NATIONAL
IMMIGRATION
LAW CENTER
www.nilc.org

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

June 22, 2009

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

Re: Comments on Docket Number DHS-2009-0013 Privacy Act of 1974: Implementation of Exemptions; U.S. Citizenship and Immigration Services 009 Compliance Tracking and Monitoring System (CTMS) 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: Implementation of Exemptions; U.S. Citizenship and Immigration Services 009 Compliance Tracking and Monitoring System (CTMS) Notice, 74 Fed. Reg., No. 98, pages 23957-23958 (May 22, 2009).

In its Notice of Proposed Rulemaking (NPRM),[1] DHS exempts CTMS from certain requirements of the Privacy Act of 1974, an act that safeguards privacy interests by placing limitations on the confidential information collected by the government. CTMS is a system of records to be operated by the Monitoring & Compliance Branch (M&C) of the U.S. Citizenship & Immigration Service (USCIS). M&C is tasked with using CTMS to identify abuse and misuse 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. SAVE is an electronic system which allows federal, state and local government agencies to verify immigration status. E-Verify is an electronic system which allows employers to verify new employees' work authorization. DHS announced its creation of CTMS in a concurrently filed System of Records Notice (SORN),[2] to which we have submitted comments as well.

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.

---

[1] Notice of Proposed Rulemaking for Implementation of Exemptions regarding USCIS Compliance Tracking and Monitoring System (DHS-2009-0013), 74 Fed. Reg. 23957 (proposed May 22, 2009).

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

DHS's Claim of a Law Enforcement Exemption is Overbroad and Unwarranted.

The NPRM cites subsection (k)(2) of the Privacy Act as the basis for DHS's proposed exemptions; this subsection generally allows an agency exemptions from specified subsections of the act if "the [exempted] system of records is investigatory material compiled for law enforcement purposes."[3] Claiming such purposes, DHS seeks to exempt CTMS from the maximum allowable Privacy Act subsections under (k)(2), specifically subsections (c)(3), (d), (e)(1), (e)(4)(G), (H), and (I), and (f).[4]

In order to claim any exemptions under (k)(2), the Privacy Act requires that law enforcement ends must be at stake. DHS claims that this is the case for what are otherwise administrative compliance activities, stating that "[s]ome information in CTMS is shared with and contributes to law enforcement activities of DHS components and other Federal agencies."[5] More specifically, DHS reasons that "the exemptions are required to preclude subjects of these [DHS] activities from frustrating USCIS monitoring and compliance processes and to avoid disclosure of research techniques, as these processes and techniques may inform law enforcement investigations."[6]

These explanations are inadequate. In its separate but concurrently filed SORN, DHS states: "Information in CTMS is used to prevent misuse and illegal activities. Consequently, this SORN has a routine use for sharing with Federal, State, local and Tribal law enforcement agencies, as well as for other standard DHS routine uses."[7] However, the inclusion of law enforcement as a method of correcting noncompliance or misuse of an administrative system is a much larger paradigmatic shift than DHS acknowledges in its NPRM and SORN. DHS itself cites other more traditional methods of reinforcing compliance, such as additional user training, assistance, and suspension for continued misuse.[8] E-Verify users, meanwhile, are subject to civil penalties pursuant to the INA, NLRA, and Title VII for discriminatory use of E-Verify.

DHS's claim of a law enforcement exemption is particularly overbroad given the agency's previous expansion of the uses to which SAVE may be put,[9] combined with its failure to acknowledge this expansion in the SORN which accompanies the NPRM. As we point out in comments to that SORN, DHS expanded the uses of SAVE in a December 2008 SORN to include use by states and localities for "any lawful purpose." However, in the current SORN, DHS reverts to a narrower description of the use of SAVE for benefits and licensing. Thus, the exemption has a much more substantial impact than DHS acknowledges.

