epic.org

ELECTRONIC PRIVACY INFORMATION CENTER

Testimony and Statement for the Record of

Marc Rotenberg
President, EPIC

Hearing on

Employment Eligibility Verification Systems (EEVS)

Before the

Subcommittee on Social Security
Committee on Ways and Means,
U.S. House of Representatives

June 7, 2007
B-318 Rayburn House Office Building
Washington, DC

Introduction

Chairman McNulty, Ranking Member Johnson, and Members of the Subcommittee, thank you for the opportunity to testify on proposed employment eligibility verification systems (EEVS) and their relationship with the Social Security Administration.

My name is Marc Rotenberg and I am the Executive Director of the Electronic Privacy Information Center (EPIC). EPIC is a non-partisan research organization based in Washington, D.C. Founded in 1994, EPIC has participated in leading cases involving the privacy of the Social Security Number (SSN) and has frequently testified in Congress about the need to establish privacy safeguards for the SSN.[1] Last year, I testified before this Subcommittee on Social Security regarding high-risk issues surrounding SSNs, and I urged the Subcommittee to limit use and disclosure of the SSN in order to reduce error, misuse, and exploitation.[2] In a hearing before the Subcommittee on Immigration of the House Judiciary Committee in 2005, I also described some of the problems that would likely result from a poorly designed employment eligibility system.[3]

Recently, EPIC prepared a detailed report on the legislative proposals to establish the employment eligibility verification systems.[4] We reviewed the bills currently pending in Congress, the recent reports of the Government Accountability Office, and the report of the Inspector General of the Social Security Administration. Our report "National Employment Database Could Prevent Millions of Citizens from Obtaining Jobs" is attached to this statement.

In my testimony today, I will highlight some of our key findings as well as the related privacy and security concerns in the proposed development of the employment eligibility verification systems. Our central conclusion is that the verification systems proposed in H.R. 1645 and S.AMDT. 1150, contain significant weaknesses that should be remedied prior to enactment.[5] As currently planned, these systems greatly diminish

---

[1] EPIC maintains an archive of information about the SSN, including Congressional testimony, at http://www.epic.org/privacy/ssn/.

[2] Marc Rotenberg, Exec. Dir., EPIC, T*estimony and Statement for the Record at a Hearing on Social Security Number High Risk Issues Before the Subcomm. on Social Sec., H. Comm on Ways & Means,* 109th Cong. (Mar. 16, 2006) ["EPIC Testimony on SSN"], *available at* http://www.epic.org/privacy/ssn/mar_16test.pdf.

[3] Marc Rotenberg, Exec. Dir., EPIC, T*estimony 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,* 108th Cong. (May 12, 2005)*, available at* http://www.epic.org/privacy/ssn/51205.pdf.

[4] 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.

[5] Security Through Regularized Immigration and a Vibrant Economy Act, of 2007, H.R. 1645, 110th Cong. (2007) ["H.R. 1645"], *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) ["S.AMDT. 1150"], *available at* http://www.epic.org/privacy/surveillance/spotlight/0507/samdt1150.pdf.

employee privacy and make personal information vulnerable to theft and misuse. The proposed verification systems would also grant to the federal government unprecedented control over the livelihoods of American citizens and significantly expand the role of the Department of Homeland Security. The Secretary of Homeland Security could create a biometric identity system for all workers in the United States and make determinations about who is allowed to work without providing the basis for a determination.

Giving the Department of Homeland Security the authority to determine employment eligibility for virtually all Americans in the workforce, including those currently employed, raises unprecedented privacy and security concerns. As the Subcommittee must be aware, last month a critical component of the DHS lost the employment records of 100,000 federal employees. 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. While the privacy office of the TSA responded promptly once the problem was uncovered, the consequences of that data breach are truly staggering.[6]

This loss of 100,000 employment records by the Department of Homeland Security at a time of growing concern about identity theft raises serious questions about the ability of the Department to safeguard the sensitive data of American workers that would be collected under the House and Senate proposals.

