BRENNAN CENTER FOR JUSTICE
AT NYU SCHOOL OF LAW

Committee on Rules and Administration
United States Senate

Testimony of

MICHAEL WALDMAN

Executive Director
Brennan Center for Justice at New York University School of Law

February 7, 2007

The Brennan Center for Justice thanks the Senate Committee on Rules and Administration for holding this hearing.[1] We appreciate the opportunity to share with you the results of our extensive studies to ensure that our nation's voting systems are more secure, reliable and accessible.[2] The Brennan Center for Justice is a nonpartisan think tank and advocacy organization that focuses on democracy and justice. We are deeply involved in the effort to ensure accurate and fair voting, voter registration, campaign finance reform and a reformed redistricting system.

I. THE BRENNAN CENTER'S WORK ON VOTING SYSTEM SECURITY

Since the electoral debacle of 2000, the United States has broadly moved toward using new electronic machines to conduct elections. This is as wide a shift in voting technology as any in our history. The new systems promise fewer ambiguous votes (for example, in the case of Florida in 2000, "hanging chads") and greater accessibility to the disabled. But they spawned doubt and suspicion, leaving many Americans uncertain whether their votes are securely cast and accurately counted. The issue became clouded in partisanship and conspiracy thinking, marked by conjecture and anecdote.

In 2005, in response to this widespread confusion and concern, the Brennan Center assembled a Task Force of internationally renowned government, academic and

[1] Michael Waldman was Special Assistant to the President for Policy Coordination and Assistant to the President and Director of Speechwriting for President Bill Clinton. During his government service, he was the top administration policy aide on political reform. He was a Lecturer in Public Policy at Harvard University's John F. Kennedy School of Government, former executive director of Public Citizen's Congress Watch, and is the author or editor of five books on government, the presidency and the law. He is a graduate of Columbia University and New York University School of Law.

[2] Lawrence Norden *et al.*, THE MACHINERY OF DEMOCRACY: VOTING SYSTEM SECURITY, ACCESSIBILITY, USABILITY AND COST (Brennan Center for Justice ed., 2006), *available at* http://brennancenter.org/subpage.asp?key=38&init_key=105

private-sector scientists, voting machine experts, and security professionals to perform the nation's first methodical threat analysis of the major electronic voting systems.[3] The Task Force sought a simple goal: to determine, quantify and prioritize the greatest threats to the integrity of our voting systems, and to identify steps that we can take to minimize those threats.

Working with election officials, the Task Force analyzed the nation's major electronic voting systems for two years. It issued *The Machinery of Democracy: Protecting Elections in an Electronic World* (the "Brennan Center Security Report") in June 2006.[4] The conclusions of the Brennan Center Security Report are clear:

- In fact, all of the nation's electronic voting systems – every single one –have serious security and reliability vulnerabilities (including especially, the malicious or accidental insertion of corrupt software or bugs).

- The most troubling vulnerabilities of each system can be significantly remedied; but few jurisdictions have implemented any of the key security measures that could make the least difficult attacks against voting systems substantially more secure.[5]

Most importantly, the Task Force recommended:

- **Automatic audits, done randomly and transparently, are necessary if voter verifiable paper records are to enhance security.** The report called into doubt basic assumptions of many election officials and the public, by finding that using voter-verified paper records without routinely comparing some portion of those paper records to the electronic tally – as is done in twenty-four states with voter-verified paper records – is of "questionable security value."

- **Wireless components on voting machines are particularly vulnerable to attack.** The report finds that machines with wireless components could be attacked by "virtually any member of the public with some knowledge of software and a simple device with wireless capabilities, such as a PDA."

- **The vast majority of states have not implemented election procedures or countermeasures to detect a software attack** even though the most troubling vulnerabilities of each system can be substantially remedied.

Among the countermeasures advocated by the Task Force are routine audits comparing voter-verified paper trails to the electronic record and bans on wireless components in voting machines. Currently only New York and Minnesota ban wireless

[3] For a list of Task Force members *see* Appendix A of this Statement. The study's methodology is described in Appendix B.
[4] *See* Lawrence Norden *et al.*, *supra*, note 2.
[5] *Id.* at 3.

components on all machines; California bans wireless components only on DRE machines. The Task Force also advocated the use of "parallel testing": random, Election Day testing of machines under real world conditions. Parallel testing holds its greatest value for detecting software attacks in jurisdictions with paperless electronic machines, since, with those systems, meaningful audits of voter-verified paper records are not an option.

