Association for
Computing Machinery

Advancing Computing as a Science & Profession

Testimony before the House Subcommittee on Social Security, Committee on Ways and Means Hearing on

"Employment Eligibility Verification Systems and the Potential Impacts on the Social Security Administration's (SSA's) Ability to Serve Retirees, People with Disabilities, and Workers"

6 May 2008

Statement of
Eugene H. Spafford

Professor and Executive Director
Purdue University Center For Education and Research in Information Assurance and Security (CERIAS)

Chair of The U.S. Public Policy Committee
of The Association For Computing Machinery (USACM)

Introduction

Thank you Chairman McNulty and Ranking Member Johnson for the opportunity to testify at this hearing.

By way of self-introduction, I am a professor at Purdue University. I also have courtesy appointments in the departments of Electrical and Computer Engineering, Philosophy, and Communication. I am also the Executive Director of the Center for Education and Research in Information Assurance and Security. CERIAS is a campus-wide multidisciplinary institute, with a mission to explore important issues related to protecting computing and information resources. We conduct advanced research in several major thrust areas, we educate students at every level, and we have an active community outreach program. CERIAS is the largest such center in the United States, and we were recently ranked as the #1 such program in the country. CERIAS also has a close working relationship with dozens of other universities, major commercial firms and government laboratories.

In addition to my role as an academic faculty member, I also serve on several boards of technical advisors, and I have served as an advisor to Federal law enforcement and defense agencies, including the FBI, the Air Force and the NSA. I was also a member of the most recent incarnation of the President's Information Technology Advisory Committee (PITAC) from 2003 to 2005. I have been working in information security for 25 years.

I am also the chair of USACM, the U.S. public policy committee of the ACM. With over 88,000 members, ACM is the world's largest educational and scientific computing society, uniting educators, researchers and professionals to inspire dialogue, share resources and address the field's challenges. USACM acts as the focal point for ACM's interaction with the U.S. Congress and government organizations. It seeks to educate and assist policy-makers on legislative and regulatory matters of concern to the computing community.

USACM is a standing committee of the ACM. It tracks US public policy initiatives that may impact the membership of ACM and the public at large, and provides expert input to policy-makers. This input is in the form of non-partisan scientific data, educational materials, and technical analyses that enable policy-makers to reach better decisions. Members of USACM come from a wide-variety of backgrounds including industry, academia, government, and end users.

My testimony is on behalf of USACM and not Purdue University. This is a follow-on to the testimony by Peter G. Neumann, Ph.D., on the same subject, before this committee on June 7, 2007.

Our Concerns

There are three major areas of concern we have as regards employment eligibility verification systems (EEVS): the accuracy and timeliness of system results, the security and privacy protections afforded to information kept in the system, and the technical feasibility of various ap-

proaches to creating such a system. Many of these concerns are also applicable to related programs such as US-VISIT and REAL-ID, and to peripheral systems that may depend on EEVS or result from interconnections among those other systems; our concerns are thus applicable to many other systems involving decisions made using large databases and distributed IT systems.

To begin with, I should stress that USACM takes no position on the actual question of whether an employment eligibility system should be mandated, or on any other issue directly related to employment or eligibility. Our concerns are directly addressed to **IF** such a system is developed that important technological questions are properly addressed.

Related to this, we wish to note that any widespread shift to mandating an EEVS as the sole means of determining employment eligibility has significant social impact as well as technological impact. Historically, someone in this country willing to put in a honest day's work would be employed (or not) on the decision of a person. Requiring that decision to be overruled by technology is a not-insignificant change that would remove or penalize human judgement in exigent or compassionate circumstances, especially in cases of error.

For reference, here is a short summary of the major concerns as addressed in Dr. Neumann's testimony last year.

