THE MACHINERY OF DEMOCRACY: PROTECTING ELECTIONS IN AN ELECTRONIC WORLD

EXECUTIVE SUMMARY

BRENNAN CENTER TASK FORCE
ON VOTING SYSTEM SECURITY,
LAWRENCE NORDEN, CHAIR

VOTING RIGHTS
& ELECTIONS SERIES

BRENNAN CENTER
FOR JUSTICE
AT NYU SCHOOL OF LAW

THE MACHINERY OF DEMOCRACY: PROTECTING ELECTIONS IN AN ELECTRONIC WORLD

EXECUTIVE SUMMARY

THE BRENNAN CENTER TASK FORCE

ON VOTING SYSTEM SECURITY

LAWRENCE NORDEN, CHAIR

VOTING RIGHTS

& ELECTIONS SERIES

BRENNAN CENTER

FOR JUSTICE

AT NYU SCHOOL OF LAW

www.brennancenter.org

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.

Government Experts

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

John Kelsey, PhD, NIST

Rene Peralta, PhD, NIST

Professor Ronald Rivest (MIT), Technical Guidelines Committee, Election Assistance Commission

Academic Experts

Professor Matt Bishop, University of California at Davis

Professor David Dill, Stanford University

Professor Douglas W. Jones, University of Iowa

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

Private Sector Experts (Commercial and Non-Profit)

Georgette Asherman, independent statistical consultant, founder of Direct Effects

Lillie Coney, Electronic Privacy Information Center

Jeremy Epstein, Cyber Defense Agency LLC

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

Howard A. Schmidt, Former White House Cyber Security Advisor for George W. Bush; Former Chief Security Officer, Microsoft

Dr. Bruce Schneier, Counterpane Internet Security

Matthew Zimmerman, Electronic Frontier Foundation

ABOUT THE EDITOR AND TASK FORCE CHAIR

Lawrence Norden is an Associate Counsel with the Brennan Center, working in the areas of voting technology, voting rights, and government accountability. For the past year, Mr. Norden has led the Brennan Center's voting technology assessment project. He is the lead author of *The Machinery of Democracy: Voting System Security, Accessibility, Usability, Cost* (Brennan Center forthcoming 2006) and a contributor to Routledge's forthcoming *Encyclopedia of American Civil Liberties.* Mr. Norden is a graduate of the University of Chicago and the NYU School of Law. Mr. Norden serves as an adjunct faculty member in the Lawyering Program at the Benjamin N. Cardozo School of Law. He may be reached at lawrence.norden@nyu.edu

ABOUT THE BRENNAN CENTER

The Brennan Center for Justice at NYU School of Law unites thinkers and advocates in pursuit of a vision of inclusive and effective democracy. The organization's mission is to develop and implement an innovative, nonpartisan agenda of scholarship, public education, and legal action that promotes equality and human dignity, while safeguarding fundamental freedoms. The Center works in the areas of Democracy, Poverty, Criminal Justice, and Liberty and National Security. Michael Waldman is the Center's Executive Director.

ABOUT THE VOTING RIGHTS & ELECTIONS SERIES

The Brennan Center's Voting Rights & Elections Project promotes policies that protect rights to equal electoral access and political participation. The Project seeks to make it as simple and burden-free as possible for every eligible American to exercise the right to vote and to ensure that the vote of every qualified voter is recorded and counted accurately. In keeping with the Center's mission, the Project offers public education resources for advocates, state and federal public officials, scholars, and journalists who are concerned about fair and open elections. For more information, please see www.brennancenter.org or call 212-998-6730.

This paper is the second in a series, which also includes:

Making the List: Database Matching and Verification Processes for Voter Registration by Justin Levitt, Wendy Weiser and Ana Munoz.

Other resources on voting rights and elections, available on the Brennan Center's website, include:

Response to the Report of the 2005 Commission on Federal Election Reform (2005) (co-authored with Professor Spencer Overton)

Recommendations for Improving Reliability of Direct Recording Electronic Voting Systems (2004) (co-authored with Leadership Conference on Civil Rights)

ACKNOWLEDGMENTS

Most importantly, the Brennan Center thanks NIST and its many scientists for devoting so many hours to its extensive and thorough peer review of the analysis and report. The report, in its current form, would not exist without NIST's many important comments and contributions.

In particular, we thank John Kelsey of NIST for the substantial material and ideas he provided, which have been incorporated into the report and the report's attack catalogs. We also specially thank Rene Peralta for his original contributions and analysis. Finally, we are enormously grateful to Barbara Guttman, John Wack and other scientists at NIST, who provided material for the attack catalogs, helped to develop the structure of the report, and edited many drafts.