I. The Proposed Employment Verification System Will Increase the Likelihood of Inaccurate Employment Determinations

The House and Senate proposals would significantly expand the Basic Pilot employment verification system instituted in 1997. Currently the program is essentially a voluntary program that is used by only one-fifth of one percent of employers.[7] The expansion of Basic Pilot under the House and Senate proposals would require all U.S. employers, approximately 7.4 million employers in the private sector and 90,000 in the public sector, to verify all new hires within 4 years.[8] This will create serious problems for the 143.6 million employees who would be exposed to preexisting data accuracy problems with the Basic Pilot system.

As currently drafted, the House and Senate proposals would cross-reference large volumes of employee information against government databases.[9] If even a small fraction of employee records contained errors, millions of individuals would be prevented from working if the flaws were not corrected. The number of incorrect nonconfirmations may

[6] Transp. Sec. Admin., TSA Public Statement on Employee Data Security (May 2007), *available at* http://www.tsa.gov/datasecurity/statement_05-07-2007.shtm.
[7] U.S. Citizenship & Immigration Serv., Dep't of Homeland Sec., *I Am an Employer... How Do I Use the Employment Eligibility Verification/Basic Pilot Program?* 1 (Jan. 2007), *available at* http://www.uscis.gov/files/nativedocuments/EEV_FS.pdf.
[8] S.AMDT. 1150 §302(a) (amending §274A(d)); H.R. 1645 §301(a) (amending §274A(c)).
[9] H.R. 1645 §301(b)(2), §306; S.AMDT. 1150 §302(a) (amending §274A(c)(9)(F)), §304(a)(1), §308.

be significant. A 2002 independent study of Basic Pilot, undertaken by the Immigration and Naturalization Service (INS), determined that 42% of final nonconfirmations were erroneous and the affected individual was eligible for work.[10]

Correcting such inaccuracies would place considerable burdens upon employees. They would have to navigate the appeals process for as long as two and a half months in order to prove their eligibility to work.[11] Some employees will also face hardship from their employers while trying to correct database errors. The INS report found that almost half of employees awaiting appeal had their pay cut, job training delayed, or were prohibited from working altogether.[12]

Recent reports have also determined that employers are using the Basic Pilot to prescreen applicants, in some instances denying them job opportunities because of faulty data maintained by the federal government.[13] Even though the practice of pre-screening is prohibited, it would seem obvious that employers will try to prescreen so as to avoid the additional burden that might result from a "further action" or "tentative nonconfirmation" notification. And the employee may never know the basis for the determination.

Although the House and Senate proposals provide for accuracy and security reviews, these audits take place months after establishment of the program.[14] Any solution adopted after the fact will likely arrive in the midst of an onslaught of verification requests. To minimize the problems that will arise from database inaccuracies, such errors should be corrected prior to enactment of the bills. A comprehensive accuracy and security audit of agency databases to fix existing problems would prevent setbacks if an employee verification system were established in the future.

II. Data Aggregation

Both the House and Senate bills offer government agencies unprecedented power over the means by which an individual may prove identity to gain employment. Both bills greatly expand the federal government's data collection and data sharing roles. Aggregation of large amounts of data increases the possibility that the information could be used for unintended purposes, such as long-term tracking of individuals and identity theft.

An all-inclusive database provides an appealing mark for thieves trying to create false identities for criminal activities. Large centralized databases of sensitive

---

[10] Inst. for Survey Research, Temple Univ., and Westat, *INS Basic Pilot Evaluation Summary Report* 8 (Jan. 29, 2002) ["Summary of Independent Analysis of Basic Pilot"], *available at* http://www.uscis.gov/files/nativedocuments/INSBASICpilot_summ_jan292002.pdf.