---

[3] 5 U.S.C. § 552a (1974).
[4] DHS-2009-0013, *supra* note 1, at 23958.
[5] DHS-2009-0013, *supra* note 1, at 23957.
[6] *Id.*
[7] DHS-2009-0015, *supra* note 2, at 24024.
[8] *Id.*
[9] System of Records Notice for the USCIS Verification Information System (VIS) (DHS-2008-0089), 73 Fed. Reg. 75445, 75446 (proposed Dec. 11, 2008), *available at* http://edocket.access.gpo.gov/2008/pdf/E8-29283.pdf.

Proposed Exemption from subsection (c)(3)
Subsection (c)(3) of the Privacy Act requires that every individual have access to a record of all disclosures made of personal information collected by an agency that is subsequently disclosed to any person or other agency.[10] DHS bases its exemption claim on the grounds that such access "could alert the subject of an investigation of an actual or potential criminal, civil, or regulatory violation to the existence of the investigation, and reveal investigative interest on the part of DHS as well as the recipient agency" and thereby impede investigations.[11] However, DHS's concern appears overinclusive, preventing individuals not under DHS investigation from accessing information that was guaranteed them by the Privacy Act.

Among the information collected by CTMS are social security numbers, physical addresses, and immigration status information that, if wrongly disclosed, could create a risk of identity fraud or citizenship status discrimination. All disclosures involve risks to privacy at least as great as the risk of disrupting a criminal investigation, and individuals should be made aware when they have been exposed to such a risk.

Moreover, in the E-Verify context, transparency will aid, rather than injure, M&C's capacity to investigate user abuse of the program. If workers are made secure in their knowledge of all uses of information provided to M&C, they will be more likely to come forward to lodge complaints with M&C. In turn, M&C will be able to better fulfill its goal of monitoring employer compliance with E-Verify anti-discrimination provisions.

DHS cited no examples of SAVE-specific misuse either in this NPRM or its separately filed SORN to warrant such a broad exemption. When DHS expanded the uses to which SAVE could be put in its December 2008 SORN, it did not offer even a hint of due process or privacy protections in how the system is used by state and local government agencies. It did not require notice to affected individuals, consent for the system to be used regarding their citizenship or immigration status, access to records to correct information, redress if information is incorrect or a benefit is wrongly denied. Nor did it even require that information in the databases that are relied upon be accurate. Finally, it required no evaluation of how the system is used or whether it is reliable. Under these circumstances, exempting CTMS from the requirement that individuals have access to a record of all disclosures made of personal information collected by an agency that is subsequently disclosed to any person or other agency is unwarranted.

Proposed Exemption from subsection (d)
Subsection (d) of the Privacy Act requires that every individual have access to records kept relating to him, the ability to amend or correct his records, as well as the ability to seek review of agency actions pertaining to amendment of such records.[12] DHS bases its exemption on grounds similar to those above, that "access to the records contained in this system of records could inform the subject of an investigation of an actual or potential criminal, civil, or regulatory violation, to the

[10] 5 U.S.C. § 552a.
[11] DHS-2009-0013, *supra* note 1, at 23958.
[12] 5 U.S.C. § 552a.

existence of the investigation, and reveal investigative interest on the part of DHS or another agency" and thereby impede investigations.[13] For the same reasons as above, DHS has not adequately justified its claim of exemption. The ability to access and correct records and seek review of agency actions are fundamental aspects of due process of law.

DHS further states that "[a]mendment of the records could interfere with ongoing investigations and law enforcement activities and would impose an impossible administrative burden by requiring investigations to be continuously reinvestigated."[14] Such interference is entirely speculative.

The hypothetical situations provided by DHS in its NPRM are simply insufficient to justify the ramifications for affected individuals. Essentially, they would be unable to access their records in CTMS, nor would they be able to apply for corrections of erroneous information on the speculative basis that they might frustrate investigative purposes. In reality, this exemption might paradoxically lead to administratively burdensome results because investigations might be based on erroneous information that could have been corrected by the individual.