We are also extremely appreciative of Principal Investigator Eric Lazarus's enormous efforts on behalf of this report. His vision, tenacity, and infectious enthusiasm carried the team through a lengthy process of analysis and drafting.

A special debt of gratitude is also owed to election officials throughout the country, who spent many hours responding to surveys and interview questions related to this report. In addition to team members Professor Ronald Rivest and Dr. David Jefferson, we particularly thank Patrick Gill, Woodbury County Auditor and Recorder and Past President of the Iowa State Association of County Auditors; Elaine Johnston, County Auditor, Asotin County, Washington; Harvard L. Lomax, Registrar of Voters for Clark County, Nevada; Debbie Smith, Elections Coordinator, Caleveras County, California; Jocelyn Whitney, Developer and Project Manager for parallel testing activities in the State of California; Robert Williams, Chief Information Officer for Monmouth County, New Jersey; and Pam Woodside, former Chief Information Officer for the Maryland State Board of Elections. We would also like to acknowledge the National Committee for Voting Integrity for their cooperation and assistance in this effort.

Jeremy Creelan, Associate Attorney at Jenner & Block LLP, deserves credit for conceiving, launching. and supervising the Brennan Center's voting technology assessment project, including development of this report, as Deputy Director of the Center's Democracy Program through February 2005. The Program misses him greatly and wishes him well in private practice, where he continues to provide invaluable *pro bono* assistance.

The Brennan Center is grateful to Task Force member Lillie Coney, Associate Director of the Electronic Privacy Information Center. Among many other contributions, she provided invaluable assistance in assembling the Task Force, and frequently offered the Brennan Center sage strategic advice.

This report also benefited greatly from the insightful and thorough editorial assistance of Deborah Goldberg, Director of the Brennan Center's Democracy

Program. We are extremely grateful to Professor Henry Brady of the University of California at Berkeley and Professor Benjamin Highton of the University of California at Davis for their insights into the possible effects of denial of service attacks on voting systems. The Brennan Center also thanks Bonnie Blader, independent consultant, who provided the Task Force with crucial research, David M. Siegel, independent technology consultant, for his original contributions on the subject of software code inspections, and Tracey Lall, Ph.D. candidate in Computer Science at Rutgers University, who contributed many hours of critical security analysis. Douglas E. Dormer, CPA, CTP provided invaluable assistance in developing the analysis methodology and in keeping the task force focused. Joseph Lorenzo Hall also must be thanked for helping the Task Force members understand the diversity and commonality in voting system architectures. Much of the legal research was conducted by Gloria Garcia and Juan Martinez, J.D. candidates at Benjamin N. Cardozo School of Law, and Annie Lai and S. Michael Oliver, J.D. candidates at NYU School of Law. Lowell Bruce McCulley, CSSP, was exceptionally helpful in creating the attack catalogs. Finally, we thank Brennan Center Research Associates Annie Chen, Lauren Jones, Ana Munoz, and Neema Trivedi for their many hours of dedicated assistance.

Generous grants from an anonymous donor, the Carnegie Corporation of New York, the Ford Foundation, the HKH Foundation, the Knight Foundation, the Open Society Institute, and the Rockefeller Family Foundation supported the development and publication of this report. The statements made and views expressed in this report are the responsibility solely of the Brennan Center.

CONTENTS

TEXT

FIGURES

INTRODUCTION

In these pages, the Brennan Center for Justice at NYU School of Law (the "Brennan Center") summarizes the nation's first systematic analysis of security vulnerabilities in the three most commonly purchased electronic voting systems. To develop the analysis, the Brennan Center convened a Task Force of internationally renowned government, academic, and private-sector scientists, voting machine experts, and security professionals.

The Task Force examined security threats to the *technologies* used in Direct Recording Electronic voting systems ("DREs"), DREs with a voter verified auditable paper trail ("DREs w/ VVPT") and Precinct Count Optical Scan ("PCOS") systems. The analysis assumes that appropriate physical security and accounting procedures are in place.

FIGURE 1

VOTING SYSTEMS

Type of Voting System	Description of Voting System	Examples of Voting System
Direct Recording Electronic (DRE)	A DRE machine directly records the voter's selections in each contest, using a ballot that appears on a display screen. Typical DRE machines have flat panel display screens with touch-screen input, although other display technologies have been used. The defining characteristic of these machines is that votes are captured and stored electronically.	Microvote Infinity Voting Panel Hart InterCivic eSlate Sequoia AVC Edge Sequoia AVC Advantage ES&S iVotronic ES&S iVotronic LS Diebold AccuVote-TS Diebold AccuVote-TSX Unilect Patriot
DRE with Voter Verified Paper Trail (DRE w/ VVPT)	A DRE w/ VVPT captures a voter's choice both internally in electronic form, and contemporaneously on paper. A DRE w/ VVPT allows the voter to confirm the accuracy of the paper record to provide voter-verification.	ES&S iVotronic system with Real Time Audit Log Diebold AccuVote-TSX with AccuView printer Sequoia AVC Edge with VeriVote printer Hart InterCivic eSlate with VVPAT Unilect Patriot with VVPAT
Precinct Count Optical Scan (PCOS)	PCOS voting machines allows voters to mark paper ballots, typically with pencils or pens, independent of any machine. Voters then carry their sleeved ballots to a scanner. At the scanner, they un-sleeve the ballot and insert into the scanner, which optically records the vote.	Diebold AccuVote-OS ES&S Model 100 Sequoia Optech Insight