- The data used to drive such a system — and particularly social security number (SSN) records — are known to have a non-negligible set of errors. In some analyses this error rate approaches 10%. Thus, any system using the SSN Numident data should address the issue of false positive results that might prevent legitimate candidates from working. It should also address *convenient* and *accessible* methods for individuals to correct records.
- IT systems with large databases of personal information are significant targets for abuse, theft, and corruption. A distributed, widely available database such as envisioned for EEVS would be an especially valuable target, and poses especially difficult problems for protection of security and privacy. In particular, authorized users "phishing" (using electronic means to fraudulently acquire sensitive information) for valid ID information and cyberstalking would be problems without special protections.
- The communications and end-systems used with the EEVS also need to be appropriately protected. This is especially a concern if small employers are required to access the system from a variety of end-points. For instance, requiring small business owners to obtain, maintain and secure appropriate computer access methods may be unduly burdensome.
- Availability of the system, especially under stressful conditions with loss of personal records such as after a Hurricane Katrina, will be necessary and non-trivial. The victims of such a disaster will be without access to documentation of their status but it will be in the best interest of all if they can find gainful employment without additional stress.
- There should be strong requirements for audit of access, breach notification, independent audit and review, and penalties for unauthorized use or abuse of the system or its data.
- Scalability is a concern, because all trials to date have been of systems of considerably smaller capacity. Our experience has shown that scaling large systems, even with working prototypes, introduces significant challenges that are often not foreseen. These stress budgets and designs, and may result in compromise of important protections, or even failure of the whole project.

The U.S. government has a particularly unfortunate record in this regard, with recent examples from the IRS, FAA, and US Army all coming to mind.
- We have concerns regarding authenticated identification of individuals seeking employment, and the relationship to authorized IDs. For a variety of reasons out of the scope of this testimony, USACM is opposed to the current REAL-ID and ACM is on record as against any national ID card, in general. However, separate from that issue remains the question of how people can prove, to a reasonable level of proof, who they are in regard to an EEVS.
- Accessibility to the system by small businesses, single employers, remote rural employers, and individuals with disabilities needs to be supported and secured. These users pose extra concerns and we are unaware of any existing system that has demonstrated support for all these concerns for any significant population.
- Similarly, there needs to be appropriate and timely access to the system of appeals and redress for individuals who are illiterate, disabled, without transportation, or in rural areas.
- "Feature creep" and "piggybacking" of the system by other agencies should be specifically prohibited, with strong safeguards in place.

We continue to have these concerns about any system that may be deployed for employment verification. Any legislation to mandate such a system should include safeguards sufficient to ensure that both employers and employees are adequately protected from technical failures and abuses of the system.

We would be pleased to discuss any of these issues at greater length at the committee's request.

Proposed Legislation

We are aware of two pending pieces of legislation that address EEVS. We have performed some analysis of these proposals.

HR 5515, New Employee Verification Act (NEVA) of 2008

This proposal contains many features that address concerns and limitations we have brought forward. However, we have the following specific concerns:

- Allowing only 10 days for an employee to contest and correct an initial disapproval is almost certainly too short a time. Not only will it be a burden for some employees to assemble the necessary paperwork and contact appropriate offices, but they may be working full time with no opportunity to take time off during business hours to conduct the appeal, and they may not have ready access to their records or to a means of communicating the appeal. As examples, consider a migrant farm worker, or someone working on board a ship.
- Additionally, a 20-day limit to make a final determination is perhaps too short. Given the observed error rate of the current system and the SSN database on which it is based: there will almost certainly be a significant delay in appeals at the Social Security Administration. Each appeal will need to be investigated by an employee and a correction entered into the system.

Without a significant increase in personnel, this process will undoubtedly be slow. (We remind the committee of the backlog in passport processing in the recent past as a cautionary illustration.)

- The SEEVS system appears to allow an unlimited number of private firms to have access to the identity information of citizens. This poses very serious privacy and security risks. Although the proposed legislation provides for penalties for error and disclosure, there is no provision made for the increase in personnel necessary to review audits, receive complaints, investigate problems, and prosecute offenders. Without ensuring that there are resources to enforce the rules there is little protection actually provided. Furthermore, there is no guidance given as to the minimum levels of security and audit required of each SEEVS operator.
- The proposed legislation implies that biometric technologies are adequate to provide security and accuracy in the system. However, biometric technology is not yet mature enough for such a large-scale application. Furthermore, there are privacy and accuracy concerns with most biometric systems that have yet to be addressed. We recommend that biometrics not be mandated in the legislation.

To the credit of NEVA there are specific restrictions imposed on the use of information obtained from EEVS, allowability of queries against the database, and the provision of false information. Furthermore, there are specific criminal and civil penalties described for violations. Also, the proposed legislation requires regular audit, report, and oversight activities. These are all positive.

The creation of an advisory panel is also commendable. The inclusion of language prohibiting other uses of the EEVS system is also in keeping with our concerns.

