, and then only when necessary. Keeping huge quantities of personal information in a single government database enhances the appeal of that database to those who will attempt to misuse it. And if that database is compromised in the same way that TSA's employment records were, the fact that it contains such voluminous and detailed information makes the breach that much more serious. Instead, limiting the scope of information collected and retained to decentralized databases would reduce the vulnerability. The same goes for employers. Requiring employers to retain such detailed information for years after hire without strong safeguards not only burdens the employers, but also vastly increases the susceptibility of employee information to loss or misuse. Safeguards and privacy

---

[39] Frederick G. Streckewald, Assistant Deputy Comm'r, Disability & Income Sec. Programs, Soc. Sec. Admin., *Statement at a Hearing on Social Security Number High-Risk Issues Before the Subcom. on Soc. Sec. of the H. Comm. on Ways & Means*, 109th Cong. (Mar. 16, 2006), *available at* http://www.ssa.gov/legislation/testimony_031606a.html.

[40] H.R. 1645 §301(a) (amending §274A(c)(4)(F)), §306(a) (amending §205(c)(19)(B)).

implications should be established prior to implementation of the systems.

Third, the House and Senate proposals rely heavily on technology that has yet to be established. At this time, no states have adopted the REAL ID program, and its future is actively contested at both the national and state level.[41] It may therefore be imprudent to enact a wide-scale employment verification system based on a program whose future is in doubt. The verification system would be more effective, and future complications more easily anticipated, if the technology underpinning the documents was worked out beforehand.

Fourth, there must be better accountability for the extraordinary powers granted to the Secretary of Homeland Security. The Secretary should not be given discretionary authority to require the establishment of biometric identification for private employment in the United States or to require the routine collection of fingerprints in the private sector. One the Department's own identification systems, which included contactless RFID technology, was proved deeply flawed and subsequently revised.[42] All determinations of the Secretary regarding employment eligibility should be subject to the full privacy safeguards set out in the Privacy Act of 1974, including the right to inspect and correct data upon which an agency makes a decision, as well as additional safeguards proposed in the various measures.

---

[41] EPIC, *National ID Cards and REAL ID Act Page*, *supra* note 27.

[42] In 2005, DHS began testing RFID-enabled I-94 forms in its United States Visitor and Immigrant Status Indicator Technology ("US-VISIT") program to track the entry and exit of visitors. The RFID-enabled forms stored a unique identification number, which is linked to data files containing foreign visitors' personal data. EPIC warned that this flawed proposal would endanger personal privacy and security, citing the plan's lack of basic privacy and security safeguards. The Department of Homeland Security's Inspector General echoed EPIC's warnings in a July 2006 report. The Inspector General found "security vulnerabilities that could be exploited to gain unauthorized or undetected access to sensitive data" associated with people who carried the RFID-enabled I-94 forms. A report released by the Government Accountability Office in late January identified numerous performance and reliability issues in the 15-month test. The many problems with the RFID-enabled identification system led Homeland Security Secretary Michael Chertoff to admit in Congressional testimony on February 9th that the pilot program had failed, stating "yes, we're abandoning it. That's not going to be a solution" for border security. Dep't of Homeland Sec., *Notice With Request For Comments: United States Visitor and Immigrant Status Indicator Technology Notice on Automatic Identification of Certain Nonimmigrants Exiting the United States at Select Land Border Ports-of-Entry*, 70 Fed. Reg. 44,934 (Aug. 5, 2005), *available at* http://frwebgate1.access.gpo.gov/cgi-ôbin/waisgate.cgi?WAISdocID=021420363270+2+0+0&WAISaction=retrieve; EPIC, *Comments on Docket No. DHS-2005-0011: Notice With Request For Comments: United States Visitor and Immigrant Status Indicator Technology Notice on Automatic Identification of Certain Nonimmigrants Exiting the United States at Select Land Border Ports-of-Entry* (Dec. 8, 2005), *available at* http://www.epic.org/privacy/us-visit/100305_rfid.pdf; Dep't of Homeland Sec. Inspector Gen., *Additional Guidance and Security Controls Are Needed Over Systems Using RFID at DHS (Redacted)* 7 (July 2006), *available at* http://www.dhs.gov/xoig/assets/mgmtrpts/OIGr_06-53_Jul06.pdf; Richard M. Stana, Dir., Homeland Sec. & Justice Issues, Gov't Accountability Office, *Testimony Before the Subcom. on Terrorism, Tech., & Homeland Sec., S. Comm. on the Judiciary*, 110th Cong. (Jan. 31, 2007), *available at* http://www.gao.gov/new.items/d07378t.pdf; and Michael Chertoff, Sec'y, Dep't of Homeland Sec., *Testimony at a Hearing on the Fiscal Year 2008 Dep't of Homeland Sec. Budget Before the H. Comm. on Homeland Sec.*, 110th Cong. (Feb. 9, 2007), *available at* http://www.epic.org/privacy/us-visit/chertoff_020907.pdf.