Fortunately, steps can be taken to make electronic voting systems substantially more secure. For the most part, they do not involve significant changes in system architecture. But they do require legislative changes – and resources, training, coordination and professionalization on a scale heretofore not known in American election administration. These changes can be made while assuring that our voting systems are fully accessible to all Americans.

II. BRENNAN CENTER TASK FORCE RECOMMENDATIONS IN DETAIL

There is a substantial likelihood that the election procedures and countermeasures currently in place in the vast majority of states would not detect a cleverly designed software attack program. The regimens for audits and testing proposed in the Brennan Center Security Report are important tools for protecting voting systems from many types of attack, including software attack programs.

Most jurisdictions have not implemented these security measures. Of the 27 states that require a voter-verified paper record, less than half require automatic audits of those records after every election, and only two of these states – California and Washington – conduct parallel testing.[6] Moreover, even those states that have implemented these countermeasures have not developed the best practices and protocols that are necessary to ensure their effectiveness in preventing or revealing attacks or failures in the voting systems.

Recommendation #1: Conduct Automatic Routine Audit of Voter Verifiable Paper Records.

Advocates for voter-verified paper records have been extremely successful in state legislatures across the country.[7] Currently, 27 states require their voting systems to produce a voter-verified record, but 14 of these states do not require automatic routine audits comparing the paper and electronic records.[8] The Task Force concluded that an

[6] The states that have some kind of statutory requirement for audits are: AZ, CA, CO, CT, HI, IL, ME, MN, NM, NY, NC, WA, and WV.

[7] The Brennan Center recommends voter-verified audit records that are independent of the software used in voting machines. The only such technology currently available and in use – and the only technology studied by the Task Force – is voter-verified paper records. Non-paper technologies that meet this standard may be developed and available in the future.

[8] The 27 states are: AL, AZ, CA, CO, CT, HI, ID, IL, ME, MI, MN, MO, MT, NC, NH, NJ, NM, NV, NY, OH, OR, SD, UT, VT, WA, WI, and WV.

independent voter-verified paper trail without an automatic routine audit is of questionable security value.[9]

By contrast, a voter-verified paper record accompanied by a solid automatic routine audit can go a long way toward making the least difficult attacks much more difficult. Specifically, the Task Force recommended the following audit measures, which, it concluded, would render attacks far less likely because they would force an attacker to involve hundreds of more informed participants in her attack.

- A small percentage of all voting machines and their voter-verified paper or audit records should be audited.
- Machines to be audited should be selected in a random and transparent way.
- The assignment of auditors to voting machines should occur immediately before the audits. The audits should take place by 9 a.m. on the day after polls close.
- The audit should include a tally of spoiled ballots, undervotes, and overvotes.
- A statistical examination of anomalies, such as higher than expected cancellations or under-and overvotes, should be conducted.
- Solid practices with respect to chain of custody and physical security of paper or other audit records prior to the audit of those records.

Recommendation #2: Conduct Parallel Testing.

Although we strongly believe the best current security measure is to use voter-verified paper records as the basis for auditing the electronic record, steps can be taken to improve security should jurisdictions fall short of that goal.

For paperless DRE voting machines, parallel testing is probably the best way to detect most software-based attacks, as well as subtle software bugs that may not be discovered during inspection and other testing. For DREs with voter-verifiable paper trails and ballot-marking devices, parallel testing provides the opportunity to discover a specific kind of attack (for instance, printing the wrong choice on the voter-verified paper record) that may not be detected by simply reviewing the paper record after the election is over. However, even under the best of circumstances, parallel testing is an imperfect security measure. The testing creates an "arms-race" between the testers and the attacker, but the race is one in which the testers can never be certain that they have prevailed.

While a few local jurisdictions have taken it upon themselves to conduct limited parallel testing, we know of only four states, California, Georgia, Maryland and

[9] Laws providing for inexpensive candidate-initiated recounts might also add security for voter-verified paper trails. The Brennan Center Security Report did not examine such recounts as a potential countermeasure.

Washington, that have regularly performed parallel testing on a statewide basis. It is worth noting that California and Washington employ automatic routine audits *and* parallel testing as statewide countermeasures against potential attack.