[11] H.R. 1645 §301(a) (amending §274A(c)(19)(A); S.AMDT. 1150 §302(a) (amending §274A(d)(5)(C)(iii)(II)).

[12] Summary of Independent Analysis of Basic Pilot at 31, *supra* note 10.

[13] *Id*. at 19-20; Office of Inspector Gen., Soc. Sec. Admin, *Congressional Response Report: Employer Feedback on the Social Security Administration's Verification Programs, A-03-06-26106* 6 (Dec. 18, 2006), *available at* http://www.ssa.gov/oig/ADOBEPDF/A-03-06-26106.pdf.

[14] S.AMDT. 1150 §302(a) (amending §274A(d)(2)(E); H.R. 1645 §301(a) (amending §274A(c)(2)(C)).

information also create the potential for devastating hardships for the millions of Americans who would be affected by identity theft from even a single security breach. In addition to the personal and financial troubles a data breach causes, some individuals would also experience threats to their safety. Privacy is better safeguarded by storing data in multiple, decentralized locations, and only when necessary.

Both the House and Senate proposals require DHS and the Social Security Administration to work together to operate the employment verification system as a fully integrated, cross-agency system.[15] However, the responsibility for data retention is given to DHS exclusively. The Senate bill requires that the Social Security Administration, Internal Revenue Service, and Department of State disclose personal data to DHS, including: driver's license and state identification numbers; tax information; employment data; passport and visa information; and birth and death records.[16] In addition, both bills give the Secretary of DHS the discretion to choose which documents can be required for employment eligibility.[17]

The House bill requires "administrative, technical, and physical safeguards" in order to minimize the unauthorized disclosure of personal information.[18] This includes the use of encryption, security updates, and periodic tests.[19] While these are all necessary and important components to safeguard data privacy, security includes all parts of a system's hardware, software, tapes, disks, and personnel. Although both bills state that database access will be limited to authorized users only, employees with no connection to employment verification could access the database as well. This likelihood is increased by the interlinking nature of the system proposed under both the House and Senate bills.

Both of the proposals require employers to submit employer and employee attestations, names, addresses, birth dates, and Social Security numbers for every employee. The House bill requires that employee information be stored by the employers for three years after the date of hire, or one year after termination for each employee, whereas the Senate bill requires employers to retain records for seven years after the date of hire, or two years after termination.[20] The employee records must be maintained by employers for a significant amount of time, thus increasing the likelihood of security breaches. The Senate proposal also contains a provision allowing employers to require new employees to submit their fingerprints to DHS. However the bill does not require employee notice or consent.[21] While the purpose of the action is to avoid identity theft, the involuntary collection of biometric data for employment verification is expansive and too invasive to adopt at this time. [22]

---

[15] H.R. 1645 §301(a) (amending §274A(c)(2)(B)); S.AMDT. 1150 §302(a) (amending §274A(d)(1)).
[16] S.AMDT. 1150 §302(a) (amending §274A(d)(9)(D)(i)).
[17] H.R. 1645 §301(a) (amending §274A(b)(1)(E); S.AMDT. 1150 §302(a) (amending §274A(c)(1)(E)).
[18] H.R. 1645 §301(a) (amending §274A(c)(4)(F)).
[19] *Id.*
[20] H.R. 1645 §301(a) (amending §274A(b)(3), (b)(4)); S.AMDT. 1150 §302(a) (amending §274A(c)(3), (c)(4)).
[21] S.AMDT. 1150 §307(a).
[22] S.AMDT. 1150 §307(b)(1).

Employers are to submit employment verification requests via the Internet, other electronic media sources, or over phone lines. These systems are vulnerable to interception, but the bills do not specify proper safety protocols for employers. Employers will also be responsible for collecting and storing large quantities of personally identifiable information for their employees seeking verification.[23]

Requiring employers to retain and protect their employees' personal information creates a significant burden. Employers will incur additional costs for storage, training, and necessary safety precautions. In addition, employers also have the added burden of being forced to verify all of their new hires with the federal government. This could lead to lost revenue as well as the difficulty inherent in implementation of the new procedures.

