Response to "Testimony of George Gilbert — December 20, 2004"

Justin Moore

January 20, 2005

1 Introduction

The goal of this document is to serve as a response to the testimony given by George Gilbert before the North Carolina General Assembly Joint Select Committee on Electronic Voting Systems on December 20, 2004. Mr. Gilbert, while an experienced election director, makes several assertions about technology and the position of his opponents that are either incomplete, misleading, or factually incorrect. This document aims to provide constructive criticism of Mr. Gilbert's testimony and set the record straight in an objective fashion.

2 Testimony of George Gilbert

2.1 Opening Remarks

> *In the short time we had to survey the diverse opinions of the 100 county Directors, we reached three conclusions: 1) in counties that use DRE voting systems, both the election officials and voters are generally happy with them and trust them, 2) in counties that use optical scan voting systems, both the election officials and voters are generally happy with them and trust them and 3) no one thinks hand counting ballots is more accurate than automated tabulation.*

Here, Mr. Gilbert attempts to combine two distinct issues: the popularity of a voting system among election officials, and its accuracy and reliability. The popularity of a system has no bearing whatsoever on its quality; even a well-liked computer will crash if it is flawed.

As for Mr. Gilbert's final point, a 2001 study by CalTech and MIT examined five voting systems — hand-counted paper ballots, optically scanned ballots, lever machines, punchcards, and paperless Direct Record Electronic (DRE) machines — and came to the exact opposite conclusion [34]. Their data, covering two-thirds of the 3,155 counties in the United States over four presidential elections, provides this conclusion:

> The central finding of this investigation is that manually counted paper ballots have the lowest average incidence of spoiled, uncounted, and unmarked ballots,

> followed closely by lever machines and optically scanned ballots. Punchcard methods and systems using direct recording electronic devices (DREs) had significantly higher average rates of spoiled, uncounted, and unmarked ballots than any of the other systems.

The report goes on to state that counties which switched to DREs from other systems immediately saw the number of spoiled, uncounted, and unmarked ballots increase by up to 1.5% of all ballots cast. This is not intuition or a straw poll among election officials, but instead the facts surrounding voting system accuracy.

> *Our confidence in our voting systems is not blind trust. All counties employ extensive training, testing and auditing procedures. We take very seriously our responsibility to maximize the accuracy and integrity of our voting process. Many of these processes need improvement. In particular, enhanced training and support mechanisms are badly needed. Few, if any of us are satisfied that the security of our voting process is adequate. None expressed the feeling that it is gravely threatened.*

While it is true that election official training is the primary factor in determining the quality and accuracy of an election, one must examine all the parts of an election system. Paperless DREs remove both responsibility and control from election officials and places them in the hands of the voting machine vendors. If this is to be the case, then it should be the software engineers and security experts that provide an expert opinion as to whether or not the addition of this component is a grave threat to the security of our voting process.

> *This committee has an opportunity to establish a floor beneath which the quality of our elections will not fall. Such a floor will require enhanced standards for voting systems, enhanced support and training for election officials at all levels and the institutional mechanisms to evaluate and support voter registration and voting technology as it continues to evolve and improve.*
>
> *We have heard numerous calls for paper records of votes cast electronically. These voices would have you recommend the mandate of one particular technology that purports to "solve" certain hypothetical voting system problems.*

While Mr. Gilbert would like to dismiss our concerns as "hypothetical", one only needs to look at the newspaper headlines to see that our concerns are real [12, 1]. As of the writing of this document, the state of North Carolina is looking to spend $3.5 million on holding a replacement election due to the failure to store votes by a single paperless DRE in one county [33]. A paper record of these votes would have eliminated the need for this replacement election. In 2002, Wake County had to recall 436 voters to the polls after paperless DREs failed to record their votes properly [43]. A 2003 election in Hinds County, Mississippi experienced so many computer failures that the state had to void the election results and hold a new election [18, 17].

Furthermore, Table 1 shows that Burke County is facing the odd scenario of having fewer votes for President than any state-wide office, as well as the state senate race [24]. These

Contest	Votes Cast	# Less than Gov.	% Less than Gov.
Governor	32,104	0	0.00
U.S. Senate	32,085	19	0.06
State Senate, Dist. 44	32,084	20	0.06
Lt. Governor	31,677	427	1.33
Comm. of Insurance	31,577	527	1.64
Atty. General	31,569	535	1.67
Sec. of State	31,561	563	1.69
U.S. Congress, Dist. 10	31,542	562	1.75
Treasurer	31,392	712	2.22
Comm. of Labor	31,237	867	2.70
Auditor	31,224	880	2.74
Public Instruction	31,188	916	2.85
Comm. of Agriculture	31,170	934	2.91
President	30,762	**1,342**	**4.18**

Table 1: At least 1 in every 24 voters in Burke County did not cast a vote for President this year, while fewer than 1 in 1,500 did not cast a vote for the State Senate race.

documented failures and never-before-seen voting distributions are not hypothetical, nor are they rare when dealing with DREs.