Recommendation # 3: Ban Wireless Components on All Voting Machines.

Our analysis shows that machines with wireless components are particularly vulnerable to attack. We conclude that this vulnerability applies to all three types of electronic voting systems. Only two states, New York and Minnesota, ban wireless components on all machines.[10] California also bans wireless components, but only for DRE machines. Wireless components should not be permitted on any voting machine.

Recommendation # 4: Mandate Transparent and Random Selection Procedures.

The development of transparently random selection procedures for all auditing procedures is key to audit effectiveness. This includes the selection of machines to be parallel tested or audited, as well as the assignment of auditors themselves. The use of a transparent and random selection process allows the public to know that the auditing method was fair and substantially likely to catch fraud or mistakes in the vote totals. In our interviews with election officials we found that, all too often, the process for picking machines and auditors was neither transparent nor random.

In a transparent random selection process:

- The whole process is publicly observable or videotaped.
- The random selection is to be publicly verifiable, *i.e.*, anyone observing is able to verify that the sample was chosen randomly (or at least that the number selected is not under the control of any small number of people).
- The process is simple and practical within the context of current election practice so as to avoid imposing unnecessary burden on election officials.

Recommendation # 5: Ensure Local Control of Programming.

Where a single entity, such as a vendor or state or national consultant, runs elections or performs key tasks (such as producing ballot definition files) for multiple jurisdictions, attacks against statewide elections become easier. Unnecessary centralized control provides many opportunities to implement attacks at multiple locations.

[10] Two other states, West Virginia and Maine, ban networking of machines without banning wireless components themselves. Banning the *use* of wireless components (even when that involves disabling them), rather than requiring *removal* of these components, still leaves voting systems unnecessarily insecure.

Recommendation # 6: Implement Effective Procedures for Addressing Evidence of Fraud or Error.

Both automatic routine audits and parallel testing are of questionable security value without effective procedures for action where evidence of machine malfunction and/or fraud is uncovered. Detection of fraud without an appropriate response will not prevent attacks from succeeding. In the Brennan Center's extensive review of state election laws and practices, and in its interviews with election officials for the threat analysis, we did not find any jurisdiction with publicly-detailed, adequate, and practical procedures for dealing with evidence of fraud or error discovered during an audit, recount or parallel testing.

In addition, the security of our voting systems would be enhanced by mandating good ballot chain of custody practices to ensure that ballots are neither tampered with nor lost, and by ending the exclusive private control that many vendors have over the code on voting machines owned by local jurisdictions and enabling those jurisdictions to access the firmware and software on their own voting machines.

III. DEVELOPMENTS SINCE THE RELEASE OF THE REPORT

Since the Brennan Center's Security Report was released seven months ago, several jurisdictions have made significant improvements. In particular, Arizona, Utah and Wisconsin announced that they would audit their voter-verified paper records in November 2006. We are gratified that several counties have explicitly used the report to craft their security procedures.

On December 1, 2006, scientists at the National Institute of Standards and Technology issued two draft white papers.[11] Specifically, the papers called upon the Technical Guidelines Development Committee of the Election Assistance Commission (the "EAC") to add two new requirements to the 2007 Voluntary Voting System Guidelines: (1) to ban or severely restrict the use of wireless components on all voting systems, and (2) to require that all voting systems provide evidence of voter intent that is *independent* of the voting system and that will allow for an *independent* audit of the vote totals provided by the voting system (*e.g.*, voting systems that include a voter-verified paper record). We note that these reports reinforce the conclusions and many of the recommendations of the Brennan Center Task Force. We believe there is a critical mass – nearing a consensus – of expert opinion on the risks of these electronic systems, and the reforms that can vastly improve them.

Despite this growing awareness of the problem, in the communities where elections are administered, little has changed. The vast majority of counties and states in

[11] *See Requiring Software Independence in VVSG 2006: STS Recommendations for the TGDC* and *Wireless Issues and STS Recommendations for the TGDC*, available at http://vote.nist.gov/DraftWhitePaperOnSIinVVSG2007-20061120.pdf and http://vote.nist.gov/DraftWhitePaperOnWirelessInVVSG2007-20061120.pdf respectively.

the United States still have not implemented any of the key recommendations detailed in the Brennan Center Security Report, leaving us vulnerable to serious security and reliability problems on Election Day.

