IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF NEW YORK

_____

UNITED STATES OF AMERICA,
Plaintiff

DECLARATION OF POKEY ANDERSON

v

Case No. 06-CV-0263 (GLS)

NEW YORK STATE BOARD OF ELECTIONS; PETER KOSINSKI and STANLEY L. ZALEN, Co-Executive Directors of the New York State Board of Elections, in their official capacities; and, STATE OF NEW YORK,
Defendants

_____

Pursuant to 28 U.S.C. sec 1746, **POKEY ANDERSON**, declares as follows:

1. Over the past four years I have interviewed dozens of computer experts, attorneys, journalists, election officials and citizens involved in election issues around the country. I have co-anchored a wide ranging news analysis show, The Monitor, airing Sundays on KPFT, Houston. **http://themonitor.wordpress.com.**

2. I was part of the radio broadcast team providing continuous live coverage of the National Election Reform Conference, Portland, Oregon (9-30-05 to 10-2-05). I have

been an invited guest to discuss vote counting issues on public television (KUHT) in Houston (9-28-04), and on Access TV. I have an invited guest at panels at Rice University (10-23-06) and local political groups. I have been an invited guest on radio stations besides KPFT, including WBAI in New York City (1-27-04 and 6-30-05).

3. My most recent research on electronic voting machines can be found at "Peering Through Chinks in the Armor of High-Tech Elections," which described the myriad vulnerabilities of electronic voting machines, **http://www.votersunite.org/info/PeeringThruChinks.pdf.** I explored the insecurity of voting on DREs and Optical Scanners, utilizing the research of leading computer scientists. More and more reports revealed that security on these machines was so weak, test hackers have needed only one to four minutes access to the equipment to completely take control of the software.

4. In an attack by Professor Ed Felten at Princeton[1], he showed that the code could easily be configured to “disappear” once its work was done, leaving no trace of tampering.

5. Professor Felten further explained about the security used on Diebold Accu Vote-TS electronic voting machines. I dubbed this the "Leave No Comedian Behind

[1] "**How to Hack an Election in One Minute**," by Daniel Turner, Technology Review, September 18, 2006, http://www.technologyreview.com/Infotech/17508/?a=f

Election Security Provisions;" wherein a hotel mini-key bar was the security Diebold had provided to safeguard the votes. Professor Felten explained:

> *The access panel door on a Diebold AccuVote-TS voting machine - the door that protects the memory card that stores the votes, and is the main barrier to the injection of a virus - can be opened with a standard key that is widely available on the Internet. ... the exact same key is used widely in office furniture, electronic equipment, jukeboxes, and hotel minibars."*[2]

6. In 2005, Finnish computer expert Harri Hursti hacked the Leon County, Florida optical scan system in front of Supervisor of Elections Ion Sancho. It took Hursti a few minutes to change the result of a test election, and he never entered the room that had the tabulator in it -- he had reprogrammed the memory card in his hotel room. He told me:

> *Fundamentally, the whole idea, and the discovery which I made from the publicly available documents, was that there is an executable program, which is living and stored in the removable media -- what we call the memory card. And that memory card is really the modern day ballot box itself. So, while there was no indication in the user manuals or documentation that such a program is stored there, it was there. And it really means that there's no such thing as an empty ballot box. Well, the whole thing there is that that program is responsible for all the reporting functions of the optical scan count unit. Once you change that program, you can do a lot of other stuff. ... What's very important to understand is that there was no protection against random errors or intentional tampering to change or -- and replace the program in the memory card. It was there, just wide open. You could rewrite it -- write it over with your own program. And of course when you have*

---

[2] "**'Hotel Minibar' Keys Open Diebold Voting Machines**," September 18, 2006, by Ed Felten, Freedom to Tinker.

your own program then there is a very far-reaching implication.[3]

7. A similar threat possibility was identified on ES&S DREs. Once again, the path of intrusion could be a removable vote storage device inserted into the larger machine. Once again, the successful attacker could completely control the machine and the results.

8. A tight Sarasota, Florida race for Congress, with 18,000 voters seeming not to have cast ballots in that race even though they voted for a lower profile hospital board contest, sparked unusual scrutiny of the electronic voting machines used. The tally suggests that the race was decided by a margin of under 400 votes, but the 18,000 undervotes remain a gnawing question with no convincing reason for them. For those using the DREs in Sarasota, the undervote rate was three to seven times higher than the rate in neighboring counties voting for the same contest.

9. The SAIT team[4] reporting to the State of Florida wrote about the ES&S system:

Our security analysis revealed several software defects that could allow an attacker to introduce a virus into the voting system that spreads through

---

[3] Monitor, June 19, 2005, KPFT Radio Houston

[4] Software Review and Security Analysis of the ES&S iVotronic: 8.0.1.2 Voting Machine Firmware," Alec Yasinsac, David Wagner, Matt Bishop, Ted Baker, Breno de Medeiros, Gary Tyson, Michael Shamos, Mike Burmester, SAIT (Security and Assurance in Information Technology Laboratory), For the Florida Department of State, February 23, 2007.

removable storage devices. [pp. 44]

10. The SAIT team found vulnerabilities that could allow an attacker to take control of a voting machine by corrupting data.