> *Such a mandate would not establish a floor under our election systems but a ceiling above which we could not rise.*
>
> *It is time to inject a little reality into the discussion of "voter verified paper ballots." This so-called "verified paper trail "solution" would be extremely costly, nearly doubling the start up costs of accessible DRE voting systems (See Attachment I). It would be less secure and less accurate than most current electronic systems. It would seriously delay, or even close the door on, much needed improvements in the security, accuracy and accessibility of voting in North Carolina.*

Again, Mr. Gilbert attempts to confuse two separate issues: the cost of a paper trail and its effect on the security, accuracy, and accessibility of voting. Additionally, Mr. Gilbert provides no reliable facts, statistics, or examples to support his assertions. The attached spreadsheet makes several back-of-the-envelope calculations, but does not include any citations for discussions with voting machine vendors, experiments to determine how many DRE systems are needed in a given situation, or links to other states — such as Nevada — that use voter-verified paper ballots (VVPB). He provides no indication as to how he arrived as his figures.

Second, even though Mr. Gilbert admits he has no engineering or computer science background, he presents as fact that a VVPB system will decrease the effectiveness of electronic voting. This is in direct opposition to the virtually unanimous consensus of the computer

security and software engineering communities, who state that paperless DREs decrease the accuracy and effectiveness of a vote tabulation system [35].

Finally, Mr. Gilbert asserts — again, without any supporting evidence — that adding a VVPB will permanently prevent any further improvement in voting accuracy or security. While it is impossible to predict the future, we find it extremely hard to believe and highly unlikely that a voting machine vendor will turn down the opportunity to receive a portion of the up to $70 million North Carolina will spend on voting systems, simply because the state requires a VVPB.

> *Most election directors are not engineers or computer scientists. We do, however, represent 1,134 years of practical experience in administering elections using numerous voting systems, including DRE and optical scan, and would like to share with this committee some of the lessons those years have taught us, particularly as they relate to the questions of accuracy and security in vote tabulation.*

Here, Mr. Gilbert asserts that the users of a technology are equally or more qualified to characterize its costs and benefits than the very people who work in that field. While we have no doubt that Mr. Gilbert can provide substantial and effective comments on the usability of DRE machines, it is unlikely that he can quantify the security and reliability of these systems. For that, we must turn to experts in the fields of software engineering and computer security.

Opposing Mr. Gilbert's associates' 1,134 combined years of election are approximately 2,000 signatories of a petition opposing paperless DREs, all of whom classify themselves as "technologists." [37] While it is impossible to get an exact count, it is likely that these people — including the author of this paper — represent between 20,000 and 50,000 years of technological expertise. These people invented many of the technologies we use every day, and wrote the books and research papers that have shaped the technology industry over the last thirty years.

2.2 Assertions

> **Voters cannot see how their vote is counted with paper or with electronic records.**
>
> *The voter does not see what happens to their ballot, whether electronic or paper, after it is cast. Vote counting is public, but the ballots are anonymous. Verifying that a ballot is properly marked is the voter's responsibility. Verifying that that ballot is accurately counted is the Board of Elections responsibility.*

This is a subtle simplification of our position. We argue that the voters cannot see that their ballot is **marked** or even **created** in a way that expresses their intent. If a machine failure or tampering prevents the machine from creating the ballot properly, no amount of auditing, recounts, or end-of-the-day, post-mortem printouts can fix improperly marked ballots (especially if there is nothing to print).

Figure 1: Ballistic Recovery Systems and NASA are designing a parachute for small planes.

Both of Mr. Gilbert's assertions regarding responsibility are, technically, impossible with paperless DREs. Voters cannot "see" the file used to save their ballot; if they could, voters in Carteret County would have "seen" that their ballot did not exist. Similarly, election officials can only see the totals printed out by the computer, and did not "see" that the computer only contained 3,000 votes instead of 7,500 votes.

Airlines don't give parachutes to passengers to improve confidence in their safety.

Airlines give passengers oxygen masks (should the cabin tear open), buoyant seat cushions (should the plane crash into water), an inflatable life jacket with a whistle and bright light (should the passenger be unable to swim or need to attract attention during a rescue mission), and incorporate inflatable and floating escape ramps.

On top of this, Figure 1 depicts a new safety measure: a parachute for the plane itself, in the event of a complete loss of control or aerodynamics [4]. Future work will incorporate this safety measure into regional commuter jets [2]. Mr. Gilbert should examine the safety measures incorporated by airlines and private pilots before making inaccurate and misleading analogies.

Manual tabulation does not meet Federal Voting System Standards and cannot be effectively audited.

