

Declaration of David R. Jefferson

I, David R. Jefferson, hereby declare:

1. I am a professional computer scientist with a Ph.D. in computer science from Carnegie-Mellon University, awarded in 1980.
2. I was a professor of computer science for 14 years from 1980 to 1994, first at the University of Southern California and then at UCLA.
3. From 1994-2002 I worked in Silicon Valley in the research laboratories of Digital Equipment Corporation, Compaq Computer Corporation, and Hewlett-Packard.
4. I currently work on supercomputing applications at Lawrence Livermore National Laboratory, a nuclear weapons laboratory, where national security and cyber security are among our very highest priorities.
5. As a separate activity I have worked on technical issues related to elections and voting for over 16 years. Much of my work, but not all of it, has been in advisory capacities to the California Secretary of State over five successive administrations, three Democratic and two Republican.
6. In 1999-2000 I served as chair of the Technical Committee committee of Secretary of State Bill Jones' Task Force on Internet voting, which issued a sharply cautionary report recommending against institution of Internet voting because of serious and fundamental security problems.

7. In 2004 I served on Secretary of State Kevin Shelley's Ad-hoc Task Force on Touchscreen Voting. Our report eventually led to the requirement for voter-verified paper trails for all electronic voting systems in California.
8. From 2005 to 2007 I chaired the Technical Advisory Board for Secretary of State Kevin Shelley, and then its successor body, the Voting Systems Technology Assessment and Advisory Board, under Secretary of State Bruce McPherson. In that role I led a half dozen in-depth technical investigations of voting system issues for the Secretary of State.
9. From 2005-2006 I sat on the Secretary of State's Voting Systems and Procedures Panel, which held public hearings and made formal recommendations about voting system certification to the Secretary.
10. In 2007 I served as chair of the Post Election Audit Standards Working Group under the current Secretary of State, Debra Bowen.
11. In 2003 I was a member of the review panel for the Department of Defense's SERVE Internet voting system. I was part of a subset of that panel that wrote a paper recommending that the system be scrapped because of numerous security vulnerabilities. That recommendation was followed, and the program was killed in early 2004.
12. I have testified, advised, and published about election and voting technology, and especially security issues, on numerous other occasions in the last decade. In all cases I have taken aggressive positions in favor of tighter security around voting systems and election procedures.

13. I am a member of the Board of Directors of the California Voter Foundation (www.calvoter.org) and of VerifiedVoting.org (www.verifiedvoting.org), two non-profit, non-partisan organizations dedicated to security and transparent election technology (among other things).
14. I am familiar with the general architecture of Diebold voting systems, with GEMS and its data contents, and with the security issues regarding them.
15. As a preamble, it is my professional opinion that the GEMS election management system (and also similar products from competing vendors) are full of security vulnerabilities of all kinds. The security mechanisms that are there are generally incorrectly implemented, or seriously incomplete, or easily circumvented, and in general hopelessly inadequate to prevent manipulation of ballot records or vote totals by anyone with even a very short period of access to the the system. The opinion is based on two very thorough reviews of those systems published this year. The first was done by world class computer scientists led by computer science Prof. David Wagner of U.C. Berkeley and Prof. Matt Bishop of U.C. Davis and published a few months ago by California Secretary of State Debra Bowen in her “Top to Bottom Review” of California voting systems. (See http://www.sos.ca.gov/elections/elections_vsr.htm.) The other was a similar thorough review under the name EVEREST by an equally distinguished scientific panel under the auspices of Ohio Secretary of State Jennifer Brunner and led by Penn State computer science Prof. Patrick McDaniel. (See <http://www.sos.state.oh.us/sos/info/everest.aspx>.) Several other less comprehensive and less authoritative reports reached similar conclusions earlier.

16. The significance of this observation is that in essence the *only real security* for election data stored in GEMS comes from *physically limiting access* to the actual running copy of GEMS used in the election. The password protections, cryptographic mechanisms, and most other security features provided by GEMS are poorly designed, easily circumvented, and essentially useless in the prevention of attacks. Given these deficiencies, the only generally effective security measure for GEMS is preventing potential attackers from getting physical access to the one running copy that is used in managing an election. (Even that precaution is seriously undermined in Arizona because of the practice of allowing remote modem access to GEMS from precinct systems on election day, a practice prohibited in California. If Arizona is really interested in securing GEMS data, prohibiting that access must be one of the highest priority actions to take.)
17. For several reasons there would be no *new* or *additional* security risk posed by providing plaintiffs with all the copies of the databases they request now or in the future:
 - a. First, the structure of the GEMS databases, the number and names of the tables, the types and precise formats of the data they contain, the structure and format of election definition files and of audit logs, and even the code for a recent version of GEMS, have all become public one way or another. There are no secrets of that kind left.
 - b. As the court knows, the Alaska Division of Elections released a copy of the GEMS database to the Alaska Democratic Party in 2006 after concluding (correctly in my opinion) there was no security reason not to do so. Presumably the Democratic

Party in Arizona (and anyone else) can get a copy of that database and learn all about its structure from them.

