March 1, 2006

We are writing to inform you of our deep concern regarding the impending purchase by Pennsylvania counties of electronic voting technologies possessing fundamental flaws that could place the outcomes of future elections at risk. While we believe the goals of the Help America Vote Act (HAVA) are laudable, our optimism is tempered by the knowledge that certain commercial e-voting systems we see offered for sale are vulnerable to a wide variety of threats, many of which could be carried out by a single perpetrator or a small group needing only a modest understanding of computer security. We base this assessment on our years of professional experience, both as faculty members in the Department of Computer Science and Engineering at Lehigh University and elsewhere, and our international reputations as experts in designing, implementing, and debugging complex software and hardware systems. Many of our fellow computer scientists across the country feel this same way.

Our concerns fall into three basic areas:

- **The first is the need for openness in the design and implementation of e-voting machine software and hardware.** Such policies give independent experts a chance to study what is being done and whether it is being done correctly. Past analyses of voting system software have identified numerous security holes, including the ineffective and misleading misuse of cryptographic keys hardwired into the code. Basing the security of a complex system on the ill-conceived belief that it will be possible to keep the source code secret has frequently proven to be a very bad idea. A system's security should not depend on such impossible-to-guarantee assumptions.

- **The second is the absolute necessity for independent hardcopy audit trails to ensure that e-voting systems are trustworthy**. This measure of safety is easy to add to an electronic display system by simply equipping it with an inexpensive printer that allows the voter to verify his/her vote on paper, behind glass. This receipt is then automatically inserted into in a secure lockbox to be retrieved should a recount be necessary. Without such a provision, there is simply no way to perform a true recount. We have heard manufacturers of e-voting systems call recomputing the final tally internal to the machine a “recount” -- but this notion is laughable. Simply re-adding a set of numbers that have already been compromised by a hacker's attack will not return a different result. If the only record of the election is stored internal to the e-voting

system, then the election can be compromised with no recourse for correction.

- **The third is the issue of online voter registration databases, which may prove to be a great convenience to voters, but also raise serious possibilities of fraud if not implemented correctly.** Such systems would be highly vulnerable to hacker attacks aimed at altering records, registering non-existent voters, deleting legitimate voters, and attempting to overwhelm the system at key times during the election process ("denial of service" attacks). There is no doubt such attacks will be attempted – the Internet offers sufficient proof of this fact (and in most such cases, the stakes are much lower and hence less attractive to our adversaries than a state-wide or national election). The solution, employing good security practices aimed at protecting online voter registration databases, is complicated by the fact that such databases must be made accessible to large numbers of individuals (many of whom are volunteers and not professionals) who help administer elections.

We close by observing that e-voting systems offer tremendous promise, but also substantial danger to our democratic process if not correctly implemented and operated. It is our fervent hope that you will call on independent experts from the field of computer science to help in assessing proposed e-voting systems and not simply trust what the manufacturers have to say in a matter of such importance to all citizens.

Sincerely,

Daniel Lopresti
Associate Professor

Glenn D. Blank
Associate Professor

Christine Hofmeister
Assistant Professor

Edwin Kay
Professor

Henry F. Korth
Professor

This letter reflects the opinions of the above individuals and does not necessarily represent the official position of Lehigh University.