DATE: May 23, 2006

TO: Georgia State Election Board

As representatives of the undersigned groups, we are calling today on the Georgia State Election Board to immediately decertify the state's Diebold Election System (DES) and for the Elections Division to begin immediate preparations for the deployment of an alternative means of voting in time for the 2006 primaries and General Election.

A security vulnerability recently exposed in the architecture of the DES is being called a "major national security risk" by computer science and security experts. The effect of this vulnerability is that voting systems could be infected throughout an entire state, enabling an attacker to alter election results on a massive scale without detection. Once the vulnerability is exploited, the voting system could be under the control of the attacker, not only for the current election, but also for future elections.

"It's the most severe security flaw ever discovered in a voting system," said Michael I. Shamos, a professor of computer science at Carnegie Mellon University who is an examiner of electronic voting systems for Pennsylvania . . . ."[1]

The computer scientists who are knowledgeable of the technical details of this vulnerability state that the problem cannot be fixed or "cleaned up." It represents an open backdoor that is part of the design of the Diebold TS-R6 and TSX voting systems.

"It is like the nuclear bomb for e-voting systems," said Avi Rubin, computer science professor at Johns Hopkins University. "It's the deal breaker. It really makes the security flaws that we found (in prior years) look trivial."[2]

Because the electronic voting system in Georgia is paperless and therefore affords no independent means for auditing the vote count, Georgia's votes could be (and may already have been) hacked or otherwise altered without leaving any evidence.

It is clear that the current mechanisms for detecting security vulnerabilities, including state and national certification and testing, are not sufficient to protect the state from election fraud. The state's Kennesaw Center for Elections did not catch this security vulnerability; neither did the national Independent Testing Authorities (ITAs); nor the "Logic and Accuracy" testing; nor the "hashing;" nor the escrowed code; nor the software version control system; nor any other mechanisms on down the list that voters have been told would ensure that Georgia's voting system would be secure.

Some aspects of this vulnerability were already known to the state of Georgia and Diebold from Maryland's RABA report of January 20, 2004. How much about this exploit was detected at that time is being debated by computing security professionals, as sections of the report were redacted. However, it is clear that Diebold did not (could not) correct the flaws.

---

[1] "New Fears of Security Risks in Electronic Voting Systems," Monica Davey, *New York Times*, May 12, 2006.

[2] "Diebold voting systems critically flawed," Robert Lemos, *Security Focus*, May 12, 2006. http://www.securityfocus.com/news/11391

As to the threat, "For there to be a problem here, you're basically assuming a premise where you have some evil and nefarious election officials who would sneak in and introduce a piece of software," [a spokesman for Diebold] said. "I don't believe these evil elections people exist."[3]

Not only can poll workers or other election officials exploit this vulnerability, but also technicians or any other individual(s) with knowledge and a few minutes of access. Although Pennsylvania is going to "sequester" their Diebold machines and reload software on them, experts say this will not mitigate the problem. Even so, there is evidence that under the best intentions, Georgia's Elections Division has been unable to provide the kind of physical security that such attempts at mitigation would require. For one example, see "Unsecured voting machines at Georgia Tech, March 2, 2004: http://www.brendanloy.com/gallery/album21).

Other efforts at mitigation, rather than decertification, would require that voters could justifiably trust the security measures and procedures of the state. However, there is evidence that the state knowingly allowed voters to cast ballots in the last federal election on an insecure system. Case in point, in April 2004, Internet Security Systems (ISS) was called in by the governor to consult with the Georgia Technology Authority on the security of Georgia's DES. They found that the system was not secure and could not be secured in time for the 2004 General Election. This information was not made public, which meant that voters unknowingly were allowed to cast their votes on an insecure system in that presidential election.

Voting in a democracy is not about "trusting" that behind the curtain, individuals will do the right thing, as Diebold's spokesman quoted above seems to think. It's about systems of checks and balances, transparency, security, and auditability. The state's voting system fails on all counts. "If Diebold had set out to build a system as insecure as they possibly could, this would be it," said Rubin.[4]

Please consider the implications to the Board as well as the State of Georgia if nothing is done, or if efforts are made to give citizens a false sense that their votes are safe and being counted correctly, when in fact as long as this security vulnerability is there, no one among us can know with any degree of certainty if our votes are being counted as we intend.

We trust you will take the right action and immediately call for the decertification of the DES in Georgia.

Sincerely yours,

Donna Price
Director, Georgians for Verified Voting
http://www.gaforverifiedvoting.org

John Fortuin
Director, Defenders of Democracy
http://www.defendersofdemocracy.com

[3] Ibid, NYT.

[4] Ibid, Newsweek.