



NATIONAL
IMMIGRATION
LAW CENTER
www.nilc.org

June 22, 2009

Mary Ellen Callahan
Chief Privacy Officer
Department of Homeland Security
Washington, DC 20528

Re: Comments on Docket Number DHS-2009-0015 Privacy Act of 1974; USCIS-009 Compliance Tracking and Monitoring System (CTMS) System of Record Notice.

Dear Ms. Callahan:

The National Immigration Law Center (NILC) submits the following comments in response to the request for public comment by the Department of Homeland Security to the Privacy Act of 1974; USCIS-009 Compliance Tracking and Monitoring System (CTMS) System of Record Notice, 74 Fed. Reg., No. 98, pages 24022-24027 (May 22, 2009).

In the System of Records Notice (SORN), DHS announces: (1) the creation of a Monitoring and Compliance Branch (M&C) within the United States Citizenship and Immigration Services (USCIS) Verification Division; and (2) the launch of CTMS, a system of records to be operated by the M&C. M&C is tasked with using CTMS to identify abuse of the Systematic Alien Verification for Entitlements (SAVE) and E-Verify programs and apply corrective measures such as retraining users or reporting suspect activity to law enforcement.

NILC protects and promotes the rights and opportunities of low-income immigrants and their family members. NILC specializes in immigration law and the employment and public benefits rights of immigrants. We conduct policy analysis and impact litigation and provide publications, technical advice, and trainings to a broad constituency of legal aid agencies, community groups, government agencies and *pro bono* attorneys.

NILC has extensive experience in dealing with the adverse impact of United States laws, policies, rules and procedures on immigrant communities in the United States. NILC also has developed specialized expertise in employment issues affecting immigrants, immigrant eligibility for public benefits, and the use of SAVE and E-Verify.

The SORN does not adequately address documented, widespread employer abuse of E-Verify.

E-Verify (formerly known as Basic Pilot) allows employers to electronically verify the work authorization of new employees. When Congress authorized E-Verify in 1996, it enacted a variety of privacy and antidiscrimination protections to accompany the program. For example, employers are prohibited from using E-Verify selectively or discriminating on national origin or citizenship grounds. They are required to post notices in the workplace informing workers of the use of E-Verify, and they may not verify applicants prior to their acceptance of a job offer or re-verify existing employees. Most importantly, they are prohibited from taking negative employment actions against employees who receive tentative non-confirmations (TNCs) while the

BOARD OF DIRECTORS

Allen Erenbaum
Chair
Mayer, Brown,
Rowe & Maw

Cynthia Lange
Secretary
Fragomen, Del Rey,
Bernsen & Loewy, PC

Lucas Guttentag
Treasurer
American Civil
Liberties Union,
Immigrants'
Rights Project

Della Bahan
Bahan & Associates

Richard Boswell
University of California
Hastings College of Law

Muzaffar Chishti
Immigration Policy
Institute at
New York University
School of Law

Iris Gomez
Massachusetts Law
Reform Institute

Lin-Hua Wu
Kekst and Company

*Organizations listed
for identification
purposes only*

EXECUTIVE DIRECTOR

Marielena Hincapié

LOS ANGELES
HEADQUARTERS

3435 Wilshire Boulevard
Suite 2850
Los Angeles, CA 90010
213 639-3900
fax 213 639-3911

WASHINGTON, DC

1444 Eye Street, NW
Suite 1110
Washington, DC 20005
202 216-0261
fax 202 216-0266

employees are contesting the TNCs, and they must notify employees of their right to contest a TNC.¹

Despite Congressional efforts, these protections have not been successful in preventing employer abuse of E-Verify. According to a 2007 study conducted by Westat, 47 percent of employers put workers through E-Verify before the employees' first day at work. 9.4 percent do not notify workers of a TNC, and of those who do notify workers, 7 percent do not encourage them to contest the TNC.² When E-Verify returns a negative TNC, 22 percent of employers restrict work assignments; 16 percent delay job training; and 2 percent reduce pay. The information about employer misuse of the system was voluntarily provided by the employers themselves and only a small percent of all E-Verify users were surveyed, so it is reasonable to assume that actual misuse of the system is in fact higher.

