CENTER FOR
DEMOCRACY
&
TECHNOLOGY
Working for Civil Liberties on the Internet

1634 I Street, NW Suite 1100
Washington, DC 20006
202.637.9800
fax 202.637.0968
http://www.cdt.org

March 12, 2008

Department of Homeland Security Data Privacy and Integrity Advisory Committee
Public Meeting, March 12, 2008, El Paso, Texas
[Docket No. DHS-2008-0025]

Re: Comments for the Record, Privacy and Civil Liberties Implications of E-Verify

Via: PrivacyCommittee@dhs.gov

Dear DPIAC Members:

The Center for Democracy & Technology submits these brief comments to highlight key privacy and civil liberties implications of E-Verify, the Department of Homeland Security's ("DHS") electronic employment eligibility verification system, previously known as "Basic Pilot."

We encourage the Committee to thoroughly investigate the privacy and civil liberties issues presented below and to make recommendations to DHS, and if appropriate to Congress, on how to better protect privacy and civil liberties as the program is refined and expanded to more employers. (We also encourage the Committee to review the *November 27, 2007 Stakeholder Meeting Report* prepared by Westat and submitted to DHS in January, which highlights questions of concern regarding E-Verify in six different topic areas.)[1]

- **Data Accuracy and Database Errors.** For E-Verify to do what it is supposed to do – verify the employment eligibility of U.S. citizens and legal immigrants – the system must have access to accurate data. E-Verify currently relies on databases managed by the Social Security Administration ("SSA") and DHS. However, the accuracy of these databases is questionable. For example, the SSA Inspector General estimated in December 2006 that the SSA database relied on by Basic Pilot has almost 18 million errors.[2] The Committee should

[1] The report is not currently available online.

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

closely examine the question of database accuracy and make recommendations to DHS, as the manager of E-Verify, to ensure that both SSA and the Department's own databases contain accurate information. In addition, if E-Verify expands to incorporate other databases such as the State Department's passport database or state driver's license and ID card databases, the Committee should ask DHS what safeguards will be employed to ensure that the system is checking against accurate data.

- **Due Process and Redress.** It is extremely troubling that E-Verify does not have a formal administrative review process for resolving Tentative Non-Confirmations (TNCs) and Final Non-Confirmations (FNCs), nor judicial review of FNCs. There is also no clear means by which individuals who are wrongly denied the right to work and suffer hardship can seek redress against the government or employers. *The fact that a person could be denied the right to work based on erroneous information in a government database and have no clear means to correct the record or appeal is unconscionable.* Employers are supposed to provide written notice to the newly hired employee of a TNC[3], but as the evaluation of the Basic Pilot makes clear, notice is not always provided[4]. Even if the employee receives notice of the TNC, the process for further review at the SSA can be confusing and time consuming. Review at DHS is similarly opaque. At the U.S. Citizenship and Immigration Services ("USCIS"), an Immigration Status Verifier (ISV) is assigned to manually check DHS databases to determine the applicant's citizenship or immigration status.[5] But neither DHS or SSA provides a case manager or liaison to guide the applicant through the bureaucratic process. *For an FNC, the employee is out of luck.* There is no process for further agency or judicial review. The Committee should investigate and make recommendations to DHS to ensure that employees are properly notified of TNCs and FNCs, and that there is a clear process to challenge TNCs and FNCs and to recover lost wages or otherwise be compensated for the wrongful denial of employment. Because DHS has opposed administrative review in the past, the Committee should also consider whether to make a recommendation to Congress to legislate an administrative/judicial review process for the E-Verify program and to authorize compensation in appropriate cases.

- **Privacy and Security of Personal Information, Including Biometric Data.** The E-Verify system contains a striking loophole that may permit individuals to pose as employers in order to gain access to the system and its wealth of personal information. As the September 2007 Westat report states, "One possible weakness of the system is that under current procedures, employers joining the Web Basic Pilot are not verified against any listing of employers; therefore, anyone wanting access to the system could pose as an employer and get access to

---

http://www.ssa.gov/oig/ADOBEPDF/A-08-06-26100.pdf.

[3] Department of Homeland Security, *Privacy Impact Assessment for the Verification Information System Supporting Verification Programs* (April 1, 2007) ("April 2007 PIA") at Section 7, http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_cis_vis_update_ver.pdf.

[4] Westat, *Findings of the Web Basic Pilot Evaluation* (Sept. 2007) ("Sept. 2007 Westat Report") at xxiii, http://www.uscis.gov/files/article/WebBasicPilotRprtSept2007.pdf.

[5] April 2007 PIA, *supra* note 3, at 2-3.

the system by signing an MOU."[6] Additionally, DHS is rolling out the "Photo Tool" to enable visual comparisons of immigrants' photo ID cards. However, there are no legislative or regulatory limits on the inclusion of other biometrics in the future or expanding the photo/biometric tool to American citizens, not just immigrants. The November 2007 Westat report highlights key questions related to biometrics including: Who would own the data or have access to the data? Could there be unauthorized access within the government? Could the system be hacked?[7] The Committee should investigate and make recommendations to DHS to ensure that personal information, including biometric data, is properly secured from unauthorized access.

- **National ID Database, Tracking of Americans and Mission Creep.** With the E-Verify program in place, there is a legitimate concern of "mission creep" and the possibility that over time the program will expand into the functional equivalent of a national ID card. *With the prospect that E-Verify will move beyond the SSA and DHS databases to include the passport database, state motor vehicle records, and photographs and other biometrics, there is a very real possibility that a centralized, or at least centrally accessible, ID record will be created on most Americans.*[8] Federal government tracking of citizens and non-citizens alike will become much easier, especially given that work history is now recordable via E-Verify. There is a also a risk of mission creep – that use of the system will not be limited to verification of an individual's right to work, but instead be expanded for a myriad of other potentially invasive and discriminatory purposes. The Committee should investigate and propose safeguards to ensure that the information consolidated by E-Verify not be used as a *de facto* national ID system that facilitates government tracking of individuals and other potential privacy and civil liberties violations.

- **Risks Exacerbated If E-Verify Becomes Mandatory.** Use of E-Verify is still largely voluntary (with the exception of mandates for federal contractors and those imposed by states). Given the problems associated with E-Verify discussed above – including data errors, the lack of appropriate appeal and redress procedures, the lack of meaningful privacy and security protections for personal information, and the risks of tracking and mission creep – the danger to civil liberties posed by mandating E-Verify nationally and scaling up to include every American employer cannot be overstated. The Committee should examine the privacy, security and civil liberties/rights risks associated with a mandatory E-Verify system and strongly recommend to Congress and DHS against any such expansion.

---

[6] Sept. 2007 Westat Report, *supra* note 4, at xxvi.

[7] Westat, *[E-Verify] November 27, 2007 Stakeholder Meeting Report* (Jan. 2008) at 11 [not currently available online].

[8] *See* Jim Harper, "Electronic Employment Eligibility Verification: Franz Kafka's Solution to Illegal Immigration," Cato Institute Policy Analysis No. 612 (March 5, 2008) at 10-18, http://www.cato.org/pub_display.php?pub_id=9256.

CDT appreciates the opportunity to submit these brief comments.

For questions, please feel free to contact:

Sophia Cope
Staff Attorney/Ron Plesser Fellow
Center for Democracy & Technology
202-637-9800 x104
scope@cdt.org