



United States Government Accountability Office
Washington, DC 20548

June 14, 2011

The Honorable Sam Johnson
Chairman
Subcommittee on Social Security
Committee on Ways and Means
House of Representatives

Subject: *E-Verify: Responses to Posthearing Questions for the Record*

On April 14, 2011, I testified before your subcommittee on E-Verify, an Internet-based system that is operated by the Verification Division of the Department of Homeland Security's U.S. Citizenship and Immigration Services (USCIS) and the Social Security Administration (SSA)¹. This letter responds to four questions for the record that you requested that we address on May 17, 2011. The responses are based on work associated with our December 2010 report on E-Verify² and on updated information regarding questions 3 and 4 that we obtained from USCIS on May 27, 2011. Your questions and my responses follow.

1. Under E-Verify, law-abiding Americans' personal information is being checked through the Department of Homeland Security (DHS). What is DHS doing with the personal data? Can this information be mined for other purposes? Can we assure Americans that their personal information may not be used for any other purpose?

According to privacy impact assessments published in connection with the E-Verify program, DHS has committed to using E-Verify only to respond to employment verification inquiries and for other specific and limited purposes, such as to ensure that fraud is not being committed in the system. While it is true that the data collected in the systems that support the E-Verify program could potentially be "mined" for other purposes, DHS has committed not to do so within the E-Verify program. The Implementing the Recommendations of the 9/11 Commission Act of 2007 requires DHS to report annually on activities currently deployed or under development that meet the act's definition of data mining. DHS has not reported any E-Verify actions as data-mining activities under its reporting requirements.

¹ GAO, *Employment Verification: Agencies Have Improved E-Verify, but Significant Challenges Remain*, GAO-11-552T (Washington, D.C.: April 14, 2011).

² GAO, *Employment Verification: Federal Agencies Have Taken Steps to Improve E-Verify, but Significant Challenges Remain*, GAO-11-146 (Washington, D.C.: Dec. 17, 2010).

DHS has taken actions to minimize risks to the privacy of personal information of employees who are processed through E-Verify. For example, the privacy impact assessment and other published privacy notices set limits on the collection and use of personal information for the E-Verify program. Further, DHS has designed E-Verify to collect and share little personal information about individual employees. Specifically, E-Verify does not require employers to collect any more information on employees than has already been recorded on the Form I-9,³ and controls have been established within E-Verify's automated system that limit the extent to which management program analysts at DHS can access and use personal information when searching the available databases to confirm citizenship or work authorization status. For example, management program analysts' access is limited to information applicable to the cases that are assigned to them. Controls such as these are intended to provide assurance that the personal information collected by E-Verify will not be used for other purposes, such as data mining.

2. What is the solution for having a good employment verification system, one that does not put individual jobs in jeopardy due to its shortcomings, like failing to detect identity fraud and preventing an unscrupulous employer from lying to the system and certifying an unauthorized worker?

A good employment verification system relies on a combination of factors, including (1) information technology systems that are reliable and have sufficient capacity to notify employers of employment verification results without interruptions in service, and that have quality control procedures to screen for data entry errors; (2) government databases and employee documents that contain accurate and consistent personal information on employees; (3) the ability of employees to access personal information and correct inaccuracies or inconsistent personal information in DHS databases; (4) employers who act in good faith to implement the rules of E-Verify; (5) mechanisms that can determine if employees are presenting genuine identity and employment eligibility documents that are borrowed or stolen; and (6) a credible worksite enforcement program.

With respect to ensuring that individual jobs are not jeopardized because of E-Verify data inaccuracies and willful employer noncompliance, USCIS has taken steps to improve the accuracy of E-Verify, and USCIS's ability to monitor employer compliance should expand further with the planned fiscal year 2012 implementation of a data analysis system for analyzing complex patterns in the E-Verify data that could be indicative of employer misuse. This is a step in the right direction, although USCIS still has a ways to go to staff its E-Verify Monitoring and Compliance Branch up to its authorized level⁴ and is generally not in the position to determine whether employers carry out activities required by E-Verify because interactions between

³ The Immigration Reform and Control Act of 1986 established an employment verification process—the Form I-9 process—that required employers to review documents presented by new employees to establish their identity and employment eligibility.