Fifth, further enhancements to the Social Security card that would reduce the risk of tampering or counterfeiting are sensible, but the provisions to incorporate biometric data, to make the card machine readable, and to propose that it be used more widely to determine employment eligibility should be revised. The machine-readable capability would also create a trail of digital records of the card information whenever it is used. This would create more opportunity for identity thieves to steal the information and the problem would be more severe when they have done so. Instead, perhaps a number other than the SSN, used solely for the purpose of employment verification, may suffice. This would have the added benefit of avoiding additional cost to the Social Security Administration and allowing it to focus on its original mission

Conclusion

Mr. Chairman, members of the Subcommittee, It is tempting to believe that technology and new systems of identification can help solve long-running policy problems, such as determining eligibility to work in the United States. But the reality may be that new systems of identification will create new privacy risks for employees and new burdens for employers. We have already seen how the expanding use of the Social Security Number contributed to the dramatic increase in identity theft in the United States. Given the inaccuracies that currently exist in Basic Pilot, the difficulty that the Department of Homeland Security has had managing computer security and identification systems within its own agency, and the justifiable concern of those currently employed that they will now be required to undergo new identification requirements, I would strongly urge you to proceed cautiously on this proposal. Even a small error rate will impact the livelihood of millions of Americans.

Thank you for your attention. I would be pleased to answer your questions.

Chairman MCNULTY. Thank you, Mr. Rotenberg. Thanks to all of you for your testimony, and for the clarity of your testimony. As

a matter of fact, I had a number of questions prepared for several of you, but you answered them quite clearly in your testimony.

I do want to ask Ms. Moran, because we have been discussing the database discrepancies in the abstract, if you could provide us with a real-life example of how the problems with the databases affect people.

Ms. MORAN. Sure. We provide technical assistance to a lot of labor unions and immigrant organizations across the country. In fact, we just got a technical assistance call last week from a woman in North Carolina. She is Honduran. She had temporary protected status. She was work-authorized. She presented her documents. She worked at a hog plant. When the company put her information in the system, SSA said the stuff didn't match.

The long story short is from January to April she went back to Social Security Administration four times to try to fix the error in the database. Because it wasn't fixed, ultimately the company fired the woman and she was without a job.

So today, she could theoretically go to another company and get a job, but under this new system, if she were fired, she wouldn't be able to go get a new job. Under the proposal that is in the Senate right now, she wouldn't be able to get back wages. She wouldn't be able to get attorneys fees. She could be out of—a low-income worker could be out of a job for a number of months.

So, that is just one example of many to show, really, it is pretty serious, talking about people's livelihood here.

Chairman MCNULTY. Thank you. We just received information that there was a cloture vote in the Senate, and it failed 55 to 42. There is going to be another vote at 5:00, so there is a very real question about how far this bill is going to go now. If it goes anywhere, we want to be prepared for it.

I will now call on the Ranking Member of the Subcommittee, Mr. Johnson, to inquire.

Mr. JOHNSON. Thank you, Mr. Chairman. I appreciate that.

I wonder if all of you could comment, maybe. Many have advocated the use of biometric ID as an effective way to confirm a person's identity. I would like your comments and what you think of a biometric ID. Is it the right or wrong way to go, and why?

Ms. MORAN. I will refer to the technology people on that.

Ms. MEISINGER. I believe that there is some use of biometric information. I think it should be voluntary for the employers who can afford to develop the system and work with the system, but I think the technology is there. I think biometric information has the advantage of being carried with a person wherever they go, and you don't need a card for it if you can have it locked in with other identification that may be in the system.

I think there are ways now—and I am not a technologist so I am going to defer—to build a system where it is not centralized in one government agency, which I agree, I think, is very troublesome to many people, the thought that this would all be in some centralized database.

Right now companies do reference checks on a regular basis. Data mining takes place. They go out with public data sources—where people lived, whether their house was on that street, what

the name on the mortgage was—those sorts of things in terms of to link the person.

I just think that what we would like to see is some technology experts coming together, privacy as well as employers and government, to sort through what is possible that balances. I don't think there is anything that we will ever develop that provides an absolute protection against privacy because you can't control people's behaviors, but I think there are ways to design something that gets closer to what everybody is trying to get done than what is being proposed here.

