washingtonpost.com

Md. Plans Vote System Fixes After Criticisms

Security Review Finds 328 Flaws in AccuVote

By Brigid Schulte
Washington Post Staff Writer
Thursday, September 25, 2003; Page B01

An independent review released yesterday found 328 security weaknesses, 26 of them critical, in the computerized voting system Maryland has just purchased, flaws that could leave elections open to tampering or allow software glitches to go undetected.

State officials said they still intend to honor their $55.6 million contract with Diebold Elections Systems Inc. and are moving quickly to correct the problems before all counties begin using the machines in the March presidential primary.

"Because of this report, Maryland voters will have one of the safest election environments in the nation," said Gov. Robert L. Ehrlich Jr. (R), who last month ordered the review by computer security experts Science Application International Corp.

The heavily redacted review was intended to put to rest an explosive report by Johns Hopkins University computer scientist Aviel Rubin and his colleagues, who in July questioned the security of the AccuVote touch screen voting machines.

For Diebold executive Mark Radke, that's exactly what the new review did.

"The electorate throughout the entire country should be very comfortable with the security of our system," he said.

To ensure the integrity of the state's elections, Maryland officials are acting on a 23-step plan that includes writing a detailed security strategy, hiring an information systems security officer and training 18,500 election workers in computer security.

Further, as a result of the review, Diebold has rewritten its software to include better encryption coding and harder-to-crack passwords. The encryption and password upgrades will be made only for the machines destined for Maryland, Radke said, and would not be available for the 33,000 touch-screen machines already in use elsewhere.

For Rubin, the state's review "stirs the hornet's nest." While praising the thoroughness of the review, Rubin said he remains unconvinced that the state's actions would ensure safe elections. He called their action plan "unrealistic and naive."

"Accidents do happen," he said, saying it was misguided to build a security system that would rely on human poll workers with human fallibilities. "And it's not like we can't design better voting systems."

After analyzing Diebold's software source code that had mistakenly been left on an open Internet site, Rubin wrote a scathing report, saying that anyone with a minimum of computer knowledge could manufacture "homebrew" Smartcards and outsmart the system. He excoriated Diebold's software designers, who had built passwords such as 1111 into the machines, and said he would have flunked them in basic computer security classes.

Rubin's report fueled an already ugly, if obscure, battle pitting 900-some computer scientists -- who insist that currently manufactured voting machines cannot be trusted -- against elections officials and advocates for the disabled who say the touch-screen machines will be far better than any in use.

Some elections officials dismissed the Rubin report as flawed because it looked at software in isolation and not at how the voting machine would actually be used, with the poll workers and often thick manuals of policies and procedures that provide security checks.

Indeed, the security review acknowledged as much, saying the report looked not only at the software, but the entire human management and operation system. Still, Science Application International Corp. said it agreed with much of Rubin's technical analysis. And their conclusions were damning.

"The system, as implemented in policy, procedure, and technology, is at high risk of compromise," the company wrote in its executive summary. The action plan, they wrote, would reduce the risk to the system.

In particular, the review said Diebold needed to enhance computer encryption and password security. In the last election, the four Maryland counties using the Diebold machines in a pilot transmitted uncoded election results via modem at the close of the voting day.

"Unencrypted information could be intercepted and released prematurely or altered," the review said.

Further, it recommended, and Diebold agreed, that the manufacturer's main server be immediately removed from network connections to avoid possible backdoor attacks on the system.

The reviewers also recommended better computer security training for poll workers and a tighter audit system. Failure to do so, they wrote, "makes it significantly more likely that an intruder's actions will not be detected."

And without proper training, even well-meaning poll workers may not even know where security holes are that need to be monitored. "Exploitation of any of the resultant security holes," the review said, "could lead to voting results being released too soon, altered or destroyed."