Neither the House nor Senate proposals require employers to retain sensitive employment data in a secure manner. While most employers would undoubtedly engage in safe storage practices, as identity theft becomes more lucrative, and thieves become more sophisticated, the chances of data breaches increase significantly. The Senate bill does contain a provision requiring the Comptroller General to conduct an annual report to ensure 97 percent employer compliance with specified privacy requirements listed in the bill.[24] Although 97 percent compliance is substantial, if even 3 percent of Americans are subjected to the devastation privacy breaches can cause, that would be too many. For this reason, additional federal safety guidelines should be included in both bills. The current proposals require that privacy trainings be conducted for employers; however, grants and other tools would also help employers successfully implement the necessary changes. These tools would be especially helpful for small business owners who may not have sophisticated technology or large budgets at their disposal.

As currently drafted, neither of the bills offers employees a private right of action against employers who negligently retain employee data. This is undesirable because employees must be protected, in the event that overburdened employers take short-cuts that could jeopardize employee data.

The risks of misuse and data breach are very real. Every day new stories surface in which hapless people are the victims of identity theft or security breaches. These events are caused by both unauthorized and authorized users of databases. For example, in 2006 an official of the Maryland Motor Vehicle Administration was one of three people charged with conspiring to sell unlawfully produced identification cards.[25] Similarly, in 2006, a police officer admitted accessing motor vehicle records to gather personal data on a romantic interest and co-workers.[26] Such abuses may increase under a national employment eligibility verification database.

III. REAL ID Requirements

[23] H.R. 1645 §301(a) (amending §274A(c)(12)(A)(ii); S.AMDT. 1150 §302(a) (amending §274A(c)(1).
[24] H.R. §301(a) (amending §274A(c)(18)(B)).
[25] *Fake ID Cards*, Wash. Post, Mar. 15, 2006, at B02.
[26] Michael Kiefer, *Officer Admits to Tampering; Databases Used to Check on Women*, Ariz. Republic, Apr. 6, 2006, at B3.

As the Subcommittee is likely aware, there is growing opposition to the implementation of the REAL ID Act. For example, Nevada recently passed a joint resolution urging Congress to repeal the scheme.[27] Fourteen other states have enacted legislation against it as well. In addition, there are bills in both the House and Senate seeking to repeal the Act.[28] During the public comment period on REAL ID draft rule, DHS received over 12,000 comments.[29]

Significantly, it took the Department of Homeland Security two years to issue the draft rule. The delay has raised further questions about the competence of the agency to successfully create a national identification system.

Therefore, it is surprising that the proposals to establish the Employment Eligibility Verification System assume a functioning, reliable REAL ID document and one proposal actual would make REAL ID-compliant identity the only document that could be used to determine employment eligibility. Identification documents listed under both bills include biometric, machine-readable Social Security cards or passports.[30] In addition, the Senate bill also includes REAL ID compliant driver's licenses.[31] Although REAL ID's drafters did not envision it as a national identification system, merely to set federal requirements for driver's licenses, both of the proposed verification systems would obligate individuals to adopt REAL ID as a prerequisite to employment. In fact, the Senate bill stipulates that non-REAL ID compliant cards would not be accepted after 2013.[32] Thus, both bills would help to create a national identification system, and they would move driver's licenses farther from their original use. There is even a scenario under which the Congress would pass legislation that would make employment in this country permissible only upon the presentation of a document that does not exist.