Manual counting of paper ballots has no equivalent to the Federal Voting System Standards for either security or accuracy.

This is a complete misinterpretation of the purpose of the Federal Voting System Standards. The FVSS provide a standard for certifying that complex, computerized systems meet certain performance and reliability goals; whether these goals are sufficient are a separate matter. The original purpose of the FVSS established by the Federal Election Commission (FEC) in 1990 was stated in the opening paragraph of the original standards [16].

> State and local officials today are confronted with voting system failures and increasingly complex voting system technology. The U.S. Congress, responding to calls for assistance from the states, authorized the Federal Election Commission (FEC) to develop national voting systems standards for computer-based systems, but mandated that they be voluntary.

Quite simply, manual counting is not addressed by the FVSS since there are no computer-based systems; the integrity of the count is based on procedure, not technology.

> *Manual counting by an ad hoc group of ballot counters brought together for a particular recount cannot be audited or tested for accuracy (or integrity).*

This statement is, at best, misleading. The definition of an audit, from the Merriam-Webster dictionary [22] is

> **1 a :** a formal examination of an organization's or individual's accounts or financial situation **b :** the final report of an audit
>
> **2 :** a methodical examination and review

We are not sure if Mr. Gilbert means to imply that it is impossible to perform a methodical examination and review of paper ballots. The integrity of an audit depends on the integrity of the people conducting the audit and the details of the rules governing the audit. For example, Ohio avoided the dimpled/pregnant/hanging chat fiasco that plagued Florida in 2000 because Ohio state law states clearly how many corners of the punchcard must be freed from the paper to count as a vote [27].

If Mr. Gilbert is claiming that there is a shortage of trustworthy people in North Carolina, or a lack of guidance in state law for conducting hand counts of paper ballots, we are confused. We assume he does not mean the former, and at least three counties use hand-counted paper ballots without raising the kind of integrity questions seen in Gaston [44], Guilford [25], Craven [5, 6], Wake [43], and Carteret [12] counties the last three years.

> **If anyone really believes that thousands, tens of thousands, even millions of paper ballots could be hand counted accurately, they have never attempted to hand count such ballots. Most people no longer even attempt to count out a roll of dimes.**

Again, the 2001 CalTech/MIT study's findings contradict Mr. Gilbert's assertions [34]. The facts show that error rates for hand-counted paper ballots are 33% to 50% lower than paperless DREs. The hand recounts in the Washington state gubernatorial race uncovered thousands of votes not counted by the computer tabulators [41]. Again, Mr. Gilbert provides no facts to support his claims.

> *If a printed paper replica of a DRE ballot is mandated, no vendor has any incentive to develop more accurate, more secure paperless systems that could exceed the accessibility, accuracy and security of a paper based system.*

As mentioned above, we find it unlikely that vendors will stop improving the quality of their products, especially given the tens of millions of dollars up for grabs. Again, Mr. Gilbert makes unfounded assertions about the accuracy and security of paperless systems, assertions that are flat-out rejected by those with software engineering and security experience.

> *We are already experiencing serious misallocation of research and development involving DRE systems as a result the prospective mandates of a DRE paper trail. We have multiple examples of lost DRE votes due to inadequate vote storage mechanisms. We have no documentation of fraud, malware or tabulation error in DRE systems.*

As one who has spent several years working in the software industry, both during the dot-com era and in Silicon Valley, it is highly unlikely that a software vendor will halt quality assurance (QA) and testing simply to attach a printer to a computer. In truly strict software development methods, the programmers performing QA are a completely separate team from the programmers writing the initial product, which are a completely separate group from the research group. Unless the voting machine vendors practice lackluster and unprofessional software development methods, the two or three teams should be independent and able to focus on separate tasks.

Secondly, Mr. Gilbert again makes unfounded assertions as to the accuracy and integrity of the DRE machines. History may provide some guidance as to who has the burden of proof in this situation [30].

> "Because the idea that you accept risks, the consideration of this thing is always during flight. It is a flight review, and so you decide what risks to accept. I read all of these reviews, and they agonize whether they can go even though they had some blow-by in the seal or they had a cracked blade in the pump of one of the engines, whether they can go the next time or this time, and they decide yes. Then it flies and nothing happens.
>
> "Then it is suggested, therefore, that that risk is no longer so high. For the next flight we can lower our standards a little bit because we got away with it last time. If you watch the criteria of how much blow-by you're going to accept or how many cracks or how long the thing goes between cracks, you will find that the time is always decreasing and an argument is always given that the last time it worked.

> "It is a kind of Russian roulette. You got away with it, and it was a risk. You got away with it, but it shouldn't be done over and over again like that. When I look at the reviews, I find the perpetual movement heading for trouble."

