COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

to

DEPARTMENT OF HOMELAND SECURITY
Docket No. DHS-2007-0066

I. INTRODUCTION

By notice published on February 28, 2008, the Department of Homeland Security ("DHS") announced a notice to alter a system of records and revised Privacy Impact Assessment ("PIA") for the Verification Information System, which is operated by the U.S. Citizenship and Immigration Services ("CIS").[1] The Verification Information System gathers and accesses a vast amount of personal data on citizens and immigrants and uses this data to underpin the federal government's Employment Eligibility Verification System. DHS seeks to:

> (1.) Add two new categories of records one derived from the Computer Linked Application Information Management System (CLAIMS 4) (62 FR 11919), and the other derived from the Redesigned Naturalization Automated Caseworker Systems (RNACS) (67 FR 20996);
> (2.) update the category of records derived from Treasury Enforcement Communication Systems (TECS) (66 FR 52984) to include Real Time Arrivals (RTA) data;
> (3.) correct the categories of individuals to include United States (U.S.) citizens;
> (4.) reflect changes to the verification process of expanded use of the Photo Screening Tool to make it mandatory for all employers that are verifying employment eligibility of their non-U.S. citizen employees if the individual's photo is on file with United States Citizenship and Immigration Service (USCIS) in the Biometric Storage System (72 FR 17172); and
> (5.) update the routine uses to remove routine use L. for the sharing of VIS data because the other routine uses cover the allowable extent of sharing from VIS.[2]

The Electronic Privacy Information Center ("EPIC") has analyzed and testified about databases and verification programs used by federal entities. In June 2007

---

[1] Dep't of Homeland Sec., *Notice to Alter a Privacy Act System of Records*, 73 Fed. Reg. 10,793 (Feb. 28, 2008) [hereinafter "Notice of Changes to VIS"], *available at* http://edocket.access.gpo.gov/2008/E8-3833.htm; and Privacy Office, Dep't of Homeland Sec., *Privacy Impact Assessment for the Verification Information System Supporting Verification Programs*, Feb. 22, 2008 [hereinafter "VIS Revised Privacy Impact Assessment"], *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_cis_vis_update_ver.pdf.

[2] Notice of Changes to VIS at 10,793, *supra* note 1.

Congressional testimony, EPIC Executive Director Marc Rotenberg urged Congressmembers to strengthen privacy and security safeguards associated with employment eligibility verification systems and the underlying databases, including VIS.[3] In February 2007, we explained that the Transportation Security Administration's "internal quality assurance procedures" were not working, and urged the agency to fully apply Privacy Act requirements of notice, access, and correction to the new traveler redress program called "TRIP" and its underlying watch list system.[4] In Congressional testimony in 2005, Executive Director Rotenberg also described some of the problems that would likely result from a poorly designed employment eligibility system, and some changes were made to EEVS based on EPIC's recommendations.[5] EPIC has analyzed flaws in such systems in a number of reports.[6]

Today we write to urge the Department of Homeland Security to ensure that Privacy Act obligations are applied to the Verification Information System and the Employment Eligibility Verification System. The systems should not be exempted from key fair information practices, required by the Privacy Act, such as the requirements that an individual be permitted access to personal information, that an individual be permitted to correct and amend personal information, and that an agency assure the reliability of personal information for its intended use. With the Employment Eligibility Verification

---

[3] Marc Rotenberg, Exec. Dir., EPIC, *Testimony and Statement for the Record at a Hearing on Employment Eligibility Verification Systems (EEVS) Before the Subcomm. on Social Sec., H. Comm on Ways & Means,* 110th Cong. (June 7, 2007), *available at* http://www.epic.org/privacy/ssn/eevs_test_060707.pdf.

[4] EPIC, *Comments on Docket Nos. DHS-2007-0003: Implementation of Exemptions; Redress and Response Records System* (Feb. 20, 2007), *available at* http://www.epic.org/privacy/airtravel/profiling/trip_022007.pdf.

[5] Marc Rotenberg, Exec. Dir., EPIC, *Testimony and Statement for the Record at a Hearing on H.R. 98, the "Illegal Immigration Enforcement and Social Security Protection Act of 2005," Before the Subcomm. on Immigration, Border Sec., and Claims, H. Comm on the Judiciary,* 109th Cong. (May 12, 2005)*, available at* http://www.epic.org/privacy/ssn/51205.pdf.