The full report (the "Security Report"), which has been extensively peer reviewed by the National Institute of Standards and Technology ("NIST"), may be found at www.brennancenter.org. Following the analysis outlined here, the Brennan Center and Task Force members recommend countermeasures that should be taken to reduce the technological vulnerability of each voting system.[1]

CORE FINDINGS

Three fundamental points emerge from the threat analysis in the Security Report:

- All three voting systems have significant security and reliability vulnerabilities, which pose a real danger to the integrity of national, state, and local elections.
- The most troubling vulnerabilities of each system can be substantially remedied if proper countermeasures are implemented at the state and local level.
- Few jurisdictions have implemented any of the key countermeasures that could make the least difficult attacks against voting systems much more difficult to execute successfully.

VOTING SYSTEM VULNERABILITIES

After a review of more than 120 potential threats to voting systems, the Task Force reached the following crucial conclusions:

For *all three* types of voting systems:

- When the goal is to change the outcome of a close statewide election, attacks that involve the insertion of software attack programs or other corrupt software are the least difficult attacks.
- Voting machines that have wireless components are significantly more vulnerable to a wide array of attacks. Currently, only two states, New York and Minnesota, ban wireless components on all voting machines.

For DREs *without* voter verified paper trails:

- DREs without voter verified paper trails do not have available to them a powerful countermeasure to software attacks: post-election automatic routine audits that compare paper records to electronic records.

For DREs w/ VVPT and PCOS:

- The voter verified paper record, *by itself,* is of questionable security value. The paper record has significant value only if an automatic routine audit is performed (and well designed chain of custody and physical security procedures are followed). Of the 26 states that mandate voter verified paper records, only 12 require regular audits.

- Even if jurisdictions routinely conduct audits of voter verified paper records, DREs w/ VVPT and PCOS are vulnerable to certain software attacks or errors. Jurisdictions that conduct audits of paper records should be aware of these potential problems.

SECURITY RECOMMENDATIONS

There are a number of steps that jurisdictions can take to address the vulnerabilities identified in the Security Report and make their voting systems significantly more secure. We recommend adoption of the following security measures:

1. Conduct automatic routine audits comparing voter verified paper records to the electronic record following every election. A voter verified paper record accompanied by a solid automatic routine audit of those records can go a long way toward making the least difficult attacks much more difficult.

2. Perform "parallel testing" (selection of voting machines at random and testing them as realistically as possible on Election Day.) For paperless DREs, in particular, parallel testing will help jurisdictions detect software-based attacks, as well as subtle software bugs that may not be discovered during inspection and other testing.

3. Ban use of voting machines with wireless components. All three voting systems are more vulnerable to attack if they have wireless components.

4. Use a transparent and random selection process for all auditing procedures. For any auditing to be effective (and to ensure that the public is confident in such procedures), jurisdictions must develop and implement transparent and random selection procedures.

5. Ensure decentralized programming and voting system administration. Where a single entity, such as a vendor or state or national consultant, performs key tasks for multiple jurisdictions, attacks against statewide elections become easier.

6. Institute clear and 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 discovered. Detection of fraud without an appropriate response will not prevent attacks from succeeding.

Fortunately, these steps are not particularly complicated or cumbersome. For the most part, they do not involve significant changes in system architecture. Unfortunately, *few jurisdictions have implemented any of these security recommendations.*

Good threat analyses allow us to identify and implement the best security precautions.

VOTING SYSTEM VULNERABILITIES

WHAT IS A THREAT ANALYSIS AND WHY IS IT NECESSARY?

In the last several years, few issues in the world of voting systems have garnered as much public attention as voting system security. This attention to voting system security has the potential to be a positive force. Unfortunately, too much of the public discussion surrounding security has been marred by claims and counter-claims that are based on little more than speculation or anecdote.

In response to this uninformed discussion, and with the intention of assisting election officials and the public as they make decisions about their voting machines, the Task Force undertook a methodical analysis of potential threats to voting systems. The threat analysis provides election officials and concerned citizens with *quantifiable* criteria for measuring the level of security offered by voting systems and potential safety measures. It should assist jurisdictions in deciding (a) which voting systems to certify or purchase, and (b) how to protect those systems from security threats after they have been purchased. The Security Report sets forth the detailed results of that analysis, which are summarized here.

