United States Government Accountability Office

GAO

Testimony

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

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

EMPLOYMENT VERIFICATION

Agencies Have Improved E-Verify, but Significant Challenges Remain

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

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

GAO
Accountability * Integrity * Reliability

GAO-11-522T

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

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

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

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

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

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

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

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

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

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

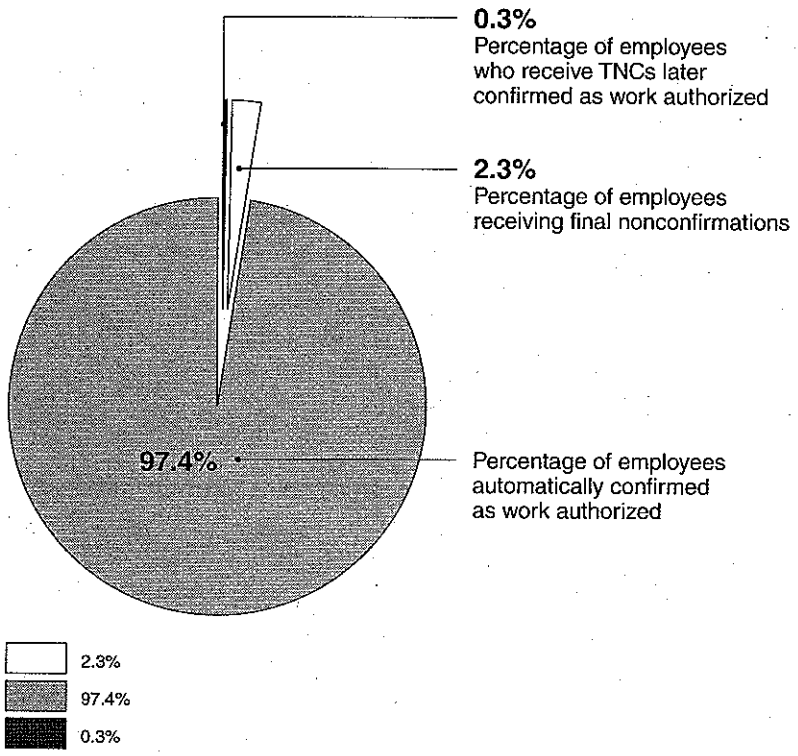
three states for site visits—Colorado, North Carolina, and Arizona—based on, among other reasons, the length of time each state's E-Verify law had been in effect. While the views provided are not generalizable, they provided us with additional perspectives on the benefits and challenges associated with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

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

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

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

Figure 1: E-Verify Results for Fiscal Year 2009



Source: GAO analysis of DHS data.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

GAO Contacts and Staff Acknowledgments

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

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

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

This is a work of the U.S. government and is not subject to copyright protection in the United States. The published product may be reproduced and distributed in its entirety without further permission from GAO. However, because this work may contain copyrighted images or other material, permission from the copyright holder may be necessary if you wish to reproduce this material separately.

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's Web site (www.gao.gov). Each weekday afternoon, GAO posts on its Web site newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to www.gao.gov and select "E-mail Updates."

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's Web site, http://www.gao.gov/ordering.htm.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Ralph Dawn, Managing Director, dawnr@gao.gov, (202) 512-4400
U.S. Government Accountability Office, 441 G Street NW, Room 7125
Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548

Please Print on Recycled Paper