> *Unfortunately, the testing procedures that are standard practice in the elections community are unlikely to discover these vulnerabilities or the presence of a virus. ... If these vulnerabilities were exploited, it would be possible to hide their existence. A cleverly constructed virus can cover its tracks so that infected machines could not be detected by ordinary means and an appropriately programmed virus could self-destruct and erase all its tracks. ... [If] carefully constructed, it can allow an attacker to transfer program control to her own malicious code. Once this happens, the attacker controls the machine."* [pp. 37-38]

11. The two biggest elections vendors, Diebold and ES&S, were vulnerable to sneaky software being injected into the voting system from a little device that could fit into the palm of your hand.

12. I asked Bruce O'Dell[5] what he thought about the apparently missing 18,000 votes in Sarasota:

> *The technology to invisibly compromise voting systems is mature and the rewards*

---

[5] Bruce O'Dell has spent his career working with very large-scale computer systems with stringent security, audit and accountability requirements - systems for financial accounting, insurance claims processing, mortgage origination, bond trading, stock trading, loan servicing, and online financial account aggregation. At American Express he was lead software architect for a project to create a company-wide security component, and received their Chairman's Award for Quality, in 1998, for helping to develop methods for securely deploying new software to networks of thousands of computers.

are essentially limitless. It's professionally irresponsible to not presume vulnerable extreme-high-value systems are already actively being exploited.

13. A poll in our largest state indicates that those voters are not exactly convinced that our current election systems work. Of likely California voters in August 2007, less than half, only 44%, have a "great deal of confidence" that their votes are being accurately counted. More than half, 55%, have "some confidence" or "only a little confidence" or "no confidence" that their votes are being accurately counted[6].

14. Threat analysis is part of what computer security professionals do. Nationally-known Stanford professor David Dill has addressed whether we need to be concerned about elections being manipulated electronically:

> Think about it rationally. What are the assets being protected? If we're talking presidential elections or control of Congress, there aren't a lot of assets in this world in monetary terms that are worth more than that. You're talking about the whole US economy. ... There are people who may be interested in effecting election outcomes who may have massive resources. And [who] either are very sophisticated or can buy people who are very sophisticated to mess with the

[6] California Secretary of State Bowen Comments on Field Poll About Voter Confidence in Elections," by California Secretary of State Debra Bowen, August 31, 2007, http://www.votetrustusa.org/index.php?option=com_content&task=view&id=2573&Itemid=113

machines. We've got a hard problem [of defending voting machine security] when we're up against sophisticated people. [7]

15. In another of my articles*, Are Elections Very Important?*, http://www.opednews.com/articles/opedne_pokey_an_070917_are_elections_very_i.htm, I looked at risks and rewards of stealing elections, and reviewed some experts' observations. I concluded that while there has always been manipulation in elections, the difference between stealing in a hand-counted paper ballot election (counting at the precinct) and an electronic election is the difference between successfully robbing a convenience store and successfully robbing Fort Knox. The scale of what can be accomplished by a few corrupt people is completely different. Even a convenience store takes precautions, with video cameras, and stowing large bills away, so that the most that theoretically can be stolen is $35. Electronic elections in this country are like having TAKE SOME FREE GOLD Day at Fort Knox. It's like leaving our community treasury out on the sidewalk.

16. After reviewing the security level on a major computerized voting system now used across the nation, on expert guessed that it could maybe deter an eighth grader. William Arbaugh, after testing Diebold touchscreens for the State of Maryland said:

There's no security that's going to be 100 percent effective. But the level of effort was pretty low. A high school kid could do this. Right now, the bar is maybe 8th grade.[8]

---

[7] Prof. David Dill, speech at Rice University, February 25, 2004.

[8] *Md. computer testers cast a vote: Election boxes easy to mess with*, by Stephanie Desmon, January 30, 2004, Sun (Maryland), http://www.sunspot.net/news/local/bal-te.md.machine30jan30,0,4050694.story?coll=bal-local-headlines.

17. Former National Security Agency code breaker Michael Wertheimer also tested the Diebold touchscreens for the State of Maryland. He told Time Magazine:

If you believe, as I do, that voting is one of our critical infrastructures, then you have to defend it like you do your power grid, your water supply.[9]

18. An election should be observable from start to finish, with human eyes unmediated by "help" from software. And human eyes should be able to tell if it's honest. We need to get it right on election night. Send everybody home convinced of the final result. Computers can't do that. Paper ballots can.

19. Given all the vulnerabilities with electronic computerized voting systems I would respectfully urge this Court to reject any demand that New York purchase these highly insecure, theft-enabling machines and permit New Yorkers to vote in the most transparent, secure way so that they can know their votes were counted as cast.

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

/s/_____

POKEY ANDERSON

Executed on December 11, 2007

---

[9] *The Vexations Of Voting Machines,* by Viveca Novak, Time Magazine, April 26, 2004, http://www.time.com/time/magazine/printout/0,8816,1101040503-629410,00.html.