[6] *See* EPIC, Social Security Numbers, http://epic.org/privacy/ssn/; EPIC, Secure Flight, http://www.epic.org/privacy/airtravel/secureflight.html; and EPIC, National ID Cards and the REAL ID Act, http://epic.org/privacy/id-cards/.

System, DHS is attempting to gain the authority to determine employment eligibility for virtually all Americans in the workforce. It is inconceivable that the drafters of the Privacy Act would have permitted such a system to be granted broad exemptions from Privacy Act obligations. Consistent and broad application of the Privacy Act obligations are the best means of ensuring accuracy and reliability of the data used in a system that profoundly affects Americans' employment.

II. WHAT IS THE VERIFICATION INFORMATION SYSTEM ("VIS")?

According to the Department of Homeland Security, "Verification Information System (VIS) is the technical infrastructure that enables USCIS to operate [its employment eligibility verification system]. VIS is a nationally accessible database of selected immigration status information containing in excess of 100 million records."[7] DHS says, "VIS is currently comprised of citizenship, immigration and employment status information from several DHS systems of records, including" Treasury Enforcement Communication Systems, Biometric Storage System, USCIS Central Index System, USCIS Computer Linked Application Information Management System, Immigration and Customs Enforcement's Student and Exchange Visitor Information System (SEVIS), and the Social Security Administration's NUMIDENT System.[8] In short, VIS gathers and accesses a vast amount of personal data on citizens and immigrants and uses this data to underpin the federal government's employment eligibility verification system.

[7] Notice of Changes to VIS at 10,793, *supra* note 1.
[8] *Id*. at 10,793-794.

III. HISTORY OF EMPLOYMENT ELIGIBILITY VERIFICATION

The Immigration Reform and Control Act of 1986 ("IRCA") made it illegal for employers to "knowingly" employ unauthorized workers, and E-Verify (then known as "Basic Pilot") grew out of the requirement for work-eligibility verification.[9] Basic Pilot, a joint project of U.S. Customs and Immigration Services and the Social Security Administration, is an electronic employment eligibility verification system created in 1997 and implemented in all 50 states.[10] The program was initially voluntary for all employers, but, as explained in the next section, this has changed.[11]

A new employee is required to fill out an Employment Eligibility Verification form (commonly known as an I-9 form) stating that she is authorized to work in the United States, and produce identification documents.[12] This identification can be a configuration of one or two documents from a list of 29 possible items, including U.S. passport, driver's license, Social Security card, and school ID card.[13] Employers do not need to verify the authenticity of the ID documents, but they do need to keep a copy of them on file: for three years after the date or hire or one year after the date employment ends, whichever is later.[14] The documents must merely pass a good-faith test: Do they look real? If an employee is found to be unauthorized, the employer must terminate her

[9] Immigration Reform and Control Act, 8 U.S.C. §1324a (1986), supplanted by Illegal Immigration Reform and Immigrant Responsibility Act, 8 U.S.C. §1324a(b) (1996) ["IRIRA"].
[10] *Id*., Basic Pilot Extension Act, Pub. L. No. 107-128 (2001); and Basic Pilot Program Extension and Expansion Act, Pub. L. No. 108-156 (2003).
[11] Press Release, Dep't of Homeland Sec., Fact Sheet: Improving Border Security and Immigration Within Existing Law (Aug. 10, 2007) ["DHS Press Release on E-Verify"], *available at* http://www.dhs.gov/xnews/releases/pr_1186757867585.shtm.
[12] IRIRA, *supra* note 9.
[13] Employment Eligibility Immigration Form (Form I-9), OMB No. 1615-0047, at 3.
[14] IRIRA, *supra* note 9.

employment. Employers who do not fire unauthorized workers or who knowingly hire unauthorized workers face fines and other sanctions.[15]

An employer can voluntarily sign up for the E-Verify program. In E-Verify, an employer fills out an online form with the new employee's name, date of birth and Social Security Number, and if the new hire states she is not a U.S. citizen, the "A" Number or I-94 Number within three days of the employee's hire date.[16] This information is checked against Social Security Administration databases "to verify the name, SSN, and date of birth of newly-hired employees, regardless of citizenship."[17] The SSA "maintains a record of each Social Security card, both original and replacement cards, in a system of records called the Numerical Identification File ("NUMIDENT")."[18] NUMIDENT includes "all relevant data connected to the issuance of the Social Security card, including the appropriate codes related to citizenship status and the type of Social Security card issued."[19] (There are three types of Social Security cards, and an individual is assigned a particular type dependent on the citizenship status and work-authorization status of the individual.[20])