The above was said by Dr. Richard Feynman on April 3, 1986, during the Presidential Commission on the Space Shuttle *Challenger* Accident. That Commission concluded

> "[the] eventual cause of the *Challenger* accident was a technical failure of a solid rocket booster O-ring. This hardware failure was a direct result of management failures that included poor communications, misinterpretation of information, incentives to launch unless proven categorically unsafe and excessive optimism under schedule pressures."

This sentiment was echoed in 2003 by NASA Director Sean O'Keefe in the wake of the *Columbia* disaster [13].

> "[T]here needs to be a fundamental shift from the current ethic of 'prove that it is unsafe' to one wherein all the processes seek to 'prove that it is safe.' "

While the shuttle disasters are dramatic examples of this mentality, history is full of situations in which higher-level management overrode the vehement warnings of experienced engineers.

> *Most proponents of a paper trail acknowledge that lost votes are a greater threat than fraud or hacking. Most would acknowledge that, if an accurate electronic record exists, it can more accurately be tabulated electronically than by a comparable manual count.*

Proponents of a paper trail assert that paperless systems are less reliable and more failure-prone than paper-based systems, regardless of the order in which one ranks the risks associated with paperless systems. Mr. Gilbert creates an idealized case — one in which there is an accurate electronic record — and asserts that, in that case, computerized tabulation is superior. This flies in the face of Mr. Gilbert's stated goal of "inject[ing] a little reality" into this discussion. We are here to evaluate the system as is exists and operates in real conditions, not as it might exist in an idealized situation.

> *Most DRE vendors are concentrating their research and development on systems and modifications to existing systems that meet the paper trail standard. Little attention appears to being placed on mechanisms to enhance the independent storage and security of the electronic ballot records.*

Again, Mr. Gilbert asserts that the primary problem with paperless machines is independent storage and security of electronic ballot records. Again, Mr. Gilbert ignores the history of DRE failures, encompassing every aspect of the paperless system.

- A DRE in Fairfax, VA, in 2003 was proven to switch approximately 1% of the votes from the Republican candidate for school board to the Democratic candidate. The margin of victory for the Democrat was within this 1% margin, but no audit could determine what actually happened that day [7, 8].

- A DRE in Baltimore, MD, was proven to have an incorrect ballot layout that prevented an unknown number of citizens from casting a vote in the U.S. Senate primary. No corrective measures were available [20].

- Approximately one-third of the precincts in San Diego, CA, experienced a total failure of their DREs during a Marcy primary, causing several of these precincts to remain closed until at least noon. Unknown numbers of voters were turned away, disenfranchised [21].

These problems are the tip of the iceberg; VerifiedVoting.org publishes a 51 page document, detailing a variety of DRE failures and unexplained behavior through March, 2004 [36].

> *How many years will this critical need be set back while we bask in the false security of paper ballots. I would speculate, until the first major recount is required.*

Washington state underwent a hand recount of three million ballots, revealing a different governor than the one elected by the original count [40, 39].

Contrast this with North Carolina, which will "bask" in a full state-wide re-vote this spring. At what point will we dispel the false accuracy and reliability of paperless DREs?

> **If tampering or mis-tabulation is suspected, a hand recount of ballots would likely become unmanageable or too costly to provide a realistic solution.**
>
> *If we truly suspected that an electronic tabulation system (DRE or optical scan) had malfunctioned in properly recording or tabulating the votes, which contests would have to be recounted? With no way of knowing which contests might have been affected or by how much, a comprehensive, full ballot, recount would likely be required.*

The failure or tampering of a DRE is a distinct event from the failure or tampering of an optical scan machine. If an optical scan machine fails or is tampered with, it is possible to retrieve the ballots cast on that machine and re-run them through a different, functional tabulator. If that is insufficient, we can count them by hand.

If a DRE fails or is tampered with and we do not learn this until after voters cast their ballots on the machine, there is little we can do. This is exactly the situation with Carteret County; we can do nothing but hope that the margin of victory for all contests on the ballot in that precinct are greater than the number of voters in that precinct. Otherwise, North Carolina law requires a re-vote in the jurisdiction of that contest [26].

Since a DRE has no paper ballots, the only realistic solution is a replacement election, hardly a manageable, desirable, or cost-effective measure.

Attachment II projects the cost of a comprehensive hand recount of paper ballots in the 2004 general election in Guilford County, NC, where 201,757 ballots were cast. The projected 673 people counting for eight hours a day for two weeks at a cost of more than $700,000 (more than double the cost of the election) is likely a best case scenario.

Perhaps we could examine the procedures used by the state of Washington in their statewide hand recount. The "Frequently Asked Questions — General Election Recount Procedures" page on the website of the Washington Secretary of State [38] says

Q: How long does it take to conduct the recount?

Most counties can recount all ballots in one day. Some counties may take two days. King County will need approximately four days to recount all ballots.

[*NOTE: 876,452 votes were cast in the 2004 gubernatorial race in King County*]

[. . .]