The SORN neither recognizes the substantial employer misuse of the system, nor does it propose adequate means to monitor or ensure compliance with system requirements. It lists four potential sources of information M&C will use to learn of employer abuse of E-Verify: (1) CTMS; (2) complaints from users or verification subjects; (3) media reports; and (4) law enforcement tips.³ Using these sources, M&C purports to identify such non-compliant employer behaviors as verification of applicants before they are hired (prescreening); termination of employees who receive TNCs; discriminatory use to verify only employees of one race or nationality; and failure to post notice of E-Verify use. But the SORN does not fully explain how M&C will effectively identify these types of employer misconduct using the listed information sources.

CTMS will only provide M&C with information that can be found in the Verification Information System (VIS). For some purposes, the VIS may be adequate. For example, CTMS could use VIS data to determine whether existing employees have been re-verified, because the VIS contains information on all uses of E-Verify, including multiple verifications of one employee by the same employer. However, verification of job applicants seems difficult to identify in VIS, because hire dates are not collected by VIS.⁴

Termination of employees who receive TNCs likewise seems difficult to identify in VIS, because fire dates are not collected. Discriminatory use of E-Verify to verify only employees of one race or nationality seems impossible to track because CTMS does not contain information about employees who are not verified to compare against information about employees who are verified. Finally, the SORN itself

¹ Section 402(a) of the Illegal Immigration Reform and Immigrant Responsibility Act of 1996 (IIRIRA), Pub.L. 104-208, 110 Stat. 3009 (1996), codified at 8 U.S.C. § 1324a note. The prohibited practices are also included in the Memorandum of Understanding that employers sign with DHS and the Social Security Administration.

² Findings of the Web-Based Basic Pilot Evaluation (Westat, Sept. 2007), *available at* <http://www.nilc.org/immsemplymnt/ircaempverif/WebBasicPilotRprtSept2007.pdf>.

³ System of Records Notice for the USCIS Compliance Tracking and Monitoring System (DHS-2009-0015), 74 Fed. Reg. 24022, 24023 (proposed May 22, 2009).

⁴ System of Records Notice for the Verification Information System, 73 Fed. Reg. 10793 (proposed February 28, 2008).

admits to the impossibility of having the CTMS track failure to post notice of E-Verify use.⁵

Employee complaints, media reports, and law enforcement tips are sources that the SORN mentions only briefly, but they are the only sources that seem likely to be able to identify most types of employer misuse of E-Verify. The usefulness of these sources is dependent on employee knowledge of M&C, strong initiative by M&C to track nationwide media reports, and time and resources available to law enforcement agencies to aid in the enforcement of non-criminal violations of anti-discrimination law. All of these variables seem unlikely to materialize, and even more significantly, all three sources will be unhelpful if whistleblower employees are unwilling to come forward to M&C, the media, and law enforcement. As discussed below, immigrant employees will likely remain silent if the possibility of M&C participation in immigration enforcement remains open. Due to the shortcomings of all four information sources listed in the SORN, M&C's ability to identify employer misuse of E-Verify seems questionable.

The SORN does not adequately address how monitoring and compliance will be conducted given the expanded use of SAVE by states and localities.

The SAVE program was legislatively authorized as part of the Immigration Reform and Control Act of 1986 (IRCA)⁶ and was originally intended for use by a limited number of benefit-granting government agencies. IRCA specifically identified the following benefit-granting programs for which the SAVE program was to be used: Aid to Families with Dependent Children (AFDC), Medicaid, unemployment compensation, Food Stamp program, housing assistance, and Title IV education assistance.⁷ The REAL ID Act, passed by Congress in 2005, authorized use of the SAVE program to verify immigration status for issuance of state driver's license issuance and identification cards.⁸ Until late 2008, DHS recognized that "SAVE is used to verify limited citizenship and immigration status of individuals seeking government benefits, licensure, or credentials based on their citizenship and immigration status," an acknowledgement that tracked the statutory authorizations.⁹

On December 11, 2008, DHS published a SORN that greatly expanded the use of the SAVE program beyond this scope, though Congress had not passed any legislation that would authorize the expansion.¹⁰ The agency expanded the use of SAVE for the broader purpose under 8 USC section 1373 of "respond[ing] to inquiries 'by a Federal, State, or local government agency, seeking to verify or ascertain the

⁵ DHS-2009-0015, *supra* note 3, at 24023.