---

[15] *Id*.
[16] Office of Inspector Gen., Soc. Sec. Admin, *Congressional Response Report: Accuracy of the Social Security Administration's Numident File, A-08-06-26100*, Appendix D (Dec. 18, 2006) ["Inspector General Report on SSA Database"], *available at* http://www.ssa.gov/oig/ADOBEPDF/A-08-06-26100.pdf.
[17] *Id*.
[18] Inst. for Survey Research, Temple Univ., and Westat, *Findings of the Basic Pilot Evaluation* (June 2002) ["Detailed Independent Analysis of Basic Pilot"], *available at* http://www.uscis.gov/portal/site/uscis/menuitem.5af9bb95919f35e66f614176543f6d1a/?vgnextoid=9cc5d0676988d010VgnVCM1130048f3d6a1RCRD&vgnextchannel=2c039c7755cb9010VgnVCM1130045f3d6a1RCRD.
[19] *Id*. at 35.
[20] "The three types of cards appear to be identical except for the presence or absence of a particular legend. The type of card issued to U.S. citizens and lawful permanent residents, refugees, and asylees has no legend. A Social Security card with the legend 'Valid for work only with INS Authorization' is issued to noncitizens with temporary work authorization. Noncitizens without work authorization who have a legitimate non- work reason for having a Social Security number are issued cards that include the legend 'Not Valid for Employment.'" *Id*.

If the work authorization cannot be determined by the information in the SSA databases or if the employee is a non-citizen, her data is then checked against the Department of Homeland Security databases to verify employment eligibility.[21] If eligibility cannot be confirmed, E-Verify sends a "tentative nonconfirmation" of work authorization status to the employer.[22] There are several reasons for a "tentative nonconfirmation" determination including, "when the SSN, name, or date of birth does not match the information in SSA's database or if a death indicator is present," "if the new hire indicated he or she was a U.S. citizen and SSA's records did not show that the person was a U.S. citizen," or if "DHS' database does not show the newly-hired noncitizen as authorized for employment."[23]

The employer must inform the employee of the "tentative nonconfirmation" and the employee has eight business days to contest this decision.[24] If the employee contests the determination, SSA or DHS "is required to determine work-authorization status within 10 Federal working days."[25] If the review by DHS or SSA still cannot determine if the employee is eligible to work in the United States, a "final nonconfirmation" is issued.[26] A "final nonconfirmation" also is issued if the employee does not contest the "tentative nonconfirmation."[27] A "final nonconfirmation" means the employee must be fired or the employer faces federal sanctions.[28] This employment eligibility verification process has been changed recently.

---

[21] Inspector General Report on SSA Database at Appendix D, *supra* note 16.
[22] *Id*.
[23] *Id*.
[24] *Id*.
[25] Detailed Independent Analysis of Basic Pilot at 44, *supra* note 18.
[26] Inspector General Report on SSA Database at Appendix D, *supra* note 16.
[27] Detailed Independent Analysis of Basic Pilot at 44, *supra* note 18.
[28] Inspector General Report on SSA Database at Appendix D, *supra* note 16.

IV. CHANGES TO THE EMPLOYMENT ELIGIBILITY VERIFICATION SYSTEM

Last year, Homeland Security Secretary Michael Chertoff announced several changes to the employment eligibility verification program ("EEVS").[29] The agency will require more than 200,000 federal contractors to use EEVS, an increase of more than 1,076 percent over the 17,000 employers that were then registered in EEVS.[30] The system will use an "enhanced photograph capability" that will allow employers to check photographs in EEVS databases.[31] DHS will expand the number of databases EEVS checks to include visa and passport databases; and the agency is asking states to "voluntarily" allow DHS access to their motor vehicle databases.[32]

DHS also will require employers to fire employees if they were unable to resolve "no match" discrepancies within 90 days.[33] If the employers do not terminate the workers' employment, the businesses would face fines of $11,000 or more.[34] DHS also will raise fines against employers by 25 percent and increasingly use criminal action against employers, as opposed to administrative action.[35]