EPIC has previously explained at length that the REAL ID plan is fundamentally problematic.[33] The creation of machine-readable biometric Social Security and REAL ID cards will allow for greater data collection and tracking of individuals. Personal data would be recorded in digital format in many more encounters, leading to greater numbers of information databases and less secure personal information. The most reliable way to protect citizens, and reduce the growing problem of identity theft is by minimizing the collection of data, developing alternative technologies, and utilizing new organizational

---

[27] EPIC, *National ID Cards and REAL ID Act Page,* http://www.epic.org/privacy/id_cards/.
[28] *Id.*
[29] *Id.*
[30] H.R. 1645 §301(a) (amending §274A(b)(1)(B)(i)).
[31] S.AMDT. 1150 §302(a) (amending §274A(c)(1)(C)).
[32] S.AMDT. 1150 §302(a) (amending §274A(c)(1)(F)).
[33] EPIC Testimony on SSN, *supra* note 2; EPIC, *Spotlight on Surveillance, Federal REAL ID Proposal Threatens Privacy and Security* (Mar. 2007), http://www.epic.org/privacy/surveillance/spotlight/0307; EPIC and 24 Experts in Privacy and Technology, *Comments on Docket No. DHS 2006-0030: Notice of Proposed Rulemaking: Minimum Standards for Driver's Licenses and Identification Cards Acceptable by Federal Agencies for Official Purposes* (May 8, 2007) ["EPIC REAL ID Comments"], *available at* http://www.epic.org/privacy/id_cards/epic_realid_comments.pdf.

practices.[34] The REAL ID identification method does not meet these stipulations. Thus, it is an inappropriate requirement of employment verification systems.

But whether or not you accept our assessment of the REAL ID plan, the substantial opposition by the states, the high level of public opposition, as well as the far-reaching engineering problems suggest that employment verification based upon the availability of the REAL ID card is a perilous course.

IV. SSA Responsibilities

As they are currently drafted, the House and Senate proposals make extensive use of SSNs as a means of identity verification. But the number and card were never intended to used be such. The proposed additions to the Social Security card will increase their value to identity thieves and make privacy breaches more serious when they occur. The bills' requirements would also draw Social Security Administration resources away from their core mission.

When Congress passed the Privacy Act of 1974, it recognized the undesirability of using SSNs as universal identifiers. However, as they are currently drafted, the House and Senate proposals reinforce the use of SSNs as identification.[35] The verification system would require the Social Security Administration to cross-reference its information with DHS to help determine identity.[36] The House proposal recognizes that the SSN should not be an identifier: it requires that a disclaimer appear on the Social Security card stating that it is not to be used for identification purposes.[37] Yet that is precisely the practical effect under both bills.

The proposals would transform the Social Security card and include biometric and machine-readable characteristics, such as a digital photograph of the cardholder, for purposes of individual identification.[38] Including machine-readable features on the Social Security card would create a digital record each time the card is used. A widely used machine readable document increases the risk that the number will be compromised through identity theft. And the biometric data on the card would make breaches more serious for cardholders when they occur.

Adding these expensive features to the Social Security card would also divert resources from the original purpose of the Social Security Administration to administer retirement, disability and survivors' benefits. In a 2006 hearing before this Subcommittee, an Assistant Deputy Commissioner of the Social Security Administration testified that issuing Social Security cards with the new features outlined in the House proposal would cost more than $25 per card, with the cost of replacing cards for all

---

[34] EPIC, *Comments to the Federal Identity Theft Task Force, P065410* (Jan. 19, 2007), *available at* http://www.epic.org/privacy/idtheft/EPIC_FTC_ID_Theft_Comments.pdf.
[35] H.R. 1645 §301(a) (amending §274A(b)(1)(B)); S.AMDT. 1150 §302(a) (amending §274A(d)(5)(A)(i)).
[36] H.R. 1645 §301(b)(2) (amending §205(c)(2)).
[37] H.R. 1645 §301(b) (amending §205(c)(2)(G)(iii)(III)).
[38] H.R. 1645 §301(a) (amending §274A(b)(1)(B), (c)(12)(A)(iii)); S.AMDT. 1150 §305(a)(2) (amending §205(c)(2)(G)(4)).

holders approaching $9.5 billion.[39] Likewise, the safeguards the Social Security Administration and DHS must develop to ensure the system runs properly will be substantial. The bills require administrative, technical and physical layers to protect retained information. This includes encryption, an appeals process, periodic system testing and security updates.[40] These components add significantly to the workload of the agency, but are absolutely crucial from a privacy standpoint if the proposed verification system is to go forward.