Q: What is a requested recount and how does it work?

Any candidate or political party officer can request a recount in any race.

The request may only be made after the Secretary of State certifies the final returns on December 2, 2004.

To finance the recount, the requesting party must make a deposit with the state in the amount of *15 cents per vote for a machine recount and 25 cents per vote for a manual recount*.

[*NOTE: Emphasis ours.*]

By this measure, the cost of a Guilford County recount should be $201,757 \times \$0.25 = \$50,439.25$, not $700,000. The state of Washington did, in fact, spend a total of $730,000 for the hand recount [9].

Even more real and hypothetical accident and fraud scenarios can be lodged against computer generated paper trails than against paperless electronic voting.

We already know that paper is more easily lost, miscounted or modified than electronic records. We have more than 200 years of documented problems with paper records (including those in 2004) to look to.

Again, Mr. Gilbert would assert that we "know" something which is, in fact, incorrect. As shown before, the number of spoiled, uncounted, or unmarked DRE ballots is 50% to 100% higher than non-punchcard, paper-based systems. The track record of paperless DRE machines is short, but troubling, although not surprising to computer scientists.

As a point of comparison, let us examine the amount of money stolen by taking paper money and the amount of money "stolen" through online fraud, identify theft, or hacking.

Counting Method	Gregoire	Rossi	Bennett	Total
Election Day	1,371,153	1,371,414	63,346	2,805,913
Mandatory Machine Recount	1,372,442	1,372,484	63,415	2,808,341
Hand Recount	1,373,361	1,373,232	63,465	2,810,058

Table 2: The difference in number of votes between the two machine recounts was 2,428. The difference in number of votes between the hand recount and machine recount was 1,717.

The 2003 Justice Department Uniform Crime Reports statistics show $514 million taken in robberies, approximately $45.3 million of this in bank robberies [15]. The U.S. Secret Service and American Banking Association reported approximately $4 - $5 billion stolen through electronic means in 2002 [11].

The criminals have learned that electronic money is easier to manipulate and steal than paper money; there is no reason to think that electronic votes are any different, especially given the relative ease with which banks can audit for correctness, as opposed to election officials.

> *As the State of Washington is currently demonstrating in its Governor's race, with paper ballots, whether counted mechanically or manually, each recount will yield a different result. Which one is correct?*

Table 2 shows the results for the Washington state recounts, taken from the website of the Secretary of State [41]. The difference in the number of votes between the two machine counts — election day and the first recount — was 2,428 votes. The difference between the two recounts — hand and machine — was 1,717 votes. Of these 1,717 votes, 723 were absentee ballots for which the computer incorrectly rejected a valid signature. Thus, the hand recount agreed very closely with the original recount, and even reduced the number of votes missed by the machines. As of the writing of this document, the Republican candidate may demand another hand recount, at which point we will have more data to examine [3]. Currently, though, the hand recount numbers appear to agree with the conclusions of the CalTech/MIT study: hand-counted paper ballots are the most accurate voting system.

> *Stuffed ballot boxes in the Ukraine and DRE paper trails in untrustworthy hands in Venezuela are additional contemporary examples of the fact that the paper solution is less than trustworthy.*

The electoral fraud in the Ukraine and Venezuela were the result of corruption, and not tied to any particular voting technology. If the election officials are untrustworthy, nothing can be done to guarantee the integrity of the election. Below is an excerpt from an article describing how some of the fraud occurred [28].

> It was 5.30pm on election day in Ukraine when the thugs in masks arrived armed with rubber truncheons.

> Vitaly Kizima, an election monitor at Zhovtneve in Ukraine's Sumy region, watched in horror as 30 men in tracksuits stormed into the village polling station.
>
> "They started to beat voters and election officials, trying to push through towards the ballot boxes," he told The Telegraph.
>
> [. . .]
>
> Maya Syta, a journalist working at polling station 73 in a Kiev suburb, witnessed ballot papers destroyed with acid poured into a ballot box. "The officials were taking them out of the box and they couldn't understand why they were wet," she said.
>
> "Then I saw they started to blacken and disintegrate as if they were burning. Two ballots were wrapped up into a tube with a yellow liquid inside. After a few moments they were completely eaten up."

No voting technology would withstand this kind of fraud. Having a computer in the polling place would not prevent a voter from being violently assaulted and beaten. If the precinct had DREs, it would be only logical for the thugs to pour their acid on the machine instead of any paper ballots.

> *As Dr. Michael Shamos, of the School of Computer Science at Carnegie Mellon University, recently wrote to me, maintaining physical integrity of paper records from a few hundred thousand voting machines in 170,000 polling places is not a solved problem.*

While Dr. Shamos is an accomplished researcher in the field of computational geometry, he has no formal background in computer security or software engineering [31]. He has never published a peer-reviewed paper in any conference, workshop, or journal that focuses on security, networking, software engineering, computer usability, operating systems, or distributed systems. Consulting Dr. Shamos on issues of computer security or software is like a heart surgeon asking a brain surgeon for help on a quadruple-bypass; both are brilliant surgeons, but only one works in the relevant sub-field.