DHS's announced changes to EEVS came after two bills that would have created a nationwide, mandatory employment eligibility verification system failed in Congress.[36] An examination of H.R. 1645 and S. AMDT 1150 by EPIC found that the proposed

---

[29] DHS Press Release on E-Verify, *supra* note 11.
[30] *Id*.
[31] *Id*.
[32] *Id*.
[33] Dep't of Homeland Sec., *Safe-Harbor Procedures for Employers Who Receive a No-Match Letter: Final Rule*, 72 Fed. Reg. 45,611, 45,617, Aug. 15, 2007, *available at* http://edocket.access.gpo.gov/2007/E7-16066.htm.
[34] *Id*. at 45,612 –14.
[35] DHS Press Release on E-Verify, *supra* note 11.
[36] Security Through Regularized Immigration and a Vibrant Economy Act, of 2007, H.R. 1645, 110th Cong. (2007), *available at* http://www.epic.org/privacy/surveillance/spotlight/0507/hr1645.pdf; Secure Borders, Economic Opportunity and Immigration Reform Act of 2007, S.AMDT. 1150 to S. 1348, 110th Cong. (2007), *available at* http://www.epic.org/privacy/surveillance/spotlight/0507/samdt1150.pdf.

changes would make the already-flawed identification systems worse for both U.S. citizens and documented immigrants.[37] Though the Department of Homeland Security has yet to find solutions to problems in the current EEVS system, it has chosen to expand data collection and data sharing, creating even more opportunities for errors.

V. EEVS BROAD EXEMPTIONS CONTRAVENE INTENT OF PRIVACY ACT OF 1974

When it enacted the Privacy Act in 1974, Congress sought to restrict the amount of personal data that Federal agencies could collect and required agencies to be transparent in their information practices.[38] In 2004, the Supreme Court underscored the importance of the Privacy Act's restrictions upon agency use of personal data to protect privacy interests, noting that:

> [I]n order to protect the privacy of individuals identified in information systems maintained by Federal agencies, it is necessary . . . to regulate the collection, maintenance, use, and dissemination of information by such agencies." Privacy Act of 1974, §2(a)(5), 88 Stat. 1896. The Act gives agencies detailed instructions for managing their records and provides for various sorts of civil relief to individuals aggrieved by failures on the Government's part to comply with the requirements.[39]

The Privacy Act is intended "to promote accountability, responsibility, legislative oversight, and open government with respect to the use of computer technology in the personal information systems and data banks of the Federal Government[.]"[40] It is also intended to protect the privacy interests of citizens and lawful permanent residents against government intrusion. Congress found that "the privacy of an individual is directly affected by the collection, maintenance, use, and dissemination of personal information by Federal agencies," and recognized that "the right to privacy is a personal

---

[37] EPIC, Spotlight on Surveillance, *National Employment Database Could Prevent Millions of Citizens From Obtaining Jobs* (May 2007), http://www.epic.org/privacy/surveillance/spotlight/0507/.
[38] S. Rep. No. 93-1183 at 1 (1974).
[39] *Doe v. Chao*, 540 U.S. 614, 618 (2004).
[40] S. Rep. No. 93-1183 at 1.

and fundamental right protected by the Constitution of the United States."[41] It thus sought to "provide certain protections for an individual against an invasion of personal privacy" by establishing a set of procedural and substantive rights.[42]

The rights of access and correction were central to what Congress sought to achieve through the Privacy Act:

> The committee believes that this provision is essential to achieve an important objective of the legislation: Ensuring that individuals know what Federal records are maintained about them and have the opportunity to correct those records. The provision should also encourage fulfillment of another important objective: maintaining government records about individuals with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to individuals in making determinations about them.[43]

Adherence to Privacy Act requirements is critical for a system such as the Employment Eligibility Verification System and its underlying systems, including the Verification Information System. As DHS has explained, VIS "is the technical infrastructure that enables USCIS to operate SAVE and E-Verify. VIS is a nationally accessible database of selected immigration status information containing in excess of 100 million records."[44]

In the recent Notice to Alter a Privacy Act System of Records, the Department of Homeland Security claims no Privacy Act exemptions.[45] However, "VIS is currently comprised of citizenship, immigration and employment status information from several DHS systems of records, including" Treasury Enforcement Communication Systems, Biometric Storage System, USCIS Central Index System, USCIS Computer Linked Application Information Management System, Immigration and Customs Enforcement's

---

[41] 5 U.S.C. § 552a.
[42] *Id*.
[43] H.R. Rep. No. 93-1416, at 15 (1974).
[44] Notice of Changes to VIS at 10,793, *supra* note 1.
[45] *Id*. at 10,798.