The SSN is easily used for fraud not because the card lacks tamper-resistant features, but because the number is used as an identifier in so many encounters when it should not be. A more effective and secure verification system might institute a different unique number for the limited purpose of employment eligibility. This would limit the frequency of SSN disclosure and minimize the severity of any privacy breaches associated with the number. This would help curb identity theft and avoid placing increased costs and workload on the Social Security Administration.

V. Recommendations

Mr. Chairman, Members of the Subcommittee, I predict that if these proposals are adopted as currently drafted, there will be unprecedented problems in American labor markets. Employment verification relies upon the accuracy of the underlying data, the ease with which determinations can be made, the establishment of essential safeguards to ensure that the data collected is not subject to misuse, and procedural remedies to guarantee that when problems arise they can be quickly and fairly resolved. There is virtually no indication that any of these issues have been considered.

First, the existing inaccuracies within agency databases ought to be corrected before establishing the verification systems on a nationwide basis. Otherwise there is a strong likelihood that millions of eligible workers face a laborious identity correction process. This would lead to lost productivity and unnecessary expense.

Second, as little sensitive data should be collected as possible, and then only when necessary. Keeping huge quantities of personal information in a single government database enhances the appeal of that database to those who will attempt to misuse it. And if that database is compromised in the same way that TSA's employment records were, the fact that it contains such voluminous and detailed information makes the breach that much more serious. Instead, limiting the scope of information collected and retained to decentralized databases would reduce the vulnerability. The same goes for employers. Requiring employers to retain such detailed information for years after hire without strong safeguards not only burdens the employers, but also vastly increases the susceptibility of employee information to loss or misuse. Safeguards and privacy

[39] Frederick G. Streckewald, Assistant Deputy Comm'r, Disability & Income Sec. Programs, Soc. Sec. Admin., *Statement at a Hearing on Social Security Number High-Risk Issues Before the Subcom. on Soc. Sec. of the H, Comm. on Ways & Means*, 109th Cong. (Mar. 16, 2006), *available at* http://www.ssa.gov/legislation/testimony_031606a.html.

[40] H.R. 1645 §301(a) (amending §274A(c)(4)(F)), §306(a) (amending §205(c)(19)(B)).

implications should be established prior to implementation of the systems.

Third, the House and Senate proposals rely heavily on technology that has yet to be established. At this time, no states have adopted the REAL ID program, and its future is actively contested at both the national and state level.[41] It may therefore be imprudent to enact a wide-scale employment verification system based on a program whose future is in doubt. The verification system would be more effective, and future complications more easily anticipated, if the technology underpinning the documents was worked out beforehand.

Fourth, there must be better accountability for the extraordinary powers granted to the Secretary of Homeland Security. The Secretary should not be given discretionary authority to require the establishment of biometric identification for private employment in the United States or to require the routine collection of fingerprints in the private sector. One the Department's own identification systems, which included contactless RFID technology, was proved deeply flawed and subsequently revised.[42] All determinations of the Secretary regarding employment eligibility should be subject to the full privacy safeguards set out in the Privacy Act of 1974, including the right to inspect and correct data upon which an agency makes a decision, as well as additional safeguards proposed in the various measures.

---

[41] EPIC, *National ID Cards and REAL ID Act Page*, *supra* note 27.