As for the substance of Dr. Shamos's statement, maintaining the electronic integrity of paperless ballots in any large number of polling places has never been attempted, much less attempted successfully. Physical security is a straight-forward problem. Computer security and software development is a complex challenge that even banks, hospitals, and the military do not get correct. The results include crashed Automated Teller Machines [19], months of detailed hospital records and patient information stolen [29], and a multi-billion-dollar Aegis destroyer left stranded in the middle of the Atlantic Ocean [32].

It is possible to minimize risks, if one is willing to pay billions of dollars per software component; Boeing spent five years and $4 billion to write the control code for the 777 [10], a project 5% the size of Microsoft Windows alone [14].

> *In addition, there is no greater assurance that a paper trail from a DRE machines actually represents the voters choices. For instance, what if, after every 10th voter*

verifies his or her paper replica of their ballot, casts their vote and walks away, the voting machine voids that paper record and prints a new, altered one.

This argument, on the face, is ridiculous and flies in the face of Mr. Gilbert's stated goal of "inject[ing] a little reality" into this discussion. Mr. Gilbert does not attempt to explain how the machine could "void" a paper ballot and print a new one without using an extra physical ballot. In such a scenario, the machine would use 110 paper ballots for every 100 votes cast on that machine; a simple comparison of the number of paper ballots placed in the feed tray with the number of ballots the machine recorded — a fundamental component of any elementary post-election procedure — would uncover this problem.

Mr. Gilbert's example essentially makes the case for a VVPB. The basic challenge this attacker faces, assuming they want to avoid detection, is how to discard the "voided" ballot. A magnetic record on a hard disk is trivial to erase without evidence it ever existed; a paper record leaves a tangible record that must be discarded and will be detected.

It could happen. It could even go unnoticed by voters and precinct officials alike. After all, it appears that 4,438 error messages may have gone unnoticed in Carteret County in October.

A precinct official that does not keep track of the physical ballots given to them, much less being oblivious to dozens of extra ballots, is incompetent and has no place in our electoral system. An election official that does not see or understand a confusing error message on a 4" by 1.5" panel is excusable, especially if the computer continues to indicate that it is recording votes properly [1]. Any competent programmer would not to attempt to "save" ballots on a full hard drive, much less present a new ballot to a voter after the hard drive is full.

Yet they didn't. The failure *did* happen. After all, it appears that we are in for a $3.5 million state-wide replacement election.

2.3 Conclusions

Current voting system standards are inadequate. Inserting technology discredited more than 100 years ago will not make them better. But I would be willing to bet that, with standards that require better security and verification, better voting systems would be forthcoming.

Mr. Gilbert again offers no proof that current paper-based systems are less secure than the alternative he presents; he merely asserts that paper is "discredited." Again, the research in this area contradicts him [34].

Current mechanisms for reviewing and testing the hardware and software used in voting systems are inadequate. But I would be willing to bet that the engineers, computer and behavioral scientists in North Carolina's State University system could quickly tool up for solving that challenge.

We have. It is called a voter-verified paper ballot.

The signatories of the pro-VVPB petition at VerifiedVoting.org include faculty members at virtually every major university in the United States, including Harvard, Yale, MIT, Duke, Princeton, Georgia Tech, Utah, UVA, UNC-Chapel Hill, UNC-Wilmington, Johns Hopkins, Rice, UT-Austin, LSU, Maryland, Stanford, and CMU, among dozens of others. Also included are software engineers and researchers at every major technology company, including Microsoft, Apple, IBM, Hewlett-Packard, Sun Microsystems, Lockheed-Martin, AOL, Intel, Bell Labs, Xerox PARC, and MCI Worldcom, among dozens of others. Included are researchers and staff at every single government research lab, including Oak Ridge, Lawrence Livermore, NASA, and contractors such as MITRE and Honeywell [37].

The technology community has spoken. We are waiting for others to start listening.

> *Current support and training for election offices and precinct officials is inadequate. But I would be willing to bet that, working together with the state's Universities and Community Colleges, a support and training network could be built that would be the envy of the nation.*

If Mr. Gilbert is eager to shovel the responsibility for maintaining the integrity of the electoral system of North Carolina onto the computer scientists of this state, he must be willing to listen to all the feedback from the computer science community, not just a lone, unqualified voice that agrees with him.