Student and Exchange Visitor Information System (SEVIS), and the Social Security Administration's NUMIDENT System.[46] These database systems claim numerous Privacy Act exemptions.

For example, VIS gathers information from Treasury Enforcement Communications System ("TECS"), a database that the government says contains "every possible type of information from a variety of Federal, state and local sources," including the FBI's National Criminal Information Center and state motor vehicle records.[47] TECS is exempted from key fair information practices, such as the requirements that an individual be permitted access to personal information, that an individual be permitted to correct and amend personal information, and that an agency assure the reliability of personal information for its intended use.[48]

According to the Treasury Department, TECS "is exempt from 5 U.S.C. 552a (c)(3), (c)(4), (d)(1), (d)(2), (d)(3), (d)(4), (e)(1), (e)(2), (e)(3), (e)(4)(G), (H) and (I), (5) and (8), (f) and (g) of the Privacy Act pursuant to 5 U.S.C. 552a (j)(2) and (k)(2)."[49] These provisions of the Privacy Act ensure:

- an agency must give individuals access to the accounting of disclosure of their records[50];
- any agency or individual to whom the records are disclosed must also receive "any correction or notation of dispute"[51];
- individual may request access to records an agency maintains about him or her[52];

[46] *Id*. at 10,793-94.
[47] Dep't of the Treasury, *Notice of Privacy Act System of Records*, 66 Fed. Reg. 52,983, 53,029 (Oct. 18, 2001) [hereinafter "TECS Privacy Act Notice"], *available at* http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=2001_register&docid=f:18ocn2.pdf.
[48] *See generally* 5 U.S.C. § 552a (1974).
[49] TECS Privacy Act Notice at 53,029, *supra* note 47.
[50] 5 U.S.C. § 552a(c)(3).
[51] 5 U.S.C. § 552a(c)(4).
[52] 5 U.S.C. § 552a(d)(1).

- an agency must correct identified inaccuracies promptly;[53]
- an agency must make notes of requested amendments within the records;[54]
- an agency must ensure it only collects data "relevant and necessary to accomplish a purpose of the agency required to be accomplished by statute or by Executive order of the President"[55];
- an agency must "collect information to the greatest extent practicable directly from the subject individual when the information may result in adverse determinations about an individual's rights, benefits, and privileges under Federal programs"[56];
- each individual must be informed whom the agency asks to supply information[57];
- an agency must publish a notice of the existence of records in the Federal Register, along with the procedures to be followed to obtain access[58];
- an agency must establish procedures to handle disputes between the agency and individual as to the accuracy of the records[59]; and,
- an individual may seek judicial review to enforce the statutory right of access provided by the Act.[60]

With EEVS, the Department of Homeland Security is attempting to gain the authority to determine employment eligibility for virtually all Americans in the workforce. It is inconceivable that the drafters of the Privacy Act would have permitted such a system to be granted broad exemptions from Privacy Act obligations.

VI. Privacy Act Protections Are Especially Needed Because of Data Security and Accuracy Problems

a. DHS and Other Federal Agencies Face Significant Data Security Problems

[53] 5 U.S.C. § 552a(d)(2)(B), (d)(3).
[54] 5 U.S.C. § 552a(d)(4).
[55] 5 U.S.C. § 552a(e)(1).
[56] 5 U.S.C. § 552a(e)(2).
[57] 5 U.S.C. § 552a(e)(3).
[58] 5 U.S.C. §§ 552a(e)(4)(G), (e)(4)(H), (f).
[59] 5 U.S.C. § 552a(f)(4).
[60] 5 U.S.C. § 552a(g)(1).

The Department of Homeland Security's EEVS program raises unprecedented privacy and security concerns. Various federal agencies, including DHS, have suffered serious data security breaches in recent years.