For workers whose employers participate in E-Verify, the right to correct records maintained in CTMS is crucial. The SSA and DHS records on which CTMS will rely are not regularly updated. In fact, SSA estimates that 17.8 million errors exist in its database.[15] Incorrect records of immigration status or social security number may result in non-confirmations of employment authorization that leave workers unemployed for long periods of time and cost employers time and money while workers contest non-confirmations. Even worse, incorrect records may lead to unwarranted criminal investigations of workers for fraud or identity theft. If a worker could simply access his information and contest inaccuracies before they result in a non-confirmation or an investigation, negative employment consequences of SSA and DHS errors would be minimized, and investigations of innocent employees might be prevented.

Proposed Exemption from subsection (e)(1)

Subsection (e)(1) of the Privacy Act requires that agencies maintain the least amount of information possible on an individual in their systems of record.[16] DHS bases its claim of exemption on the grounds that a limited amount of information may result in unclear or irrelevant information to its investigative purposes, and that it is therefore "appropriate to retain all information that may aid in establishing patterns of unlawful activity."[17] This line of reasoning seems to wholly and unnecessarily disregard the protections that the Privacy Act sought for individuals in the first place, preempting these protections with investigative priorities.

---

[13] DHS-2009-0013, *supra* note 1, at 23958.
[14] *Id.*
[15] OFFICE OF THE INSPECTOR GENERAL, SOCIAL SECURITY ADMINISTRATION, CONGRESSIONAL RESPONSE REPORT: ACCURACY OF THE SOCIAL SECURITY ADMINISTRATION'S NUMIDENT FILE (Dec. 2006), *available at* http://www.ssa.gov/oig/ADOBEPDF/A-08-06-26100.pdf.
[16] 5 U.S.C. § 552a.
[17] DHS-2009-0013, *supra* note 1, at 23958.

As cited above, DHS's proposed exemption from subsection (d) may result in maintenance of inaccurate records; here, DHS seems to attempt to resolve the issue by collecting *more* information from the individual. This seems like not only a clear violation of privacy safeguards, but an example of the tail wagging the dog. Essentially, investigations of noncompliance, which are ostensibly only one of many proposed compliance solutions, would single-handedly allow CTMS to expand its information collecting ability.

Allowing the information in CTMS to expand without limits is worrisome because, given the expanded use of the SAVE program, the information to which DHS has access is extremely broad. Failure to limit the information available through CTMS may harm workers by allowing characteristics beyond work authorization to be discovered as a basis for employment decisions or selective enforcement of immigration law. It may also allow the storage of more than the necessary amount of information to address worker complaints, such as complainants' immigration status, which would stifle complaints and stymie enforcement efforts against employers.

Proposed Exemptions from subsections (e)(4)(G), (H), and (I), and (f)
Subsections (e)(4)(G), (H), and (I) of the Privacy Act require agencies to publish notices whenever a system of record is established or revised on how an individual could be alerted if a record was kept on him, how he might access his record and possibly correct it, as well as information on the system's categories of sources.[18] Subsection (f) similarly requires agencies keeping systems of record to make rules establishing procedures on how an individual might interact with such systems, regarding any requests for records relating to him, requests to correct such records, and procedures for review available to him.[19] DHS bases its exemption on the grounds that rulemaking is irrelevant in the face of its previous proposition to exempt itself from subsection (d). By eliminating the original requirement that an individual have access to his relevant records and ability to amend it, DHS would not be required to promulgate rules implementing that requirement. We refer back to our comments under DHS's proposed exemption under subsection (d) in opposing this exemption.

For the aforementioned reasons, NILC urges DHS to withdraw its proposed claim of Privacy Act exemptions.

Thank you for your consideration of these comments.

Sincerely,

Joan Friedland

Joan Friedland
Immigration Policy Director

---

[18] 5 U.S.C. § 552a.
[19] 5 U.S.C. § 552a.