Testimony before the House Committee on Veterans' Affairs
Hearing on
"Oversight Hearing on the Academic and Legal Implications of VA's Data Loss"

22 June 2006

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)

Member of the Board of Directors
of the Computing Research Association (CRA)

Introduction

Thank you Chairman Buyer and Ranking Member Evans for the opportunity to testify at this hearing.

By way of self-introduction, I am a professor at Purdue University with a joint appointment in the department of Computer Sciences and the school of Electrical and Computer Engineering. I also have courtesy appointments in the departments of 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 have a set of affiliate university programs working with us in a number of states, including Iowa, North Carolina, the District of Columbia, Ohio, Virginia, Idaho, and New York. CERIAS also has a close working relationship with a dozen 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 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 began this document by listing my affiliations with ACM and CRA. This testimony is not an official statement by either organization, but is consistent with their overall goals and aims. ACM is a nonprofit educational and scientific computing society of about 80,000 computer scientists, educators, and other computer professionals committed to the open interchange of information concerning computing and related disciplines. USACM, of which I serve as the chair, acts as the focal point for ACM's interaction with the U.S. Congress and government organizations. USACM seeks to educate and assist policy-makers on legislative and regulatory matters of concern to the computing community. The Computing Research Association is an association of more than 180 North American academic departments of computer science and computer engineering, industry and academic laboratories, and affiliated professional societies. The CRA is particularly interested in issues that affect the conduct of computing research in the USA.

The Nature of the Problem

We are here as a result of a significant breach of security and privacy at the Veterans' Administration reported in May of this year. The theft of a computer system may have revealed personal details of several million veterans and active-duty military personnel. This incident exposes those personnel to an increased risk of identity theft, credit fraud, and other criminal activity.

Identity theft, coupled with the general lack of accuracy and data provenance[1] tracking of large databases by government and industry, means that those individuals' good names and records may be besmirched by people who misuse the exposed personal information. This is a special risk for some of our active-duty personnel and veterans because they may find themselves denied security clearances through no fault of their own. Another possibility is that they will find their names added to the TSA's "No Fly" list because someone else has misused their identity.

This problem is not unique to the VA, however. A recent article in Computerworld[2] stated that since the start of 2005 there have been nearly 200 computer security breaches resulting in significant disclosures of personal information. Nearly 90 of those incidents have occurred this year, and the total number of records disclosed by all those incidents exceeds 88 *million*. What is more, those are only the *detected and disclosed* incidents; it may well be the case that several times that many incidents have occurred.

For decades, professionals in the field of information security have been warning about the dangers of weak security, careless handling of data, lax enforcement of policies, and insufficient funding for both law enforcement and research. Our warnings and cautions have largely been dismissed as unfounded or too expensive to address. Unfortunately, we are seeing the results of that lack of attention with incidents such as what happened at the VA. In addition we have seen new levels of sophisticated computer viruses and spyware, increasing cyber activity by organized crime, and significant failures of security across a wide variety of public sector entities and government agencies, including the Department of Defense.

I will not go into depth about the failures at the Veterans' Administration that led to this particular incident. Your committee has been conducting an investigation of the factors underlying those failures, and the testimony so far appears to be exposing those problems.

I will make special note of two information security failures present in this case, however, that I have seen time and time again in government, industry, academia and elsewhere. I often refer to these problems when I teach the basic information security classes at Purdue; I will now be able to associate these with the May VA incident as a specific example.

1. There is no centralized point of authority to ensure that rules, procedures and good practices are instituted and observed. There are good people at the VA who understand what needs to be done, and many of them try to do the right thing. However, there is no centralized position that has all three components necessary to effectively manage information security: resources, accountability, and authority. There should be a CIO or CISO (Chief Information Security Officer) who has adequate funding and trained personnel to carry out a comprehensive security plan. That office (and management above

---

[1] Data provenance is the labeling of data with information about where it came from, where it has been copied, and details about how it was derived. This can be used to determine if the data is accurate, or from whence errors might have been introduced.

2 June 20, 2006 article: "Flurry of New Data Breaches Exposed," by J. Vijayan and T. Weiss.

it) also must be held accountable for failures to satisfy necessary standards and successfully pass audits. Last of all, that same office must have authority to make changes, shut down systems (if necessary), and terminate employees for cause. Accountability without authority means the position is simply a focus for blame when failures occur; authority without resources means that only limited organizational problems can be fixed; and resources without accountability may simply lead to fraud, waste and abuse.