- c. Even if the structural features of the GEMS databases were still secret, it would not take an attacker long to learn them. Databases make this information easy to retrieve with a single command. Database table names and field names and the like are not generally security relevant, and the security of databases, especially simple ones built on the same platform as consumer products like Microsoft Access, never rests on keeping such things secret.
 - d. As a general rule in cyber security, it is bad policy to attempt to rest the security of a system on keeping its structure, behavior, data formats, or even the code itself secret. This mistake is so well established that it is called the fallacy of “security by obscurity”. The only secrets that the security of a software system should rest upon are secret PINS, passwords, cryptographic keys and the like. The system should be designed so that even if all other aspects of the system are made public, the security goals of the system are still met. (Note that this has *not* been done properly with GEMS, even though it certainly should have been. But even though it has not, and GEMS is a security sieve, there is still no security value to be gained in withholding copies of GEMS databases from the public.)
18. Because the only real security for GEMS comes from preventing physical access to the actual running instance of GEMS used by Pima County to conduct the election, and because the structural and format descriptions of the data it contains are not security relevant anyway, no additional security at all would be achieved by

withholding copies of GEMS databases from the plaintiffs. Releasing copies of GEMS data is security neutral.

19. The specific security concerns advanced by Pima County to argue against release of GEMS data are misdirected and carry no weight.
 - a. The county argued that counterfeit ballots could be generated from GEMS. The court adequately disposed of this contention. Yes, they can be printed, but the attacker would still need access to the proper paper stock, and would still need to get the phony ballots inserted into the canvass process *before* the election was certified. To the extent that such an attack is likely at all, it is equally possible already, and withholding the databases from the public makes no difference at all.
 - b. The same argument could be made about counterfeit memory cards. To the extent that this is a danger (and it is a very real and serious concern to me) the danger already exists and is in no way ameliorated by withholding copies of GEMS databases from the public.
 - c. Regarding man-in-the-middle attacks on remote transmission of election results to GEMS, again, that is a very real danger. But withholding copies of GEMS from the public would have no effect whatsoever to slow or ameliorate that kind of attack. The only cure for that problem is prohibiting remote access, as the court already noted is under consideration.
 - d. Regarding the concern about the possibility that release of a database would allow construction of a counterfeit database purporting to hold genuine election results or logs, I would suggest that there is a simple and effective way to deal

with this issue. There is a well-known, standard cryptographic technique for verifying that the data in a file or database has not been changed at all, and that is to calculate from the database a kind of “fingerprint” (a number a few hundred bits long that is technically known as a cryptographic hash). The fingerprint can be published along with the database itself. The significance of the “fingerprint” is that if even a single bit of data is added to, or deleted from, or changed, in the file from which the fingerprint was computed, the modified file has a completely different fingerprint. Furthermore, it is essentially impossible to compute or generate a phony variant database that would have the same fingerprint as the original. If someone in the public created a modified version of the GEMS database or its logs, or of any part of the data that is released, and tried to claim that it was true the original, and that Pima County’s copy had been altered, that claim could be conclusively refuted by calculating its fingerprint and comparing it to the original. This is quite a straightforward process, and is very widely used. A variant of this method is being implemented at the National Institute of Standards and Technology to aid in determining whether the binary code about to be loaded into voting machines is identical to the original certified copies or has been altered. The principle is exactly the same whether applied to code or a database.

20. It is my opinion that nothing I have said above is affected by whether one, two, or all Pima County GEMS databases are released to the public. The argument that merely releasing only one or two copies instead of a larger number of them will prevent or even slow down some hypothetical future attack is totally mistaken.

21. I believe that the only way to restore or retain public trust in elections is to provide extraordinary transparency to all aspects of their conduct. Election procedures should be designed so that every step in the process can be observed or audited by the contending parties and by the general public. Release of fingerprinted copies of any and all GEMS databases to anyone who wants them is an appropriate application of this principle.

I declare under penalty of perjury that the foregoing is true and correct.

Executed this _____ day of _____, 2007

BY: _____