⁶ Section 121 of the Immigration Reform and Control Act, Pub. L. 99-603, 100 Stat. 3359 (1986) (codified at 8 U.S.C. 1101 note).

⁷ *Id.* at § 121(a).

⁸ Pub. L. 109-13, 119 Stat. 231, 302 (2005) (codified at 49 U.S.C. 30301 note).

⁹ Privacy Impact Assessment for the Verification Information System, at 2 (September 4, 2007), *available at*

http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_uscis_vis_update.pdf

¹⁰ System of Records Notice for the USCIS Verification Information System (VIS) (DHS-2008-0089), 73 Fed. Reg. 75445 (proposed Dec. 11, 2008), *available at* <http://edocket.access.gpo.gov/2008/pdf/E8-29283.pdf>.

citizenship or immigration status of any individual within the jurisdiction of the agency *for any purpose authorized by law.*”¹¹

NILC submitted comments to DHS’s December SORN, criticizing SAVE’s expansion on the grounds that no federal law authorized it, and that it gave states and localities virtually unfettered ability to decide when and how they wish to use a federal database and immigration verification system.¹²

Although DHS gave itself permission to vastly expand the uses to which SAVE can be put only a few months ago, the instant SORN completely ignores this.¹³ In fact, it makes no mention of any expanded uses of SAVE, referring only to SAVE’s original slated use by benefit- and license-granting agencies.¹⁴

As a result, the monitoring and compliance that USCIS proposes is entirely inadequate to meet the expanded uses to which SAVE will be put. The SORN states that CTMS, as a monitoring and compliance tool, is charged with overseeing the “[f]ailure of [a] SAVE agency to initiate additional verification when necessary; unauthorized searching and use of information by a SAVE agency user; and fraudulent use of visas, permits, and other DHS documents by SAVE users.”¹⁵ The term “SAVE users” is necessarily more expansive than implied by this most recent SORN, and the definition of “unauthorized searching” also undoubtedly changes under the new “any DHS lawful purpose” regime.

Furthermore, the examples provided by the SORN as underlying reasons for implementing CTMS are entirely unrelated to the SAVE program. DHS cites issues faced by the M&C Branch such as SSN misuse in employment authorization verification and failure to conspicuously post notification of such verification procedure; however, these compliance failures are wholly E-Verify matters.

The need for monitoring and compliance which match the uses to which SAVE might be put is apparent. As NILC pointed out in its comments to the December 2008 SORN, in recent years, states and localities have passed many laws requiring verification of citizenship or immigration status for a variety of purposes. These laws repeatedly have been struck down when federal or state courts found that they

¹¹ *Id.* at 75446 (quoting Illegal Immigration Reform and Immigrant Responsibility Act § 642(c), Pub. L. 104-208, 110 Stat. 3009 (1996)) (emphasis added).

¹² Letter from Nat’l Immigration Law Ctr. to Hugh Teufel III, Chief Privacy Officer, Dep’t of Homeland Sec. (Jan. 12, 2009) (on file with author).

¹³ DHS cited to the December 11, 2008 SORN, but only to reference the Verification Information System (VIS). DHS-2009-0015, *supra* note 3, at 24023.