2. An employee or contractor makes an arbitrary decision to violate security policies so as to make his job easier. This is done without understanding why the policy is structured as it is, and without understanding the potential consequences of the violation — until it is too late, if even then. Unfortunately, we see this happening all the time, and it is usually the case that – even if detected – no sanctions are imposed so long as the work gets done and nothing untoward appears to happen. This builds a climate of contempt for the policies, and the mistaken belief that end-users are capable of making policy decisions involving enterprise security. If something untoward does happen, often the guilty parties are scolded, but nothing further occurs: an attitude of "failures are commonplace" overrides any thought of holding guilty parties fully accountable.

There are other information security problems at the VA and elsewhere in the government, which were not directly involved in the May disclosure incident. It is beyond the scope of this hearing and this testimony to document and describe all of them. It is also beyond the scope of this testimony to summarize the magnitude of cyber threats currently facing our information infrastructure, including the Veterans' Administration. There are many reports describing these threats, including reports from the PITAC, the GAO, the National Academies, the Department of Justice, and many commercial entities. From these reports the following general trends may be derived:

- The number of reported attacks of various kinds is increasing annually;
- Attacks are becoming more sophisticated and more efficient;
- Few perpetrators are ever caught and prosecuted;
- An unknown (but probably large) number of attacks, frauds and violations are not detected with current defenses;
- A large number of detected attacks are not reported to appropriate authorities;
- The problem is international in scope, both in origin of attacks and in location of victims;
- The majority of the attacks are enabled by faulty software, poor configuration, and operator error.

Undoubtedly the magnitude of the problems are greater than have been reported, and more has occurred than has been detected. Regrettably, I believe the situation is going to get worse because the problems have been ignored and neglected for too long to be quickly remedied.

As a long-time educator and researcher in this field, I can state that my peers and I can offer few immediate solutions. Although we have several good programs at colleges and universities across the United States, we are producing too small number of students to meet the demand. In part, this is an issue of enrollment, as nationally we do not get enough good students seeking de-

grees in the area. We also have only a small number of programs involved in training of practitioners, and even fewer that are involved in quality graduate education and research.

Exacerbating both of these problems is a lack of resources. Outside of a few underfunded programs through the NSF that award competitive grants to faculty, and a few Congressionally-directed allocations to some university projects around the country, there is almost no funding for basic research, capacity development, or infrastructure acquisition for programs in information security; as an example, CERIAS at Purdue is the nation's leading center in multidisciplinary information security research and education with over 80 faculty, and it has never received any government support (although some individual faculty have received funding from agencies such as NSF for their individual research). As is the case with many of our peer institutions, our ability to make progress in education and research is limited mostly by lack of resources.

Some Recommendations

In February 2005, the President's Information Technology Advisory Committee issued a report, based on hearings and considerable study by many experts. That report was entitled Cyber Security: A Crisis of Prioritization.[3] It described the nature of the problems with cyber security and some of the trends. It also analyzed the (inadequate) Federal response to those challenges. It outlined, in some detail, an agenda to begin to address some of our cyber security problems. The response to that report was that action was only taken on one of the four recommendations, and the PITAC was disbanded.

I encourage members of the committee to carefully read the PITAC Cyber Security Crisis report. I participated in the research and writing of that document, and it goes into considerable detail on the problems and issues behind our cyber security deficit, as well as making some concrete suggestions of how those issues might be addressed.

I also suggest that the committee might find my testimony to the House Armed Services Committee on October 27, 2005 to be of interest.[4] The topic was ""Cyber Security, Information Assurance and Information Superiority." In it, I discussed cyber threats to US systems, and I also outlined some suggestions for how those threats might be mitigated.

Last of all, I have included a set of recommendations from the ACM US Public Policy committee regarding privacy of personal data. There is no comprehensive privacy legislation in the US as there is in many other countries. This has led to an *ad hoc* approach to privacy regulations in government and in the commercial sector, which in turn has enabled many of the abuses and disclosures we have seen recently. It is difficult to create a culture of protection of personal data when privacy is treated as an afterthought, and when frequently it is seen as appropriate to circumvent privacy protections to reduce cost or effort. Thus, as you consider what changes at the

---

[3] Available online at <http://www.itrd.gov/pitac/reports/index.html>.

[4] Available online at <http://homes.cerias.purdue.edu/~spaf/usgov/newHASC.pdf>

VA might improve cyber protections for the data on our veterans, you might find these recommendations by the USACM to be of value.

Specific Q&A

The committee did not pose specific questions for me when I was invited to appear.

This concludes my written testimony. I will be pleased to provide additional information if requested.

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 policy 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/>.