Mr. JOHNSON. Well, I will tell you, when we had the eye scan out at the airport, which Homeland Security can't get back in again, as you know, I used to like to go to the airport because I would look in that thing and it would say, hello, Mr. Johnson.

Mr. AMADOR. I have to say that from our perspective, as was just mentioned, it should be voluntary, because the employers are of different sizes and levels of sophistication. Most employers in the United States do not have an HR division and an inside legal counsel.

So, what might be easy for one of the over 7 and a half million employers in the United States, about 2 million of those are basically self-employed individuals. Those machines are actually right now, and maybe the technology would improve and it will be cheaper, as has happened with computers and others, but right now those card readers are very expensive for somebody to——

Mr. JOHNSON. Well, you are advocating a private enterprise operation versus government, I think, in that instance.

Mr. AMADOR. Correct.

Mr. JOHNSON. Yes. Dr. Neumann?

Mr. NEUMANN. I would like to generalize your question just a little bit because when you start to talk about biometrics, the question is, how are they embedded in the overall system? You have the problem of nonsecure operating systems and application software, you have the problem of supposedly smart and secure and tamperproof smart cards that aren't, and then you have the biometrics.

Well, some biometrics are actually potentially pretty good. When they first put the photo and the face recognition stuff in the Palm Beach Airport, they could only recognize 40 percent of the people. We are photographed with perfect lighting, and that system was a failure. Well, then, we will increment it up a little bit, and we will get it to 50 and 60 and 70, but most of these systems have the fundamental problem. The gummy bear story is one of the examples of the fingerprint system. There was a demonstration at Asiacrypt a couple of years ago where somebody had taken essentially an imprint of a thumb on a gummy bear and was able to get through all of the fingerprint detection systems that were being demonstrated.

Mr. JOHNSON. Really?

Mr. NEUMANN. The next version of that is you cut off the thumb, of course, and——

Mr. JOHNSON. Well, according to you, there is not a system that can be devised that can't be circumvented.

Mr. NEUMANN. Well, one of my colleagues has in fact essentially broken every smart card. This is Paul Kotcher, who has done

differential power analysis. Just by determining the power consumption of the crypto chip, he can extract the secret key. There are some high tech solutions, but I think we are in this escalating spiral, where we continually believe that if we throw more technology at it, it will solve the problem. Then there turns out to be an utterly trivial countermeasure that completely defeats it.

In many cases, it is, for example, that a cryptography key is stored in memory or a password is pasted up on a Post-It. So, in many cases, it is a very simple attack. Here you have built this very complex system, and discovered that there is some utterly trivial way of breaking it.

Mr. JOHNSON. Thank you. Mr. Rotenberg, do you have a comment?

Mr. ROTENBERG. Yes. I was just going to say briefly that one of the obvious problems with the biometric identifiers is that when they are compromised, you have a real problem. You can change a credit card number or a bank account number, but it is not so easy to change the digital representation of your fingerprint or your eye scan.

It was interesting to us also because we have been studying the identity systems that the Department of Homeland Security has been pursuing. One of the identity systems that they developed, the digital access card, the DAC, was originally designed with only a biometric identifier. They decided that was actually a too-risky approach for Federal employees, so they have included a PIN number as a backup to the biometric. I think it is a recognition on their part that there are going to be problems with biometrics.

Mr. JOHNSON. Thank you. Thank you, Mr. Chairman.

Chairman MCNULTY. Thank you.

Mr. Brady may inquire.

Mr. BRADY. Thank you, Mr. Chairman. Thanks for holding this hearing. I think this is one of the most overlooked issues in the Senate debate right now, and may be an area where this Committee can play a big role in this whole debate.

Listening to the panel, the second panel, I think they have exposed two myths in this discussion. The first is that any Federal agency will be ready in 18 months to reliably and accurately verify employment and identification. It is not a criticism of the agencies. The task is simply overwhelming. The data that is currently available is unreliable. The pilot programs we have had in place have too many question marks. It is like we are trying to stand an elephant on a toothpick and hoping it will hold. It likely won't, and we know it in advance.

The second myth is that any single document, including a national ID card, is necessary or in fact desirable in this. I am not in the black helicopter caucus, but the truth is I think using multiple documents tailored more—the truth of the matter is some workers will be very easily verifiable. Others will be very difficult. We ought to have a system that is flexible enough to deal with that, and it seems this Committee Chairman ought to be exploring some innovative partnership between government and the cutting-edge private companies that are today verifying ID instantaneously, both for companies and for the government itself; find a way where it is more decentralized so you don't have a single, as

Dr. Neumann said, hacker, cracker, or terrorist, I think was the phrase, able to break it. We have examples today.