Moreover, to our knowledge, the EAC has not yet engaged in a comprehensive threat analysis. It is dismaying that a private task force has conducted such a threat assessment while the government agency charged with improving the nation's voting systems has not. If we want the public to feel confident that the guidelines actually make voting systems more secure, the EAC must identify the most serious security and reliability threats and state how each voting system guideline it authors addresses them.

Ultimately, Congress must consider the question of resources. The scope and speed with which the nation has transformed the way it votes and counts votes is unprecedented. It would be unreasonable to believe that such a transformation could be possible without adequate funding. The funding thus far has proven insufficient. Under HAVA, approximately $3.9 billion was authorized for the states to help them purchase and adopt new voting systems and to create new electronic statewide voter registration databases. Even this amount was not fully distributed. Complex voting security systems, in thousands of jurisdictions, involving tens of thousands of lay people, cannot be properly created in short order without a substantial new infusion of funds.

I am often asked by citizens, "I go to my ATM every day. Not once has it given me the wrong amount. And certainly it's never given me too much money!" The fact is that banks spend considerably more in a year to maintain their ATM systems than our nation has spent over six years to entirely modernize its voting technology.[12] In this instance, we got what we paid for. What is the appropriate amount for new funding? Representative Holt in his recent bill envisions a $300 million funding stream. Although we have not studied what would in fact be necessary, this amount seems to be the bare minimum required to make the necessary improvements.

IV. ELECTRONIC VOTING AND ACCURACY

Many voters and public officials understandably are concerned about the accuracy of the new electronic voting systems. For example, these concerns led Florida Governor Charlie Crist to support a move to optical scan machines.

We must make certain that the electronic systems are as accurate as possible. In many instances, accuracy problems may be less due to the design of the hardware (*e.g.*, the touch screen) than the design of the software (*e.g.*, the way voting choices are laid out on the screen). The Brennan Center examined these issues, as well. We found that there are sharp variations among the systems. The best implemented electronic voting systems are more accurate than earlier voting systems.

[12] According to the American Bankers Association, a conservative estimate for the annual maintenance of the country's ATMs is more than $4.5 billion. Source: http://www.aba.com/NR/rdonlyres/80468433-4225-11D4-AAE6-00508B95258D/41737/2ATMFacts1.pdf.

- Precinct Count Optical Scan (PCOS) and Scrolling Direct Recording Electronic (DRE) voting systems are more accurate at recording voter intention than older voting systems. In 2004, residual vote rates were less than 1% for both technologies.

- Full-Face DRE systems (*i.e.*, systems where all candidates for all offices must be visible at all times) continue to be plagued with an unacceptably high residual vote rate. In 2000, 2002 and 2004, it exceeded that of either PCOS or scrolling DRE systems.

It bears repeating: we must not romanticize earlier voting systems. Paper ballots, punch cards, and lever machines all are prone to grave accuracy problems. These problems range from "hanging chads" to miscounted ballots to lost ballots. Properly functioning electronic voting systems can be far more accurate than earlier systems.

V. ENSURING THAT VOTING SYSTEMS ARE ACCESSIBLE AND USABLE

In addition to our Security Report, the Brennan Center has also released reports on voting system usability and accessibility.[13] As with the Security Report, these reports drew on the experience and input of the nation's leading voting system experts. They provide policy makers with practical and important recommendations to help ensure that voting systems are as usable and accessible as possible.

The voting machines recently purchased by most jurisdictions in the United States offer the promise of much greater usability and accessibility than we have known in the past. We have eliminated many usability problems (think for instance, of the notorious "butterfly ballot" in Palm Beach County, Florida), and offered millions of disabled voters the opportunity to vote independently for the first time in their lives.

This does not mean that our voting systems are as usable or accessible as they should be. All too often, vendors have offered technological "fixes" that theoretically make voting easier, but, in fact, make casting a ballot far more difficult for most voters.

As Congress considers ways to ensure that our voting systems are secure and reliable, we urge you to remember that the systems must also remain usable and accessible. Usability and accessibility need not be sacrificed in the name of security or reliability.