H.R. 4088, Secure America Through Verification and Enforcement (SAVE) Act of 2007 (Title II)

The SAVE Act also describes a number of enhancements and expansion of the current E-verify system to compose a mandatory EEVS system. Some of our specific concerns with SAVE include:

- The Act allows employees only 10 days to correct an error in the EEVS after notification of a mismatch. Not only is this far too short a time (as described above for NEVA), but the notification does not occur in a manner where the employee is expecting notice. Conceivably, the notice from the Social Security Administration to the employer could occur while the employee is on vacation or sick leave and unable to either obtain the notice or respond. Nonetheless, the employer would be required to terminate employment in 10 days without a correction.
- The requirements for documentation of multiple uses of a social security number to establish validity will be particularly burdensome on individuals who regularly receive income from many employers. This includes many performers, professional athletes, consultants, migrant workers, and others who normally report income in different locales apparently concurrently.
- The Act requires the establishment of yet another linked database (for birth and death records) with personal information that might be abused, with no statutory language governing security or oversight.

In Common

Both bills allow the use of a telephone as an end-user interface, and we endorse this approach as one that will enable small business owners access without the burden of obtaining or securing Internet access. However, we caution that appropriate audit of telephone users may be more difficult, especially if calls are allowed from any phone, and this will need to be addressed in any rulemaking.

NEVA and SAVE both require creation of new databases and interconnection with existing Federal databases. We are concerned that these additions may not be appropriately designed to provide full protection against disclosure and corruption of the involved data, as well as full audit for oversight and law enforcement purposes.

It would seem appropriate to have some waiver authority instituted such that in the event of sustained system failure or natural disaster the time limits could be extended or postponed by a competent authority.

Neither bill adequately addresses how someone without access to identity documents — particularly those without a photo or fingerprint — might be able to be authorized. Individuals who have lost their possessions to theft, fire, or flood, and those who are homeless or otherwise separated from their possessions would thus be unable to obtain gainful employment. There are many poor and indigent citizens who do not have photo IDs. This problem would be further complicated if they were unable to remember their SSN or birthdate, or if their records were incorrect in the EEVS.

In summary, neither the SAVE nor NEVA bills address all of our base concerns with issues of security, privacy, misuse, scale, breach notification, and other important issues. Of the two bills, NEVA addresses many more of our expressed concerns than does the SAVE Act, but also contains some provisions that we question as to their feasibility.

Closing Comments

Building a robust, long-lived, accurate system to perform employment eligibility verification may be possible. However, there are a number of important technical concerns (in addition to social, political, legal and economic issues). As technologists we are acutely aware of the limitations and failure modes of current information technology. Coupled with results from other studies, experience with other Federal systems, and details of SSN record accuracy, we must emphasize that any EEVS system deployed nationally is likely to have many failures and exceptions. What makes this especially serious is that some of those failures may result in unemployment for unfortunate and innocent victims; it is certainly conceivable that many of those victims will be the disabled, the partially literate, immigrants, the homeless, the mentally ill, and those who have suffered loses from disasters such as house fires and identity theft. Any system design

must take the extreme failure modes into account and provide appropriate safeguards to avoid injury to the blameless seeking gainful employment to better themselves.

It is also clear that any large system such as an EEVS will be a tempting target for any number of possible criminal enterprises and misuses. Not only must such a system be built to be resistant to any attempts at abuse, it must provide appropriate auditing, alarms, and records so that deficiencies are identified, and attempts at misuse are caught and punished.

We wish to reiterate the concerns presented in Dr. Neumann's written testimony before this subcommittee last summer. Additionally, to provide the committee with a framework for examining any other legislation on this topic, the USACM's principles for privacy are enclosed as an appendix; items 14-22 are particularly pertinent.

The USACM as a group, and I as an individual, thank you for the opportunity to provide testimony on this important issue. We stand ready to respond to any questions or additional requests.

Association for
Computing Machinery

Advancing Computing as a Science & Profession

USACM

The Public Policy Committee of ACM

USACM Policy Recommendations on Privacy

June 2006

BACKGROUND

Current computing technologies enable the collection, exchange, analysis, and use of personal information on a scale unprecedented in the history of civilization. These technologies, which are widely used by many types of organizations, allow for massive storage, aggregation, analysis, and dissemination of data. Advanced capabilities for surveillance and data matching/mining are being applied to everything from product marketing to national security.

Despite the intended benefits of using these technologies, there are also significant concerns about their potential for negative impact on personal privacy. Well-publicized instances of personal data exposures and misuse have demonstrated some of the challenges in the adequate protection of privacy. Personal data — including copies of video, audio, and other surveillance — needs to be collected, stored, and managed appropriately throughout every stage of its use by all involved parties. Protecting privacy, however, requires more than simply ensuring effective information security.