Incredibly, the Department of Homeland Security last year reported that it experienced 844 "cybersecurity incidents" in Fiscal Years 2005 and 2006.[61] Among these security breaches: "A workstation was infected with a Trojan scanning for port 137, an event that clearly demonstrated individuals attempting to scan DHS systems through the internet," "Unauthorized individuals gaining access to DHS equipment and data," and "numerous 'Classified data spillages."[62]

In June, a critical component of the Department of Homeland Security lost the employment records of 100,000 federal employees.[63] That missing data drive contained the names, Social Security numbers, dates of birth, payroll history and detailed bank account information for every person hired by Transportation Security Administration ("TSA") between January 2002 and August 2005, including federal air marshals who fly undercover to help safeguard commercial aviation in the United States.[64] While the privacy office of the TSA responded promptly once the problem was uncovered, the consequences of that data breach are truly staggering. Also in June, the Government Accountability Office released a report about security breaches in both private and public sectors. The title explains the report's findings, "PERSONAL INFORMATION: Data

---

[61] James R. Langevin, Chairman, Subcom. on Emerging Threats, Cybersec., & Sci. & Tech., H. Comm. on Homeland Sec., Opening *Statement at a Hearing on "Hacking the Homeland: Investigating Cybersecurity Vulnerabilities at the Department of Homeland Security,"* 110th Cong., June 20, 2007, *available at* http://homeland.house.gov/SiteDocuments/20070620144327-44568.pdf.
[62] *Id*. at 2.
[63] Press Release, Transp. Sec. Admin., TSA Public Statement on Employee Data Security (May 2007), *available at* http://www.tsa.gov/datasecurity/statement_05-07-2007.shtm.
[64] *Id*.

Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown."[65]

In October 2006, the U.S. House of Representatives Government Reform Committee released a report detailing federal agency data breaches from January 2003 to July 2006.[66] The Department of Homeland Security was one of 17 agencies that reported breaches involving the loss or compromise of sensitive personal information.[67] In all, the agencies reported almost 800 incidents of security breaches.

These security breaches occur at a time of growing concern about identity theft, and they raise serious questions about the ability of the Department of Homeland Security to safeguard the sensitive data of American workers.

b. DHS AND OTHER FEDERAL AGENCIES HAVE SIGNIFICANT DATA ACCURACY PROBLEMS

Another complication with VIS and EEVS is that the majority of such "tentative nonconfirmations" occur because of a significant problem in the systems: Information in the databases queried is incorrect or untimely. These databases have high error rates in determining work eligibility status, causing these verification problems and backlogs. In a 1997 report and a 2002 follow-up review, the Inspector General of the Department of Justice found that data from the Immigration and Naturalization Service (the predecessor of U.S. Citizenship and Immigration Services), which E-Verify queries, was unreliable

[65] Gov't Accountability Office, *PERSONAL INFORMATION: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, GAO-07-737 (June 2007), *available at* http://www.gao.gov/new.items/d07737.pdf.
[66] Staff of H. Com. on Gov't Reform Com, 109th Cong., *Agency Data Breaches Since January 1, 2003* (Oct. 13, 2006), *available at* http://oversight.house.gov/documents/20061013145352-82231.pdf.
[67] *Id*. at 8.

and "flawed in content and accuracy."[68] In August 2005, the Government Accountability Office investigated and found errors in information from Department of Homeland Security databases.[69]

A December 2006 report by the Social Security Administration's Office of Inspector General also found accuracy problems in databases of Citizenship and Immigration Services and Social Security Administration.[70] SSA's Numerical Identification File ("NUMIDENT") is used to check employment eligibility status, but the Inspector General estimated that about 17.8 million records in NUMIDENT have discrepancies with name, date of birth or death, or citizenship status.[71] About 13 million of these incorrect records belong to U.S. citizens.[72] About 15.3 percent of the U.S. workforce is foreign-born, according to the Bureau of Labor and Statistics.[73]

In an October opinion granting a temporary restraining order enjoining the Department of Homeland Security from implementing a new "no-match" employment eligibility verification proposal, the federal judge noted, "the government recognizes, the no-match letters are based on SSA records that include numerous errors."[74] In the final rule for REAL ID implementation (released in January), Department of Homeland