¹⁴ The May 22, 2009 SORN fails to acknowledge the December expansion of SAVE in its description of the program, referring only to its use by benefit- and license-granting agencies: “Congress mandated SAVE to provide government agencies with citizenship and immigration status information for use in determining an individual’s eligibility for government benefits. The SAVE program allows Federal, State, and local government benefit-granting agencies, as well as licensing bureaus and credentialing organizations to confirm the immigration status of non-citizen applicants, by submitting to SAVE certain information supplied by the benefit applicant.” *Id.*

¹⁵ DHS-2009-0015, *supra* note 3, at 24024.

regulate immigration and are pre-empted by federal law, or that they deny due process of law, or that they violate state law.¹⁶

Neither the December 2008 SORN nor the instant SORN offer even a hint of due process or privacy protections in how the system will be used by state and local government agencies. They do not require notice to affected individuals, consent for the system to be used regarding their citizenship or immigration status, reasonable access to records to correct information, redress if information is incorrect or a benefit is wrongly denied. Nor do they even require that information in the databases that are relied upon be accurate. Finally, they require no evaluation of how the system is used or whether it is reliable. In fact, the opposite is true. In a separate Privacy Act notice (which NILC will comment on separately), USCIS proposes to exempt the new system from Privacy Act protections.

An employer's election not to participate in E-Verify after it has registered for the program does not indicate employer misuse of the system.

Among the few employer behaviors that CTMS will be able to identify is the failure to use E-Verify following registration. Inexplicably, the choice not to use E-Verify following registration is listed in the SORN as a “non-compliant behavior.”¹⁷ For most categories of employers, E-Verify is a strictly voluntary program, and only about half of registered employers use E-Verify.¹⁸ Employers have many concerns with E-Verify that may cause them to decide not to participate in the program after they are registered, including the erroneous TNC rate, which for some businesses is as high as 12 percent,¹⁹ and the expense of hiring and training new employees when current employees are occupied with or unable to resolve TNCs. E-Verify is an expensive program for employers and employees alike, and in the midst of a weak economy, it is important that its optional nature remains clear.

USCIS proposes to use limited M&C resources regarding a measure that could well yield no compliance information, while at the same time ignoring the much wider problem of employer misuse of the system.

Despite its stated intentions, CTMS seems to be designed to investigate immigration offenses by employees and others.

The SORN states that CTMS will monitor misuse of E-Verify, which “includes” investigation of a broad category of employer and agency misuse of E-Verify and SAVE.²⁰ Although USCIS claims that compliance activities will focus on

¹⁶ See, e.g. *Lozano v. City of Hazleton*, 496 F. Supp. 2d 477 (M.D. Pa. 2007).

¹⁷ DHS-2009-0015, *supra* note 3, at 24024.

¹⁸ *Employment Verification; Challenges Exist in Implementing a Mandatory Electronic Employment Verification System: Hearing Before the Subcomm. on Immigration, Citizenship, Refugees, Border Security, and International Law of the H. Comm. on the Judiciary*, 110th Cong. 12 (2008) (statement of Richard M. Stana, Director, Homeland Security and Justice Issues), available at www.gao.gov/new.items/d08895t.pdf.

¹⁹ Intel Corporation, “Comments on Proposed Employment Eligibility Regulations Implementing Executive Order 12989 (as amended),” Aug. 8, 2008.

²⁰ DHS-2009-0015, *supra* note 3, at 24024.

government or agency users of the system rather than on the individuals verified,²¹ the SORN's language does not preclude the use of CTMS as an immigration enforcement tool. In fact, CTMS seems to be suited to identifying employee misconduct. The only specific ability of CTMS listed in the SORN is its capacity to identify multiple uses of a single Social Security Number (SSN).²² Such duplicate information tends to serve as evidence of document misuse, which is largely an immigration-related employee offense. The possibility that CTMS is targeted at employee offenses is further suggested by its ten-year period of record keeping, which is based on the statute of limitations for fraud and misuse of documents.²³ While it falls short in its ability to identify employer abuse, CTMS will easily identify immigration-related employee offenses, and the SORN says nothing to indicate that these offenses will not be prosecuted.

If M&C uses CTMS for immigration enforcement against employees or verification subjects, M&C's ability to address employer or agency abuse will decrease.