> *If the General Assembly wants to insure ongoing improvements in the accuracy, accessibility and security of voting in North Carolina, a "Center for Election Systems Evaluation & Support," as outlined in my December 13th statement to this committee, is the most important step you can take. I strongly urge you to establish that floor and not a ceiling on the quality of our elections.*

The members of several technology-oriented groups — including the National Committee for Voting Integrity — stand willing to aid North Carolina in increasing the integrity of its electoral process. Software certification is only one part of the puzzle, and it is important that election officials and elected representatives realize the realistic limits of the technology available.

3 Conclusion

The night of January 27, 1986, engineers from Morton-Thiokol — the company that designed and produced the solid-booster engines for the space shuttle — held a teleconference with a team at NASA. After suffering several launch delays prior to the proposed flight the next day, NASA was incredulous that the Morton-Thiokol engineers were suggesting another delay. During a brief recess the Morton-Thiokol Senior Vice President, Jerry Mason, turned to Vice President of Engineering, Bob Lund, and told him to "take off your engineering hat and put on your management hat." [42]

The NASA managers voted to approve the launch, since they did not consider the arguments of the engineers to be proof of booster failure. At Cape Kennedy the Morton-Thiokol representative, Allan McDonald, refused to sign the formal recommendation to launch; the vice president for booster rockets, Joe Kilminster, signed in his place.

On March 11, 1986, aerospace engineer Calvin Moeller wrote to the L.A. Times, attributing the disaster to arrogance [23].

> "The arrogance that prompts higher-level decision-makers to pretend that factors other than engineering judgment should influence flight safety decisions, and, more important, the arrogance that rationalizes overruling the engineering judgment of engineers close to the problem by those whose expertise is naive and superficial by comparison."

We will not put on our management hat, and we will not allow other factors to overrule the engineering and research judgment telling us that paperless DREs are a disaster waiting to happen, if you do not consider Carteret County a disaster that has already happened. The computer science community is willing to educate and advise the election community as to the benefits, costs, and risks of the available technology. We hope that this committee accepts this offer and strives to seek expertise in each area from those who have obtained it professionally, and not merely through use of those systems.

References

[1] AP. Computer loses more than 4,000 early votes in Carteret. *Charlotte Observer*, November 2004. http://www.charlotte.com/mld/observer/news/local/10099907.htm.

[2] AP. Huge parachute designed to save crashing planes. *CNN Online*, December 2004. http://www.cnn.com/2004/TECH/12/22/airplane.parachutes.ap/index.html.

[3] AP. Wash. GOP Demands New Governor Election. *ABC News Online*, January 2005. http://abcnews.go.com/Politics/wireStory?id=388506.

[4] Ballistic Recovery Systems, Incorporated. BRS Homepage, January 2005. http://brsparachutes.com/.

[5] S. Book. Craven vote totals become offi cial. *New Bern Sun Journal*, November 2004.

[6] S. Book. Two errors led to incorrect vote totals. *New Bern Sun Journal*, November 2004.

[7] D. Cho. Fairfax Judge Orders Logs Of Voting Machines Inspected. *Washington Post*, page B01, November 2003. http://www.washingtonpost.com/wp-dyn/articles/A6291-2003Nov5.html.

[8] D. Cho. Fairfax Voting Machines A 'Failure'. *Washington Post*, page B01, January 2004. http://www.washingtonpost.com/wp-dyn/articles/A4790-2004Jan9.html.

[9] CNN. County recount gives win to Democrat, December 2004. http://www.cnn.com/2004/ALLPOLITICS/12/23/wash.gov/.

[10] V. Cortellessa, B. Cukic, D. D. Gobbo, A. Mili, M. Napolitano, M. Shereshevsky, and H. Sandhu. Certifying Adaptive Flight Control Software. *In the Proceedings of the Second International Software Assurance Certifi cation Conference*, September 2000. http://www.isacc.com/presentations/3c-bc.pdf.

[11] R. X. Cringely. How to Steal 65 Billion: Why Identity Theft is a Growth Industry. September 2003. http://www.pbs.org/cringely/pulpit/pulpit20030911.html.

[12] M. Crouch. Glitch could force state to vote again. *Charlotte Observer*, November 2004. http://www.charlotte.com/mld/charlotte/10133265.htm?1c.

[13] A. Deering and W. E. Haynes. NASA Under Siege. *Risk and Insurance*, May 2003. http://www.riskandinsurance.com/040501choice.asp.

[14] M. Delio. Linux: Fewer Bugs Than Rivals. *Wired News Online*, December 2004. http://www.wired.com/news/linux/0,1411,66022,00.html?tw=wn%5Ftophead%5F1.

[15] Federal Bureau of Investigation. Uniform Crime Reports – 2003, October 2004. http://www.fbi.gov/ucr/03cius.htm.

[16] Federal Election Commission. Performance and Test Standards for Punchcard, Marksense, and Direct Recording Electronic Voting Machines, January 1990.

[17] J. Goodman. District vote set; contender may quit. *Clarion-Ledger*, January 2004. http://www.clarionledger.com/news/0401/21/ma04.html.