---

[68] Office of Inspector Gen., Dep't of Justice, *Immigration and Naturalization Service Monitoring of Nonimmigrant Overstays, Rept. No. I-97-08* (Sept. 1997), *available at* http://www.usdoj.gov/oig/reports/INS/e9708/index.htm; *Follow-Up Report on INS Efforts to Improve the Control of Nonimmigrant Overstays, Rept. No. I-2002-006* (Apr. 2002), *available at* http://www.usdoj.gov/oig/reports/INS/e0206/index.htm/; and *Immigration and Naturalization Service's Ability to Provide Timely and Accurate Alien Information to the Social Security Administration, Rept. No. I-2003-001* (Nov. 2002), *available at* http://www.usdoj.gov/oig/reports/INS/e0301/final.pdf.

[69] Gov't Accountability Office, *Immigration Enforcement: Weaknesses Hinder Employment Verification and Worksite Enforcement Efforts, GAO-05-813* 25 (Aug. 2005), *available at* http://www.gao.gov/new.items/d05813.pdf.

[70] Inspector General Report on SSA Database at 15, *supra* note 16.

[71] *Id.* at 6.

[72] *Id*. at Appendix C-2.

[73] Press Release, Bureau of Labor Statistics, Foreign-Born Workers: Labor Force Characteristics In 2006 (Apr. 25, 2007), *available at* http://www.bls.gov/news.release/pdf/forbrn.pdf.

[74] AFL-CIO v. Chertoff, No. C 07-04472 CRB (N.D. Cal. 2007), *available at* http://www.aclu.org/images/asset_upload_file505_32133.pdf.

Security admitted there are accuracy and reliability problems in SSOLV said that it, AAMVA, and the States are working with SSA to attempt to solve these problems.[75] Such erroneous records could lead to "tentative" or "final nonconfirmation" notices for affected employees.[76]

The Federal Register notice for VIS attempts to address the problem of erroneous records. The Department of Homeland Security states:

> In order to improve the accuracy of VIS and to reduce the number of [tentative nonconfirmations] or data mismatches issued by [EEVS], as well as reduce the number of Additional Verification Requests issued by the SAVE program, USCIS is adding data from two systems which it did not previously receive data--USCIS RNACS, USCIS CLAIMS 4-- and automated access to data from a system which it previously received other information--Real Time Arrival (RTA) data from [Customs and Border Protection's] TECS.[77]

However, this addition of data systems to VIS and EEVS will not solve the tentative nonconfirmation issue. The problem is not the amount of data gathered, but the accuracy of the data queried. The best and most effective option for ensuring accuracy and completeness of data in these systems is for the Department of Homeland Security to fully apply Privacy Act obligations of access, correction, and that an agency assure the reliability of personal information for its intended use.

VII. CONCLUSION

The Verification Information System gathers and accesses a vast amount of personal data on citizens and immigrants and uses this data to underpin the federal government's Employment Eligibility Verification System. With these systems, the Department of Homeland Security is attempting to gain the authority to determine

---

[75] Dep't of Homeland Sec., *Final Rule, Minimum Standards for Driver's Licenses and Identification Cards Acceptable by Federal Agencies for Official Purposes*, 73 Fed. Reg. 5271, 5297 (Jan. 29, 2008), *available at* http://edocket.access.gpo.gov/2008/08-140.htm.
[76] Inspector General Report on SSA Database at 6, *supra* note 16.
[77] Notice of Changes to VIS at 10,794, *supra* note 1.

employment eligibility for virtually all Americans in the workforce. It is inconceivable that the drafters of the Privacy Act would have permitted such a system to be granted broad exemptions from Privacy Act obligations. Keeping huge quantities of personal information in such a centralized government database enhances the appeal of that database to those who will attempt to misuse it. If that database is compromised in the same way that various other government databases have been, the fact that it contains such voluminous and detailed information makes the breach that much more serious. For the reasons detailed above, EPIC urges the Department of Homeland Security to apply all of the Privacy Act of 1974 obligations to VIS and EEVS.

Respectfully submitted,

Marc Rotenberg
Executive Director

Melissa Ngo
Senior Counsel

ELECTRONIC PRIVACY
INFORMATION CENTER
1718 CONNECTICUT AVENUE, N.W.
SUITE 200
WASHINGTON, DC 20009
(202) 483-1140

FILED: MARCH 31, 2008