In particular, we urge Congress to require the Election Assistance Commission to study, develop and test best practices to increase voting system usability and accessibility. As we note in our usability and accessibility reports, for voting systems to

[13] Lawrence Norden *et al.*, THE MACHINERY OF DEMOCRACY: VOTING SYSTEM SECURITY, ACCESSIBILITY, USABILITY AND COST (Brennan Center for Justice ed., 2006), *available at* http://www.brennancenter.org/stack_detail.asp?key=97&subkey=38150&proj_key=76

become truly usable and accessible to all voters, members of both the general and disabled populations should be included in empirical research of these systems.

We also urge Congress to mandate usability testing of all voting systems and ballot designs used in federal elections. And to guard against disenfranchisement from inevitable breakdowns of new voting systems, Congress should require all states to make available emergency ballots in all polling places using electronic voting systems.

VI. CONCLUSION

The Brennan Center Task Force found that the voting systems most commonly purchased today are vulnerable to attacks and errors that could change the outcome of statewide elections. This finding should surprise no one. A review of the history of both election fraud and voting systems literature in the United States shows that voting systems have always been vulnerable to attack. People have tried to "stuff the ballot box" since senators wore togas. Indeed, it is impossible to imagine a voting system that could be entirely, infallibly impervious to attack.

But straightforward countermeasures can substantially reduce the most serious security risks presented by the three systems. Jurisdictions with the political will can protect their voting systems from attack. The measures identified here – auditing voter-verified paper records, banning wireless components, using transparent and random selection processes for auditing, adopting effective policies for addressing evidence of fraud or error in vote totals, and conducting parallel testing – are achievable with effort.[14] However it must be stressed that all these require human coordination. Our system of elections, run in 13,000 separate jurisdictions largely by part-time or volunteer officials, introduces numerous entry points for error, confusion and mischief. Fixing our electronic voting systems requires more than a technical fix. It requires a serious national commitment to election administration.

Do all the problems mean the United States should abandon electronic voting and return to paper ballots or other systems? We do not believe so. Paper is not a panacea. The other, earlier voting systems were rife with problems of their own, as we all recall. Done right, electronic voting could be a true improvement in the way we elect our leaders. Done wrong, electronic voting can create new opportunities for fraud, lost votes and inaccurate counts – all while diminishing confidence. So far, sad to say, America has not done this transition well. If Congress acts, we can move measurably closer to the ideal of every vote counting. The Brennan Center urges members of Congress to adopt these recommended measures as soon as possible.

---

[14] Even routine parallel testing and audits of voter verified paper records – perhaps the most costly and time consuming countermeasures reviewed in the joint threat analysis – have been shown to be quite inexpensive. Jocelyn Whitney, Project Manager for parallel testing activities in the State of California, provided the Brennan Center with data showing that the total cost of parallel testing in California was approximately *12 cents per vote* cast on DREs. E-mail from Jocelyn Whitney (February 25, 2006) (on file with the Brennan Center). Harvard L. Lomax, Registrar of Voters for Clark County, Nevada, estimates that a Task Force of auditors can review 60 votes on a voter-verified paper trail in four hours. Assuming that auditors are paid $12 per hour and that each Task Force has two auditors, the cost of such audits should be little more than *3 cents per vote*, if 2% of all votes are audited. Telephone Interview with Harvard L. Lomax (March 23, 2006). Each of these costs represents a tiny fraction of what jurisdictions already spend annually on elections. The Brennan Center's study of voting system costs shows that, for instance, most jurisdictions spend far more than this on printing ballots (as much as $0.92 per ballot), programming machines (frequently more than $0.30 per vote, per election), or storing and transporting voting systems. Lawrence Norden *et al.*, THE MACHINERY OF DEMOCRACY: VOTING SYSTEM SECURITY, ACCESSIBILITY, USABILITY AND COST (Brennan Center for Justice ed., 2006).

APPENDIX A: ABOUT THE TASK FORCE

In 2005, the Brennan Center convened a Task Force of internationally renowned government, academic, and private-sector scientists, voting machine experts and security professionals to conduct the nation's first systematic analysis of security vulnerabilities in the three most commonly purchased electronic voting systems. The Task Force spent more than a year conducting its analysis and drafting this report. During this time, the methodology, analysis, and text were extensively peer reviewed by the National Institute of Standards and Technology ("NIST").

The members of the Task Force are:

Chair
Lawrence D. Norden, Brennan Center for Justice

Principal Investigator
Eric L. Lazarus, DecisionSmith.