The U.S. Public Policy Committee of the Association for Computing Machinery (USACM) advocates a proactive approach to privacy policy by both government and private sector organizations. We urge public and private policy makers to embrace the following recommendations when developing systems that make use of personal information. These recommendations should also be central to any development of any legislation, regulations, international agreements, and internal policies that govern how personal information is stored and managed. Striking a balance between individual privacy rights and valid government and commercial needs is a complex task for technologists and pol-

icy makers, but one of vital importance. For this reason, USACM has developed the following recommendations on this important issue.

RECOMMENDATIONS

MINIMIZATION

1. Collect and use only the personal information that is strictly required for the purposes stated in the privacy policy.
2. Store information for only as long as it is needed for the stated purposes.
3. If the information is collected for statistical purposes, delete the personal information after the statistics have been calculated and verified.
4. Implement systematic mechanisms to evaluate, reduce, and destroy unneeded and stale personal information on a regular basis, rather than retaining it indefinitely.
5. Before deployment of new activities and technologies that might impact personal privacy, carefully evaluate them for their necessity, effectiveness, and proportionality: the least privacy-invasive alternatives should always be sought.

CONSENT

6. Unless legally exempt, require each individual's explicit, informed consent to collect or share his or her personal information (*opt-in*); or clearly provide a readily-accessible mechanism for individuals to cause prompt cessation of the sharing of their personal information, including when appropriate, the deletion of that information (*opt-out*). (NB: The advantages and disadvantages of these two approaches will depend on the particular application and relevant regulations.)
7. Whether opt-in or opt-out, require informed consent by the individual before using personal information for any purposes not stated in the privacy policy that was in force at the time of collection of that information.

OPENNESS

8. Whenever any personal information is collected, explicitly state the precise purpose for the collection and all the ways that the information might be used, including any plans to share it with other parties.
9. Be explicit about the default usage of information: whether it will only be used by explicit request (opt-in), or if it will be used until a request is made to discontinue that use (opt-out).
10. Explicitly state how long this information will be stored and used, consistent with the "Minimization" principle.
11. Make these privacy policy statements clear, concise, and conspicuous to those responsible for deciding whether and how to provide the data.
12. Avoid arbitrary, frequent, or undisclosed modification of these policy statements.
13. Communicate these policies to individuals whose data is being collected, unless legally exempted from doing so.

ACCESS

14. Establish and support an individual's right to inspect and make corrections to her or his stored personal information, unless legally exempted from doing so.
15. Provide mechanisms to allow individuals to determine with which parties their information has been shared, and for what purposes, unless legally exempted from doing so.
16. Provide clear, accessible details about how to contact someone appropriate to obtain additional information or to resolve problems relating to stored personal information.

ACCURACY

17. Ensure that personal information is sufficiently accurate and up-to-date for the intended purposes.
18. Ensure that all corrections are propagated in a timely manner to all parties that have received or supplied the inaccurate data.

SECURITY

19. Use appropriate physical, administrative, and technical measures to maintain all personal information securely and protect it against unauthorized and inappropriate access or modification.
20. Apply security measures to all potential storage and transmission of the data, including all electronic (portable storage, laptops, backup media), and physical (printouts, microfiche) copies.

ACCOUNTABILITY

21. Promote accountability for how personal information is collected, maintained, and shared.
22. Enforce adherence to privacy policies through such methods as audit logs, internal reviews, independent audits, and sanctions for policy violations.
23. Maintain *provenance* — information regarding the sources and history of personal data — for at least as long as the data itself is stored.
24. Ensure that the parties most able to mitigate potential privacy risks and privacy violation incidents are trained, authorized, equipped, and motivated to do so.

USACM does not accept the view that individual privacy must typically be sacrificed to achieve effective implementation of systems, nor do we accept that cost reduction is always a sufficient reason to reduce privacy protections. Computing options are available today for meeting many private sector and government needs while fully embracing the recommendations described above. These include the use of de-identified data, aggregated data, limited datasets, and narrowly defined and fully audited queries and searches. New technologies are being investigated and developed that can further protect privacy. USACM can assist policy-makers in identifying experts and applicable technologies.

For more information about USACM, please contact the ACM Office of Public Policy at (202) 659-9711 or see <http://www.acm.org/usacm/>.