USCIS is not, and should not be, responsible for immigration enforcement. Immigration enforcement is the responsibility of ICE, and the characterization of CTMS in the SORN as a "law enforcement system" is therefore troubling. If USCIS participates in enforcing immigration law against employees or verification subjects, the complaints that M&C needs to enforce employer compliance with E-Verify regulations will not be forthcoming.

Foreign-born citizens and work-authorized immigrants are those most likely to be adversely affected by employers using E-Verify, and they are much less likely to complain publicly or to USCIS if they fear immigration consequences. Foreign-born workers are likely to be targeted for selective use of E-Verify, and they are the subjects of the vast majority of TNCs and negative employment actions taken in response to TNCs.²⁴ Therefore, immigrant complaints are vital to identify employer non-compliance with E-Verify regulations. Undocumented workers are not the only group that will fail to report employer abuse if M&C enforces immigration law; many immigrants may fear retaliatory immigration consequences even if they are lawfully present and authorized to work. If M&C enforces immigration law, foreign-born employees will remain silent, and the result will be impunity for employer violations while employees are investigated and prosecuted.

²¹ DHS-2009-0015, *supra* note 3, at 24024.

²² DHS-2009-0015, *supra* note 3, at 24023.

²³ DHS states: "Records collected in the process of establishing immigration and citizenship status or employment authorization are stored and retained in the VIS Repository for ten (10) years from the date of the completion of the verification unless the records are part of an ongoing investigation in which case they may be retained until completion of the investigation. This period is based on the statute of limitations for most types of misuse or fraud possible using VIS (under 18 U.S.C. 3291, the statute of limitations for false statements or misuse regarding passports, citizenship or naturalization documents)." DHS-2009-0015, *supra* note 3, at 24026.

²⁴ The E-Verify TNC rate is 10% for immigrants compared to .1% for native-born citizens. Findings of the Web-Based Basic Pilot Evaluation (Westat, Sept. 2007), *available at* <http://www.nilc.org/immsemplymnt/ircaempverif/WebBasicPilotRprtSept2007.pdf>.

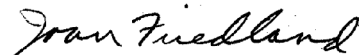
Provisions that freely share information in CTMS with law enforcement officials but keep employees from accessing their own records introduce serious privacy concerns and diminish M&C's ability to fight employer abuse.

The SORN not only leaves open the possibility of M&C being used to enforce immigration law against employees and other verification subjects, but actively provides for almost unlimited information sharing with law enforcement officials. Information sharing need only be "proper," and the records disclosed merely indicative of a "potential" violation of any type of law.²⁵ The potential violation may be informed by sources aside from the records; thus, the records of any person suspected of illegal activity may be disclosed absent any threshold of reasonable suspicion. The SORN does not suggest that state or local law enforcement agencies are bound by Privacy Act limits. Additionally, nothing in the SORN indicates that information shared with law enforcement officials will not be used to prosecute employees or other verification subjects, creating another disincentive for immigrant workers to approach M&C with information about employer violations.

Moreover, no provision in the SORN indicates that employees or verification subjects will be made aware of any disclosure of their records, as required by section (c) of the Privacy Act,²⁶ nor are they likely to have any opportunity to correct wrong and prejudicial information in them, as required by section (d)(2) of the Privacy Act.²⁷ Those who wish to see their records in CTMS must not only seek the favorable exercise of discretion by the Verification Division, which will "consider individual requests," but must also be able to specify where and why DHS would have such information as well as the date the record may have been created.²⁸ These requirements may be extremely prohibitive, considering the inherent imbalance between individuals and the government. The potential unacceptable result would be that M&C freely discloses information to law enforcement but carefully guards CTMS records from release to the subjects of the records.

Thank you for your consideration of these comments.

Sincerely,



Joan Friedland
Immigration Policy Director

²⁵ DHS-2009-0015, *supra* note 3, at 24026.

²⁶ 5 U.S.C. § 552a (1974).

²⁷ *Id.*

²⁸ DHS-2009-0015, *supra* note 3, at 24026-27.