Two questions. Mr. Amador, GAO says the cost of a completely verifiable system will be about $11.7 billion a year, much of it borne by employers and workers. Can you talk a little about that?

Ms. Meisinger, Mr. Ryan wanted to ask about the background checks that help confirm identity. From what databases do they draw?

So, Mr. Amador.

Mr. AMADOR. Yes. Last year—actually, in 2005, GAO testified and they said it would be that much. I since have called them, and I was trying to find out, well, how do you split it up? They didn't have a rigid split, but what they said, that would be the cost because you will be adding 96 percent of employers to a system. You have to find out a way of also making it telephonic.

So, they said that in addition to considering the fact that you have to hire more verifiers, modernize the system, and purchase and monitoring additional equipment, employers would also need to train employees to comply with the new law requirements and devote a great deal of human resources staff to verifying and reverifying the workforce.

Currently, under the I–9 system, the estimate is that we spend about 12 million working hours verifying the 50 to 60 million of individuals that are hired, either—some people are hired more than once in a year. Some people have more than one job, but somebody is doing the hiring.

There is also the cost of keeping these documents, filing. The requirements in the Senate right now, which we know are too many, too much, are requiring that you keep these documents for like 7 years. We think that is obviously too long, especially when you have a turnover rate that is very high.

Resolving data errors is going to be a new additional cost that is going to be more complicated and expensive than it is under the current system. A new issue is going to be dealing with wrongful denial of eligibility when you get a tentative nonconfirmation.

What they are looking at is the employer is going to have to start making calls because of course you cannot fire the individual until you go through the entire process. In the Senate version, the shortest period that it could take is 152 days. So, you have an employer dealing with days and an employee that is going to have to be taking time off from work to go in person to an SSA office to try to resolve all these things.

So, when they put all of these things together, they are just not looking at how much the one inquiry costs. They are saying, well, how did the entire thing cost? How much was spent in hours from the employer's perspective and from the employee perspective in addition to the government's perspective? And that is when, again, they were using that number when they were trying to ask for more funding. I notice that now they are trying to use lower numbers.

It is also important to mention that I think the number is based on the study that came in 2002, the Westat study that everybody—the independent study that has been mentioned before. There is a new study. Tyler mentioned it. The Chamber has been trying to get

a copy of it. DHS has it, and we would like to have your help in trying to find out if they maybe broke down this number, and some other information in it.

Mr. BRADY. Thank you.

Ms. Meisinger, I am not suggesting background checks on everyone. The point is, oftentimes using multiple sources you can verify quicker and more accurately.

Ms. MEISINGER. I think if you think of some times when you've gone online and people ask you for background questions that you might answer—mother's maiden name, street that you lived in when you were young—those sorts of things are really embedded in databases that exist in a public format.

I think that would be the recommendation, that it would be public formats, public databases. Criminal records are one that reference checkers always go into and look at. Depending on the level of depth that you are going through, you will go to the FBI. Sometimes it will just be local. It depends on the job.

There are state laws now that require this sort of in-depth background check for certain types of jobs. If it is somebody working with children, frequently they will have a much more in-depth background check to try and make sure they know everything they can know about that person, including that the person is who they say they are.

Mr. BRADY. So, you use different sources for different types of jobs and different needs.

Ms. MEISINGER. Different sources. Right.

Mr. BRADY. Which I think it would be difficult to accomplish by people in the single agency or double agency.

Ms. MEISINGER. Well, and I think right now you have got credit companies, check companies that track people's credit history. There is a competitive market to try and make sure that you are the most accurate, the most reliable, respond the quickest to the customers. I think you want to build that same sort of environment.

Mr. BRADY. Right. Thank you.

Thank you, Mr. Chairman.

Chairman MCNULTY. Thank you very much. On behalf of Mr. Johnson, Mr. Brady, and all the Members of the Committee, we want to thank each of you for your expert testimony. It has been extremely helpful.

We would ask that as the process moves forward, we may keep in contact with you for your response to questions by our Members and our staff outside of the formal setting of a hearing, so that we are able to contact you on a more immediate basis.

I would just like to say for myself that as I have looked at the Social Security agency and the many challenges that it faces, we have been tremendously distressed with the lack of progress on the issue of the disability backlog, which we have been trying to work on for a long time now.

I think it is an unmitigated disaster and I don't want to see it compounded by another disaster. If you can help us in that regard, we are deeply grateful.

This Committee hearing is adjourned.

[Whereupon, at 12:17 p.m., the hearing was adjourned.]