SYSTEMATIC THREAT ANALYSES OF VOTING SYSTEMS ARE LONG OVERDUE.

Most Americans would agree that the integrity of our elections is fundamental to our democracy. We want citizens to have full confidence that their votes will be accurately recorded. Given the current tenor of debate over voting system security, this is reason enough to conduct regular systematic threat analyses of voting systems.

Just as importantly, such analyses, if utilized in developing voting system standards and procedures, should reduce the risk of attacks on voting systems. As a nation, we have not always successfully avoided such attacks – in fact, various types of attacks on voting systems and elections have a "long tradition" in American history.[2] The suspicion or discovery of such attacks has generally provoked momentary outrage, followed by periods of historical amnesia.[3]

All technology, no matter how advanced, is going to be vulnerable to attack to some degree. The history of attacks on voting systems teaches us how foolish it would be to assume that there will not be attacks on voting systems in the future. But we can educate ourselves about the vulnerabilities and take the proper precautions to ensure that the easiest attacks, with the potential to affect the most votes, are made as difficult as possible. Good threat analyses allow us to identify and implement the best security precautions.

SOLID THREAT ANALYSES SHOULD HELP MAKE SYSTEMS MORE RELIABLE.

There is an additional benefit to this kind of analysis: it should help make our voting systems more reliable, *regardless of whether they are ever attacked.* Computerized voting systems – like all previous voting systems – have shown themselves vulnerable to error. As detailed in the Security Report, votes have been miscounted or lost as a result of defective firmware (coded instructions in a computer system's hardware), faulty machine software, defective tally server software, election programming errors, machine breakdowns, malfunctioning input devices, and pollworker error.

Almost everything that a malicious attacker could attempt could also happen by accident.

"An old maxim in the area of computer security is clearly applicable here: Almost everything that a malicious attacker could attempt could also happen by accident; for every malicious attacker, there may be thousands of people making ordinary careless errors."[4] Solid threat analyses should help to expose and to address vulnerabilities in voting systems, including not only security breaches but also simple malfunctions.

WHAT METHODOLOGY WAS USED FOR THE THREAT ANALYSIS?

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) miscalibration 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 "dif-

ficulty" 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.

FIGURE 2

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.

The full work of the Task Force, including the choice of methodology, analysis and report, were extensively peer reviewed by NIST.

Significantly, the threat analysis suggests that all three voting systems are equally vulnerable to software attacks.

WHAT WERE THE GREATEST RISKS REVEALED BY THE THREAT ANALYSIS?

Below is a discussion of the most troubling threats identified in the Security Report.

THE LEAST DIFFICULT ATTACKS USE SOFTWARE ATTACK PROGRAMS.

The "least difficult" attacks against all three systems (as measured by the metric of number of informed participants necessary to change the outcome of a statewide election) involve the insertion of corrupt software or other software attack programs in order to take over a voting machine. Significantly, the threat analysis suggests that all three voting systems are equally vulnerable to software attacks.

The most basic type of software attack program would target voting machines and switch a certain number of votes from one candidate to another. This alteration of votes could occur at any time on Election Day, as long as it was completed before poll workers printed a paper record of the vote total and extracted the electronic record of votes from the machines.

Inserting a software attack program into a voting system for the purpose of affecting an election's outcome is likely to be technically and financially challenging, particularly if the attacker wants to avoid detection. However, a substantial historical record of this type of attack against non-voting systems suggests that it can be successfully executed. The Security Report details several ways that an attacker could insert a software attack program without detection.

Firmware is software that is embedded in the voting machine.

Specifically, there are several points in the development and use of voting machine software where software attack programs could be inserted without detection. Among these points, software attack programs could be inserted through the "firmware" that is hard-wired into voting machines, during the generation of "commercial off-the-shelf" ("COTS") or vendor software used on voting machines, through software patches and updates meant to improve the performance and capabilities of voting machines, during the creation of configuration files and election definitions used to interpret voter choice and totals on voting machines, through network communications between voting machines and outside sources, as well as through "input/output" devices such as memory cards and printers.

There are many hurdles an attacker would have to overcome to ensure that the insertion of such an attack program changed enough votes to affect the outcome

of a statewide election and escaped detection. After careful analysis, the Task Force determined that none of these hurdles is insurmountable. The full Security Report discusses in detail how an attacker could prevail over the following challenges: efforts of vendors to prevent such an attack from occurring (pp. 32–33); gaining sufficient technical knowledge about the way a voting machine and its software works (pp. 36–37); gaining sufficient knowledge about the targeted election (pp. 37–38); creating an attack program that has the ability to change, add, or subtract votes (pp. 39–40); eluding independent testing authority ("ITA") inspections (pp. 42–45); avoiding detection during machine testing (pp. 44–45); and avoiding detection through records kept on event and audit logs (pp. 45–46).