[18] C. Harden. Long lines, machine malfunctions mark today's voting. *Clarion-Ledger*, November 2003. http://www.clarionledger.com/news/0311/04/mvproblems.html.

[19] R. Lemos. 'Slammer' attacks may become way of life for Net. *News.com*, February 2003. http://news.com.com/Damage+control/2009-1001%5F3-983540.html.

[20] J. Liss. Think You Voted in Md.? Think Again. *Washington Post*, page B08, March 2004. http://www.washingtonpost.com/wp-dyn/articles/A37007-2004Mar6.html.

[21] J. McDonald and L. Monteagudo. Poll workers, voters cite tied-up hotline, poor training, confusion. *Union Tribune*, March 2004. http://www.signonsandiego.com/news/politics/20040307-9999-1n7vote.html.

[22] Merriam - Webster. M-W Online Dictionary, January 2005. http://www.m-w.com/cgi-bin/dictionary?va=audit.

[23] C. Moeller. Challenger Catastrophe. *Los Angeles Times*, March 1986. Metro Section, p4.

[24] J. Moore. Summary of N.C. Voting Per Race in 2004, December 2004. http://www.cs.duke.edu/ justin/voting/dat/2004/BURKE.html.

[25] News and Observer. N.C. voting problems: 2004 edition. November 2004. http://newsobserver.com/news/story/1852104p-8179802c.html.

[26] North Carolina State Law. Section 163-182.13 – New Elections. *NCGA General Statutes*, January 2005.

[27] Ohio State Law. Section 3506.16(B)(2). *Ohio Revised Code*, January 2005.

[28] T. Parfitt and C. Freeman. Revealed: the full story of the Ukrainian election fraud. *News and Telegraph Online*, November 2004. http://www.telegraph.co.uk/news/main.jhtml?xml=/news/2004/11/28/wukra28.xml.

[29] K. Poulsen. Hospital Records Hacked – Hacker easily penetrates hospital net, pilfers thousands of patient records. *SecurityFocus*, December 2000. http://www.securityfocus.com/news/122.

[30] W. P. Rogers, N. A. Armstrong, D. C. Acheson, E. E. Covert, R. P. Feynman, R. B. Holtz, D. J. Kutyna, S. K. Ride, R. W. Rummel, J. P. Sutter, A. B. Walker, A. D. Wheelon, and C. E. Yeager. Report of the PRESIDENTIAL COMMISSION on the Space Shuttle Challenger Accident. 5:2469–2470, April 1986.

[31] M. I. Shamos. Resumé (short version), January 2005. http://euro.ecom.cmu.edu/people/faculty/mshamos/resshort.htm.

[32] G. Slabodkin. Software glitches leave Navy Smart Ship dead in the water. *Government Computer News*, July 1998. http://www.gcn.com/archives/gcn/1998/july13/cov2.htm.

[33] B. Smith. New statewide election for ag commissioner ordered. *New Bern Sun Journal*, December 2004.

[34] The Caltech/MIT Voting Technology Project. Residual Votes Attributable to Technology, March 2001. http://www.vote.caltech.edu/Reports/.

[35] U.S. Public Policy Committee for the Association for Computing Machinery. Policy Issues Related to Voting Technology and Standards, May 2001. http://www.acm.org/usacm/voting-letter.html.

[36] Verified Voting. Electronic Miscounts and Malfunctions In Recent Elections, March 2004. http://www.verifiedvoting.org/downloads/resources/documents/ElectronicsInRecentElect

[37] Verified Voting. Resolution on Electronic Voting, January 2005. http://www.verifiedvoting.org/article.php?id=5028.

[38] Washington Secretary of State. Frequently Asked Questions – General Election Recount Procedures, January 2005. http://www.secstate.wa.gov/office/osos%5Fnews.aspx?i=SPlmpeBt1xLxpksVqw%2Ft9w%3D%3D.

[39] Washington Secretary of State. Washington State 2004 General Elections Hand Recount Results, January 2005. http://vote.wa.gov/general/recount.aspx.

[40] Washington Secretary of State. Washington State 2004 General Elections Machine Recount Results, January 2005. http://vote.wa.gov/general/recount.htm.

[41] Washington Secretary of State. Washington State 2004 General Elections Results, January 2005. http://vote.wa.gov/general/.

[42] P. Werhane. Engineers and Management: The Challenge of the Challenger Incident. *Journal of Business Ethics*, pages 605–616, 1991.

[43] WRAL News. Electronic Ballots Fail To Win Over Wake Voters, Election Officials. November 2002. http://www.wral.com/news/1753809/detail.html.

[44] WRAL News. State Races Still In Play As Wake Misses Deadline, Gaston Finds 12,000 Votes. November 2004. http://www.wral.com/news/3903248/detail.html.