[Submission for the Record follows:]

On behalf of the 11,000 front-line Border Patrol employees that it represents, the National Border Patrol Council thanks the Subcommittee for holding a hearing to examine various methods of verifying the employment eligibility of workers in the United States. There is now near-universal agreement with the 1994 finding of the U.S. Commission on Immigration Reform that "reducing the employment magnet is the linchpin of a comprehensive strategy to reduce illegal immigration." There is no consensus, however, regarding the best method for accomplishing that goal. The Immigration Reform and Control Act of 1986 made it a crime to hire illegal aliens, but failed to provide employers with a simple and effective means of verifying the authenticity of the numerous documents that were permitted to be used to prove eligibility to work in this country. Thus, it is nearly impossible to establish that an employer "knowingly" hires illegal aliens, rendering the current law largely unenforceable and meaningless.

The Illegal Immigration and Immigrant Responsibility Act of 1996 required the Attorney General to conduct three pilot programs of employment eligibility confirmation: the basic pilot program, the citizen attestation pilot program, and the machine-readable-document pilot program. Of these, the basic pilot program, now known as the Employment Eligibility Verification System, has emerged as the most widely-utilized system. Although it is relatively inexpensive and easy to use, it is also extremely susceptible to identity fraud, wherein legitimate information is used by imposters. This was highlighted by the recent Bureau of Immigration and Customs Enforcement raids against several Swift & Company plants, in which nearly thirteen hundred people who were cleared to legally work under the provisions of the Employment Eligibility Verification System were arrested for being in the country in violation of our immigration laws. Although the current amount of fraud under that system is relatively low, that is due to the fact that only a very small percentage of companies are participating in the program, and most illegal aliens opt to seek employment in companies that do not use it. If its use became mandatory, however, the amount of fraud would undoubtedly increase exponentially. The Federal Trade Commission estimates that about ten million Americans are victimized by identity theft annually. With such a large universe of compromised identities to draw from, criminals would have no problem supplying illegal aliens with new identities to circumvent the system. Moreover, the information contained in the Social Security Administration's databases contains a number of inaccuracies, especially concerning citizenship. In fact, a recent study by the Office of Inspector General of the Social Security Administration found that at least 100,000 non-citizens are provided with bona fide Social Security numbers every year based on invalid immigration documents. That report also acknowledged that the agency has no way of knowing how many Social Security numbers have been improperly issued to illegal aliens.

The other two employment eligibility confirmation pilot programs suffered from similar shortcomings. The citizen attestation pilot program was limited to non-citizens, and was not designed to verify the validity of claims of citizenship, but only identity. Thus, this program was by far the most vulnerable to fraud, as well as the least useful of the experimental programs. The machine-readable-document pilot program relied upon State-issued identity documents that met specified criteria, and matched that to the information contained in Social Security Administration and Immigration and Naturalization Service databases. Because only one State's driver's licenses met the specified criteria at that time, this test was quite limited in scope. Moreover, its reliability was diminished by its reliance upon the aforementioned incomplete and inaccurate databases.

The National Border Patrol Council believes that it would be unwise to expand any of these experimental systems, but rather recommends that the lessons learned from them be used to construct a workable and effective system.

Such a system must utilize a single, counterfeit-proof, machine-readable document that contains a recent digital photograph, as well as embedded biometric information. Since every authorized worker in this country is issued a Social Security number, the logical choice for this document is the Social Security card. Instead of relying upon information contained in one or more incomplete or inaccurate databases to check for employment eligibility every time a person applies for a job, the system should verify that information conclusively prior to issuing the new secure document. Then, when an applicant presents the employment eligibility document to a prospective employer, the only check that would need to be made is a determination of whether or not the document is genuine, and that could easily be accomplished through means of an electronic reader. At the same time, this process would provide the Department of Homeland Security with a record of all employment inquiries,

which would facilitate its worksite enforcement efforts. It would be a simple matter for investigators to spot-check for compliance by matching employment inquiries with payroll and income tax withholding records.

H.R. 98, the "Illegal Immigration Enforcement and Social Security Protection Act of 2007," would mandate the establishment of such a system, and would also provide the enforcement mechanism and resources to ensure compliance therewith. This would effectively eliminate the employment magnet, allowing the Border Patrol and other law enforcement agencies to concentrate their scarce resources on stopping terrorists and other criminals from entering the United States. Such a system would have the added benefit of greatly reducing the amount of identity theft involving Social Security numbers.

The consequences of inaction and/or delay are dire. Open borders are an open invitation to further terrorist attacks. These measures need to be enacted swiftly in order to safeguard our Nation.