WIRELESS COMPONENTS CREATE UNNECESSARY RISKS.

The threat analysis shows that machines with wireless components are particularly vulnerable to software attack programs and other attacks. The Security Report concludes that this danger applies to all three voting systems examined.

A "Trojan horse" is a type of software attack program that "impersonates" a benign program.

Vendors continue to manufacture and sell machines with wireless components. Among the many types of attacks made possible by wireless components are attacks that exploit an unplanned vulnerability in the software or hardware to get a Trojan horse into the machine. For this type of attack, a Trojan horse would not have to be inserted in advance of Election Day. Instead, an attacker aware of a vulnerability in the voting system's software or firmware could simply show up at the polling station and beam her Trojan horse into the machine using a wireless enabled personal digital assistant.

Personal digital assistants ("PDAs" or palmtops) are handheld devices that were originally designed as personal organizers. PDAs can synchronize data with a personal computer.

Thus, virtually any member of the public with some knowledge of software and a personal digital assistant could perform this attack. This is particularly troubling when one considers that most voting machines run on COTS software and/or operating systems; the vulnerabilities of such software and systems are frequently well known.[5] Against all three systems, attackers could use wireless components to subvert *all* testing. Specifically, an attack program could be written to remain dormant until it received particular commands via a wireless communication. This would allow attackers to wait until a machine was being used to record votes on Election Day before turning on the software attack.

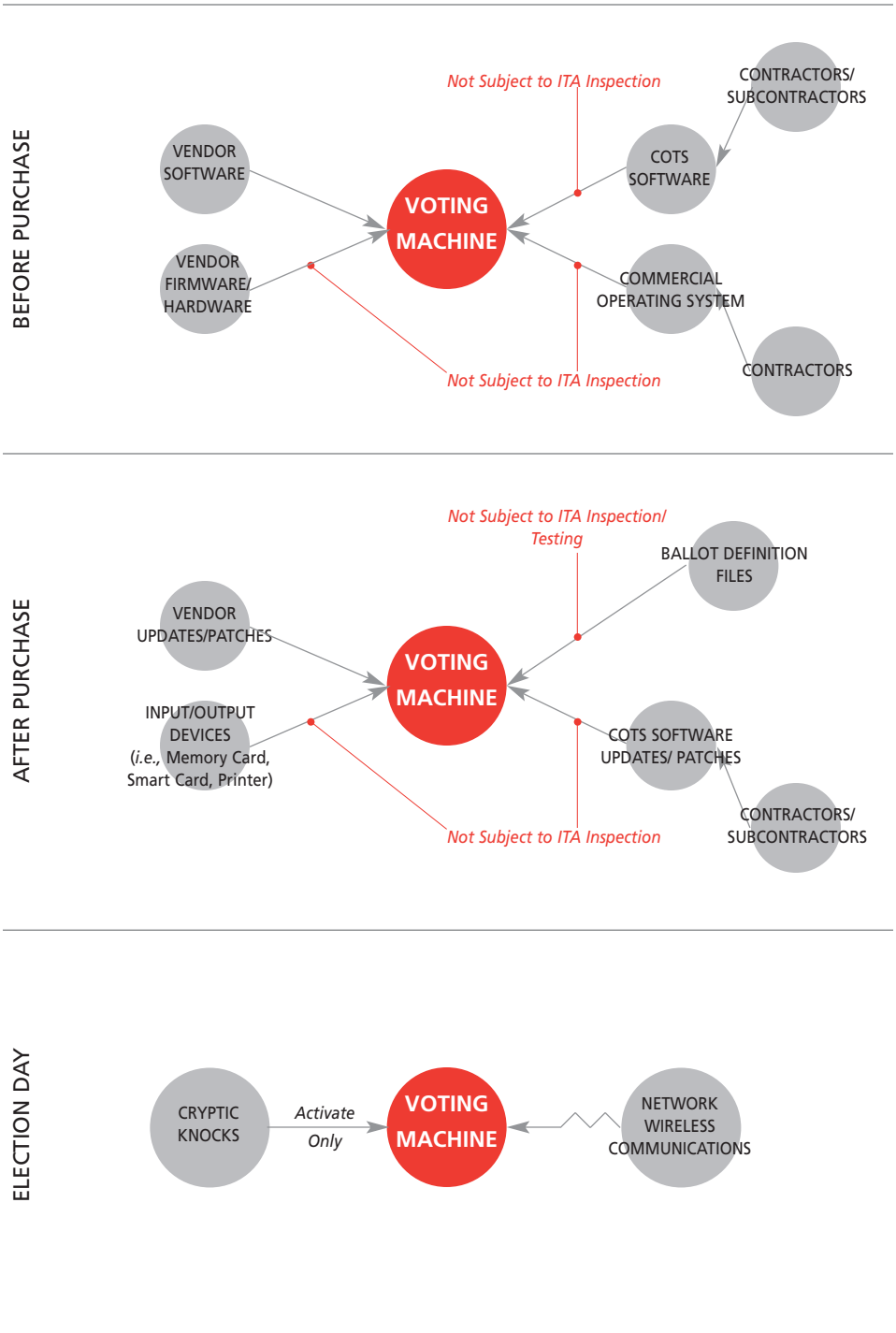
Attackers could also use wireless communications to gain fine-grained control over an attack program already inserted into a particular set of machines (*i.e.*, switch three votes in the second race on the third machine), or obtain information as to how individuals had voted by communicating with a machine while it was being used.

