Written Statement of the
American Civil Liberties Union

Laura W. Murphy
Director, Washington Legislative Office

Christopher Calabrese
Legislative Counsel

Before U.S. House Judiciary Committee
Subcommittee on Immigration Policy and Enforcement

June 15, 2011

Hearing on H.R. 2164 the "Legal Workforce Act"

The December 2010 GAO Report on E-Verify repeat memorandum of understanding (MOU) that all em

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

Self-Check

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

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

Second, the system must protect the privacy of both employers and employees. Considering high rates of identity fraud associated with the E-Verify system, it is no surprise that individuals are very concerned about the retention of their personal information in a database to which more and more people are gaining access. There must be clearly defined limits in regard to potential sharing of personal information.

Third, there must be an option for self-check access to people without credit histories. If self-check relies on background check information, then it will be unavailable to populations of foreign nationals who have only recently arrived in the U.S. and have not yet developed a credit history. This would include some of those with the most complicated immigration situations such as refugees, asylum seekers, and people with temporary protected status.[16]

Due Process Protections

More significantly, senior officialr natiHS Privacy Office atn a dataome of t7(26.295 -1.58TD-.0001 Tc-.

days.[17] This is time that an employee would be unable to work under a mandatory E-Verify system. Congress must prevent the creation of a new employment blacklist – a “No-Work List” – that will consist of would-be employees who are blocked from working because of data errors and government red tape.

The only remedy for this problem provided in H.R. 2164 is the Federal Tort Claims Act (FTCA). The FTCA falls short and does not provide an adequate procedure for the hundreds of thousands who would be impacted unfairly by the imposition of a mandatory E-Verify procedure. The U.S. Court of Claims reported an extensive backlog of cases and requires a worker to exhaust a six-month long waiting period before filing suit. During the pendency of the FTCA administrative procedure and lawsuit, the worker would be barred from working.

The best current model for due process protections can be found in Title II of the ‘Comprehensive Immigration Reform for America’s Security and Prosperity Act of 2009 - H.R. 4321 from the 111th Congress. This provision would have created worker protections for both tentative and final non-confirmations, allowed workers to recover lost wages when a government error cost them a job, limited retention of personal information, and created accuracy requirements for the system.

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

75 Tcol(gp.17)

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

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

Despite the fact that CIS has more than doubled the number of staff tasked with monitoring employers' use of E-Verify since 2008, it still does not have the means to effectively identify and address employer misuse or abuse of the system. A recent report from the SSA Office of the Inspector General (OIG) found that SSA itself had failed to comply with many of regulations put in place to protect employees. The agency failed to confirm the employment of 19% of the 9,311 new SSA employees hired for fiscal year 2008. Of those who were processed, SSA did not comply with the 3-day time requirement for verifying eligibility. The OIG also found that SSA verified the employment eligibility of 26 employees who were not new hires but had sought new positions within the agency, 31 volunteers who were not federal employees, and

than 12 million undocumented immigrants are working in the United States. Many of these workers are part of the black market, cash wage economy. Unscrupulous employers who rely on below-market labor costs will continue to flout the imposition of a mandatory employment eligibility pre-screening system and biometric national ID. These unscrupulous employers will game the system by running only a small percentage of employees through the system or by ignoring the system altogether. In the absence of enforcement by agencies that lack resources to do so, employers will learn there is little risk to gaming the system and breaking the law.

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

Additional failures will come when the worker is initially processed through the system. Crooked insiders will always exist and be willing to sell authentic documents with fraudulent information.[22] Undocumented immigrants will be able to contact these crooked insiders though the same criminals whom they hired to sneak them into the United States. Securing identification will simply be added to the cost of the border crossing.

Since 2004, more than 260 million records containing the personal information of Americans have been wrongly disclosed.[23] Many individuals' personal information, including social security numbers, are already in the hands of thieves. There is nothing to prevent a criminal from obtaining fraudulent access to E-Verify (pretending to be a legitimate employer), verifying that a worker is not already registered in the system and sending an undocumented worker to get a valid biometric using someone else's information.

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

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

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

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