Experts
Georgette Asherman, independent statistical consultant, founder of Direct Effects

Professor Matt Bishop, University of California at Davis

Lillie Coney, Electronic Privacy Information Center

Professor David Dill, Stanford University

Jeremy Epstein, PhD, Cyber Defense Agency LLC

Harri Hursti, independent consultant, former CEO of F-Secure PLC

Dr. David Jefferson, Lawrence Livermore National Laboratory and Chair of the California Secretary of State's Voting Systems Technology Assessment and Advisory Board

Professor Douglas W. Jones, University of Iowa

John Kelsey, PhD, NIST

Rene Peralta, PhD, NIST

Professor Ronald Rivest, MIT

Howard A. Schmidt, Former Chief Security Officer, Microsoft and eBay

Dr. Bruce Schneier, Counterpane Internet Security

Joshua Tauber, PhD, formerly of the Computer Science and Artificial Intelligence Laboratory at MIT

Professor David Wagner, University of California at Berkeley

Professor Dan Wallach, Rice University

Matthew Zimmerman, Electronic Frontier Foundation

APPENDIX B: METHODOLOGY

In developing the study of voting system security vulnerabilities, the Brennan Center brought together some of the nation's leading election officials, as well as a Task Force of internationally recognized experts in the fields of computer science, election policy, security, voting systems, and statistics. After considering several approaches to measuring the strength of election security, this group unanimously selected a model that: (a) identified and categorized the potential threats against voting systems, (b) prioritized these threats based upon an agreed-upon metric (which would identify how "difficult" each threat is to accomplish from the attacker's point of view), and (c) determined (utilizing the same metric employed to prioritize threats) how much more difficult each of the catalogued attacks would become after various sets of countermeasures were implemented.

After several months of work, including a public threat analysis workshop hosted by the National Institute of Standards and Technology, the Task Force identified and categorized more than 120 threats to the three voting systems. The threats generally fell into one or more of nine broad categories: (1) the insertion of corrupt software into machines prior to Election Day; (2) wireless and other remote attacks on voting machines on Election Day; (3) attacks on tally servers; (4) mis-calibration of voting machines; (5) shut-off of voting machine features intended to assist voters; (6) denial-of-service attacks; (7) actions by corrupt poll workers or others at the polling place to affect votes cast; (8) vote buying schemes; and (9) attacks on ballots or voter-verified paper trails.

The Task Force determined that the best single metric for determining the "difficulty" of each of these attacks was the number of informed participants necessary to execute the attack successfully. An "informed participant" is someone whose participation is needed to make the attack work, and who knows enough about the attack to foil or expose it.

For each attack, Task Force members looked at how many informed participants would be necessary to change the outcome of a reasonably close statewide election in which all votes were cast on one of the three voting systems analyzed. The statewide election we looked at was a fictional gubernatorial race between Tom Jefferson and Johnny Adams in a composite jurisdiction, Pennasota. Pennasota was created by aggregating the results of the 2004 presidential election in 10 "battleground" states, as determined by Zogby International polls in the spring, summer, and fall of 2004.

Election for Governor / State of Pennasota 2007

Candidate	Party	Total Votes	Percentage of Votes
Tom Jefferson	Dem.-Rep.	1,769,818	51.1
Johnny Adams	Federalists	1,689,650	48.8

To figure out how many informed participants would be needed to change the outcome of this election and make Johnny Adams the next Governor of Pennasota, the experts broke down each attack into its necessary parts, assigned a value representing the minimum number of persons they believed would be necessary to accomplish each part, and then determined how many times the attack would need to be repeated to reverse the election results.

At the conclusion of this process, election officials were interviewed to determine whether they agreed with the assigned steps and values. When necessary, the steps and values were modified to reflect feedback from the officials.

After the attacks were prioritized by level of difficulty, Task Force members reviewed how much more difficult each attack would become if various sets of countermeasures were implemented. The process for determining the difficulty of overcoming countermeasures was exactly the same as the process for determining attack difficulty: each step necessary to overcome the countermeasure was identified and given a value equal to the number of persons necessary to accomplish that step. Election officials were again consulted to confirm that the steps and values assigned were reasonable.

To ensure that the results of our analysis were robust and not limited to the composite jurisdiction of Pennasota, we ran our threat analysis against the actual results of the 2004 presidential election in Florida, New Mexico, and Pennsylvania. All of the results and findings discussed in this summary applied to our analyses of these three states.