Finally, wireless networking presents additional security vulnerabilities for jurisdictions using DREs w/ VVPT and PCOS. A major logistical problem for an attacker changing both electronic and paper records is how to get the new paper records printed in time to substitute them for the old record in transit. With wire-

less networking, the DRE or PCOS can transmit specific information out to the attacker about what should appear on those printed records. In short, permitting wireless components on DRE w/ VVPT or PCOS machines makes the attacker's job much simpler in practice.

FIGURE 3

SOFTWARE ATTACK PROGRAM: POINTS OF ENTRY



A cryptic knock is an action taken by a user of the machine that will trigger (or silence) the attack behavior. The cryptic knock could come in many forms, depending upon the attack program: voting for a write-in candidate, tapping a specific spot on the machine's screen, a communication via wireless network, etc.

Systems with voter verified paper records provide little, if any, security benefit over systems without such records, unless there are regular audits and/or recounts of the paper records.

SYSTEMS WITH PAPER RECORDS ARE STILL SUBJECT TO ATTACK.

Voting systems with some kind of voter verified paper record (*i.e.*, DRE w/VVPT or PCOS) offer an important security advantage against software attack programs not offered by voting systems without voter verified paper records (*i.e.*, DREs *without* VVPT): jurisdictions can conduct an audit of the voter verified paper record and compare that record to the electronic vote totals.

Unfortunately, most states that require voter verified paper records do not require automatic audits of paper records after each election. *Our analysis shows that systems with voter verified paper records provide little, if any, security benefit over systems without such records, unless there are regular audits and/or recounts of the paper records.*

Even assuming that such regular audits and/or recounts are conducted, jurisdictions that use, or are considering purchasing DREs w/ VVPT or PCOS should be aware of threats that are unique to these systems.

ATTACKS ON DRE W/VVPT

At least one study has suggested that an extremely low percentage of voters who use DREs w/ VVPT review the paper trail.[6]

If those findings are correct, an attacker could subvert a recount or audit by creating an attack program that directs the machine to record the wrong vote on *both* the electronic and paper records. If both records are similarly inaccurate, checking one against the other in an audit or recount will not expose an attack.

In practice, this is how it would work in the Governor's race in Pennasota:

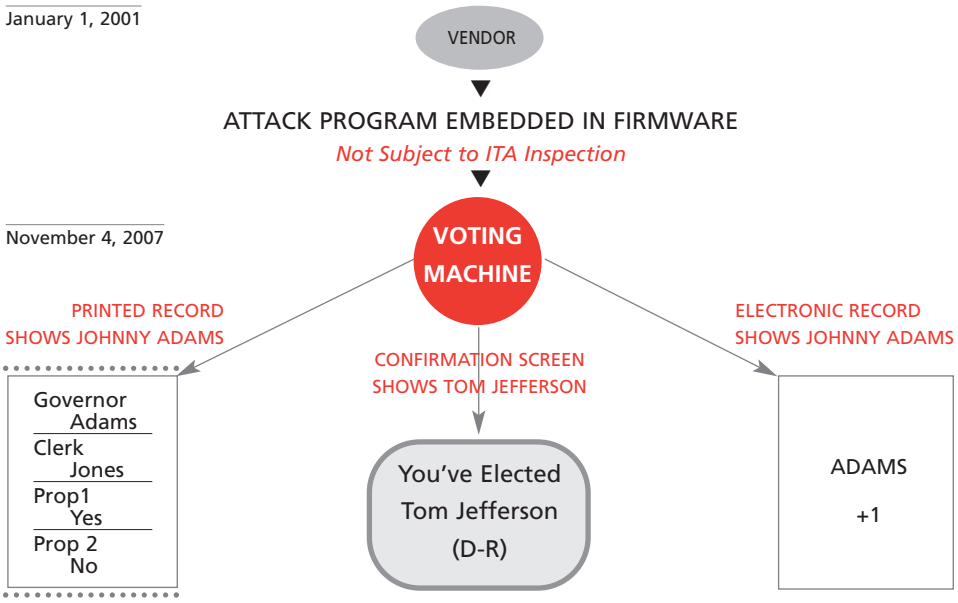
- When a targeted voter chooses Tom Jefferson, the screen would indicate that she has voted for Tom Jefferson.
- After she has completed voting in all other races, the DRE would print a paper record that lists her choices for every race, except for governor. Under the governor's race, it would state that she has selected Johnny Adams.
- When the DRE screen asks the voter to confirm that the paper has recorded her vote correctly, one of two things would happen:
  - the voter would fail to notice that the paper has misrecorded the vote and accept the paper recording; or
  - the voter would reject the paper record and opt to vote again.
- If the voter rejects the paper record, the second time around it would show that she voted for Tom Jefferson. This might lead her to believe she had acci-