⁴ We noted in our December 2010 report that USCIS's Verification Division Deputy Division Chief told us that USCIS had hired 22 of 44 monitoring and compliance analyst staff budgeted in fiscal year 2010 and planned to hire the additional 22 staff in fiscal year 2011.

employers and employees generally occur privately in workplaces where USCIS has limited capability to monitor employer compliance with E-Verify requirements.

With respect to detecting identity fraud and whether unscrupulous employers hire unauthorized workers, a challenge is that it is difficult to positively link identity documents with the persons who present them. In this regard, thought has been given to the use of biometrics that would provide for such a linkage. While this could resolve some of the weaknesses of the E-Verify system, the use of biometrics could be costly and generate privacy concerns. Further, to investigate, sanction, and prosecute unscrupulous employers, USCIS must rely on U.S. Immigration and Customs Enforcement (ICE). Although USCIS and ICE signed a memorandum of agreement in December 2008 that outlined the processes that the agencies are to use for sharing E-Verify program information, ICE has reported that it has limited resources for investigating and sanctioning employers that knowingly hire unauthorized workers or those that knowingly violate E-Verify program rules, and overall, ICE has expended relatively few resources on carrying out such activities.⁵ Policy decisions about how to effect a credible worksite enforcement program using E-Verify have yet to be made. The success of the E-Verify program will ultimately be affected by these decisions.

3. Do you have updated estimates for the cost of a mandatory E-Verify system for new hires and for using E-Verify for all current workers? Do you have an estimate of the visits to the field offices a mandatory system would generate?

With respect to the cost of a mandatory E-Verify system, USCIS said it is currently working on estimating costs. According to USCIS, it has a formula for calculating the funding and resources needed if legislation mandating E-Verify is passed. If E-Verify were mandated for all new hires nationwide, USCIS estimates that about 60 million E-Verify queries would be generated annually. If E-Verify were mandated for all current workers, USCIS estimates that approximately 120 million additional queries would be generated (in addition to the 60 million for new hires) based on 2008 U.S. Census Bureau data. According to USCIS, the formula would need to be adjusted accordingly depending on, among other things, changes in the size of the workforce and the specifics of the legislation.

With respect to field visits resulting from a mandatory E-Verify system, USCIS said that under a phased-in approach, it estimates that there will be an annual query volume of 60 million for new hires. USCIS said this would generate approximately 490,000 visits to SSA field offices, though this estimate would be subject to change.

4. DHS has just implemented a third party authentication system called Self Check. Do you know if DHS is provided with any personal information about the individual from the third party authenticator in the Self Check system?

⁵ In fiscal year 2009, ICE spent 5.2 percent of its 10.4 million agent reported workload hours on worksite enforcement, issued 52 fines as a result of Form I-9 audits, and made 444 criminal and 1,654 administrative worksite enforcement arrests.

E-Verify Self Check utilizes a third-party authenticator (independent identity assurance service) to generate an identity assurance quiz and determine whether individuals attempting to check their employment eligibility are who they claim to be. According to USCIS, DHS does not keep any information about the questions asked, the answer options given, and the answers an individual chose. The only information DHS retains from the identity assurance portion of the Self Check process is a transaction identification number and the result of the transaction. USCIS said this information is retained to determine success and to further improve the Self Check process. DHS's information retention policy for Self Check is detailed in a published System of Records Notice and Privacy Impact Assessment.

If you have any questions about this letter or need additional information, please contact me at (202) 512-8816 or stanar@gao.gov.



Richard M. Stana
Director
Homeland Security and Justice Issues