[42] In 2005, DHS began testing RFID-enabled I-94 forms in its United States Visitor and Immigrant Status Indicator Technology ("US-VISIT") program to track the entry and exit of visitors. The RFID-enabled forms stored a unique identification number, which is linked to data files containing foreign visitors' personal data. EPIC warned that this flawed proposal would endanger personal privacy and security, citing the plan's lack of basic privacy and security safeguards. The Department of Homeland Security's Inspector General echoed EPIC's warnings in a July 2006 report. The Inspector General found "security vulnerabilities that could be exploited to gain unauthorized or undetected access to sensitive data" associated with people who carried the RFID-enabled I-94 forms. A report released by the Government Accountability Office in late January identified numerous performance and reliability issues in the 15-month test. The many problems with the RFID-enabled identification system led Homeland Security Secretary Michael Chertoff to admit in Congressional testimony on February 9th that the pilot program had failed, stating "yes, we're abandoning it. That's not going to be a solution" for border security. Dep't of Homeland Sec., *Notice With Request For Comments: United States Visitor and Immigrant Status Indicator Technology Notice on Automatic Identification of Certain Nonimmigrants Exiting the United States at Select Land Border Ports-of-Entry*, 70 Fed. Reg. 44,934 (Aug. 5, 2005), *available at* http://frwebgate1.access.gpo.gov/cgi-∂bin/waisgate.cgi?WAISdocID=021420363270+2+0+0&WAISaction=retrieve; EPIC, *Comments on Docket No. DHS-2005-0011: Notice With Request For Comments: United States Visitor and Immigrant Status Indicator Technology Notice on Automatic Identification of Certain Nonimmigrants Exiting the United States at Select Land Border Ports-of-Entry* (Dec. 8, 2005), *available at* http://www.epic.org/privacy/us-visit/100305_rfid.pdf; Dep't of Homeland Sec. Inspector Gen., *Additional Guidance and Security Controls Are Needed Over Systems Using RFID at DHS (Redacted)* 7 (July 2006), *available at* http://www.dhs.gov/xoig/assets/mgmtrpts/OIGr_06-53_Jul06.pdf; Richard M. Stana, Dir., Homeland Sec. & Justice Issues, Gov't Accountability Office, *Testimony Before the Subcom. on Terrorism, Tech., & Homeland Sec., S. Comm. on the Judiciary*, 110th Cong. (Jan. 31, 2007), *available at* http://www.gao.gov/new.items/d07378t.pdf; and Michael Chertoff, Sec'y, Dep't of Homeland Sec., *Testimony at a Hearing on the Fiscal Year 2008 Dep't of Homeland Sec. Budget Before the H. Comm. on Homeland Sec.*, 110th Cong. (Feb. 9, 2007), *available at* http://www.epic.org/privacy/us-visit/chertoff_020907.pdf.

Fifth, further enhancements to the Social Security card that would reduce the risk of tampering or counterfeiting are sensible, but the provisions to incorporate biometric data, to make the card machine readable, and to propose that it be used more widely to determine employment eligibility should be revised. The machine-readable capability would also create a trail of digital records of the card information whenever it is used. This would create more opportunity for identity thieves to steal the information and the problem would be more severe when they have done so. Instead, perhaps a number other than the SSN, used solely for the purpose of employment verification, may suffice. This would have the added benefit of avoiding additional cost to the Social Security Administration and allowing it to focus on its original mission

Conclusion

Mr. Chairman, members of the Subcommittee, It is tempting to believe that technology and new systems of identification can help solve long-running policy problems, such as determining eligibility to work in the United States. But the reality may be that new systems of identification will create new privacy risks for employees and new burdens for employers. We have already seen how the expanding use of the Social Security Number contributed to the dramatic increase in identity theft in the United States. Given the inaccuracies that currently exist in Basic Pilot, the difficulty that the Department of Homeland Security has had managing computer security and identification systems within its own agency, and the justifiable concern of those currently employed that they will now be required to undergo new identification requirements, I would strongly urge you to proceed cautiously on this proposal. Even a small error rate will impact the livelihood of millions of Americans.

Thank you for your attention. I would be pleased to answer your questions.