dentally pressed the wrong candidate the first time. In any event, it would render her less likely to tell anyone that the machine made a mistake.

We can imagine the attack visually this way:

FIGURE 4

POSSIBLE ATTACK ON DRE WITH VVPT



This attack would not require any additional participants in the conspiracy. Nor, as demonstrated in the Security Report, is it entirely clear that enough voters would notice the misrecorded votes to prevent the attack from working.

The Security Report details countermeasures that should allow jurisdictions to catch this attack. Specifically, even if only a small percentage of voters notice that a machine has misrecorded their vote, there should be an unusually large number of "cancellations" on the paper trail. A jurisdiction that recorded and then reviewed the number of cancellations during a 2% audit would find enough evidence of problems to identify a problem and understand that further investigation was warranted.

Of course, encouraging voters to review the paper records could also substantially reduce the risk of a successful attack on the paper trail.

Encouraging voters to review the paper records could also substantially reduce the risk of a successful attack on the paper trail.

ATTACKS ON PCOS

One of the benefits of PCOS machines over Central Count Optical Scanners (which are very often used in tallying absentee ballots) is that they have an "over/undervote protection." The over/undervote protection on PCOS scan-

ners works as follows: when a voter fills out his ballot, but accidentally fills in two candidates for the same race (overvotes) or accidentally skips a race (undervotes), the scanner would refuse to record the vote and send it back to the voter for examination. The voter then has the opportunity to review the ballot and correct it before resubmitting.

Central Count Optical Scanners have been shown to lose far more votes than PCOS. In precincts with over 30% African American voters, for example, the lost or "residual" vote rate for Central Count Optical Scanners has been shown to be as high as 4.1% as compared with 0.9% for PCOS.[7]

The lack of over/undervote protection on Central Count Optical Scanners may be the reason for this difference.

Our attacker in Pennasota would probably *not* be able to swing the gubernatorial race from Jefferson to Adams merely by inserting an attack program that would turn off the over/undervote protection on PCOS scanners. Even if we assume that the result of turning off the protection were a loss of 4% of the votes on every scanner, and that all of those votes would have gone to Tom Jefferson, this would result in the loss of only about 20,000 votes. This would still leave Jefferson (who won by about 80,000 votes) with a comfortable (though slimmer) margin of victory.

Nevertheless, this attack could cause the loss of thousands of votes. There are at least three possible ways to catch this attack:

- Parallel testing (assuming that the attack program has not also figured out a way to shut off when it is being tested);
- Periodic testing of the over/undervote protection on Election Day;
- Counting over/undervotes during an audit of the voter verified paper record to determine whether there is a disproportionate number of such lost votes.

SECURITY RECOMMENDATIONS

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 parallel testing and automatic routine audits proposed in the Security Report are important tools for defending voting systems from many types of attack, including software attack programs.

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.

Most jurisdictions have not implemented these security measures. Of the 26 states that require a voter verified paper record, only 12 states require automatic audits of those records after every election, and only two of these states – California and Washington – conduct parallel testing.[8]

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 PAPER RECORDS.

Advocates for voter verified paper records have been extremely successful in state legislatures across the country. Currently, 26 states require their voting systems to produce a voter verified record, but 14 of these states do not require automatic routine audits.[9] The Task force has concluded that an independent voter verified paper trail without an automatic routine audit is of questionable security value.[10]

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 measures recommended below should 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 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., the day after polls close.
- The audit should include a tally of spoiled ballots (in the case of VVPT cancellations), overvotes, and undervotes.

- A statistical examination of anomalies, such as higher than expected cancellations or undervotes and overvotes, should be conducted.

- Solid practices with respect to chain of custody and physical security of paper records prior to the automatic routine audit should be followed.

