

Fri, 31 Dec 2004

Dear Representatives and Committee Members,

I look forward to speaking to you on January 7th on the security and audit issues of electronic voting systems. I would like to thank each and every one of you for taking the time to hear what your constituents and fellow North Carolinians have to say.

I am planning to speak briefly on Industry Standards for Information Security, Auditing, and demonstrate how to change vote totals on a running instance of Diebold's GEMS software, which is the software used to tabulate vote data from DREs as well as optically-scanned and absentee ballots. This is the software that was recently highlighted in Gaston County when the problems with vote numbers surfaced, leading to the resignation of Sandra Page after 15 years of service.

In preparation for the next meeting, I have included a link to a recent discussion of electronic voting by some of my Infosec colleagues from May of 2004 that you may find interesting. Topics include instant-runoff voting, paper trails, and communication with state officials and the public.  
[http://www.cs.may.ie/~mmcgailey/Download/e-voting-6-04\\_british.pdf](http://www.cs.may.ie/~mmcgailey/Download/e-voting-6-04_british.pdf)

I have also included a link to the main site for the Common Criteria, which is the international standard used for building appropriately secure systems. <http://csrc.nist.gov/cc/>

One other issue I wanted to touch base with you on is Instant Runoff Voting. I think that IRV is a fabulous goal, long term. It stands to greatly reduce runoff costs and other problems once we have systems that can reliably handle it. The problem right now is that our electronic voting systems cannot reliably count straight races, and even the DRE manufacturers have said that they are not ready for IRV. Complicating things, IRV introduces a more confusing system in terms of auditability and security, since the ballots are more complex and normal indicators such as exit polls will not be able to easily reflect IRV results. Tracing back the will of the voter in the event of problems or fraud would be more difficult with IRV until a reliable procedure and design is in place, and any abuses are much less likely to be detected since the whole point of the IRV system is avoiding recounts. That's not to say that it can't be done, just that it is extremely important to get it right the first time, with proper design and certification.

Instant Runoff Voting is a great goal for us to work toward, but if we need to get a system in place for 2006 and 2008, IRV is not logistically viable.

For IRV to work, we need systems that are trustworthy and reliable, and that takes more time and money than we have available before the next election. An analogy I use for IRV is the flying car - definitely possible, and a great idea, but right now we won't get there by strapping a missile to a Yugo. Would it fly?

Sure - but I don't think it's what we want to rely on for safe and reliable transportation.

I would be happy to work with you towards IRV as a long-term goal, as I think it has merit as a long-term solution when properly designed and tested.

I look forward to seeing all of you on the 7th, and if there is any information that you would like for me to address, please let me know!

Regards,

Chuck Herrin, CISSP, CISA, MCSE, CEH

All outgoing correspondence is digitally signed. Lack of a valid signature indicates possible forgery.

My public key is available at <http://www.chuckherrin.com/ChuckHerrin.asc>