RECOMMENDATION #2:

CONDUCT PARALLEL TESTING.

It is not possible to conduct an audit of paper records of DREs without VVPT, because no voter verified paper record exists on such machines. This means that jurisdictions that use DREs without VVPT do not have access to an important and powerful countermeasure.

Typically, a ballot-marking device is an accessible computer-based voting system that produces a marked ballot. The ballot is marked as the result of voter interaction with visual or audio prompts. Some jurisdictions use ballot-marking devices instead of accessible DREs.

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 w/ VVPT 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.

We have concluded that the following steps will lead to more effective parallel testing:

- The precise techniques used for parallel testing (*e.g.*, exactly how and when the machine is activated, how activation codes/smart cards/*etc.* are produced to allow voting, *etc.*) should not be fully determined or revealed until right before the election. Details of how parallel testing is done should change from election to election.

- At least two of each type of DRE (meaning both vendor and model) should be selected for parallel testing.

- At least two DREs from each of the three largest counties should be parallel tested.

- Localities should be notified as late as possible that machines from their precincts will be selected for parallel testing.

- Wireless channels for voting machines should be closed off, to ensure they cannot receive commands.

- Voting machines should never be connected to one another during voting. Some DREs and DREs w/VVPT may be designed so that they cannot function unless they are connected to one another. Election officials should discuss this question with voting system vendors.

- Voting machines should be completely isolated during the election, and print out or otherwise display their totals before being connected to any central server to send in its tallies.

- Parallel testing scripts should include details, such as how quickly or slowly to vote, when to make "errors," and perhaps even when to cast each vote.

- Parallel testing should be videotaped to ensure that a contradiction between paper and electronic records when parallel testing is complete is not the result of tester error.

While a few local jurisdictions have taken it upon themselves to conduct limited parallel testing, we are aware of only three states, California, Maryland and Washington, that have regularly performed parallel testing on a statewide basis. It is worth noting that two of these states, California and Washington, employ automatic routine audits *and* parallel testing as statewide countermeasures against potential attack.

Machines with wireless components are particularly vulnerable to 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 voting systems. Only two states, New York and Minnesota, ban wireless components on all machines.[11] 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.

Where a single entity, such as a vendor or state or national consultant, runs elections or performs key tasks for multiple jurisdictions, attacks against statewide elections become easier.

In a transparent random selection process:

- The whole process is publicly observable or videotaped.
- The random selection is 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 DECENTRALIZED PROGRAMMING AND VOTING SYSTEM ADMINISTRATION.

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.

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.

The following are examples of procedures that would allow jurisdictions to respond effectively to detection of bugs or software attack programs in parallel testing:

- Impound and conduct a transparent forensic examination of all machines showing unexplained discrepancies during parallel testing.
- Where evidence of a software bug or attack program is subsequently found (or no credible explanation for the discrepancy is discovered), conduct a forensic examination of all DREs used in the state during the election.[12]

- Identify the machines that show evidence of tampering or a software flaw that could have affected the electronic tally of votes.

- Review the reported margin of victory in each potentially affected race. Based upon the (a) margin of victory, (b) number of machines affected, and (c) nature and scope of the tampering or flaw, determine whether there is a substantial likelihood that the tampering or flaw changed the outcome of a particular race.

- Where there is a substantial likelihood that tampering changed the outcome of a particular race, hold a new election for the office.

The following is an illustrative set of procedures that would allow jurisdictions to respond effectively to discrepancies between paper and electronic records during an automatic routine audit:

- Conduct a transparent investigation of all machines where the paper and electronic records do not match to determine whether there is any evidence that tampering with the paper records has occurred.

- To the extent that there is no record that the paper records have been tampered with, certify the paper records.

- If there is evidence that the paper records have been tampered with, give a presumption of authority to the electronic records.

- After giving a presumption of authority to the electronic records, conduct a forensic investigation on all machines where the paper and electronic records do not match, to determine whether there has been any tampering with the electronic records.

- If tampering with the electronic records can be ruled out, certify the electronic records.[13]

- Where there is evidence that both sets of records have been tampered with, conduct a full recount to determine whether and to what extent paper and electronic records cannot be reconciled.

- At the conclusion of the full recount, determine the total number of machines that report different electronic and paper records.

- After quantifying the number of machines that have been tampered with, determine the margin of victory in each potentially affected race.

- Based upon (a) the margin of victory, (b) the number of machines affected,

and (c) the nature and scope of the tampering, determine whether there is a substantial likelihood that tampering changed the outcome of a particular race.

- In the event that a determination is made that there is a substantial likelihood that tampering changed the outcome of a particular race, hold a new election for the office.

CONCLUSION

The Task Force has found that the three 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. Indeed, it is impossible to imagine a voting system that could be impervious to attack.

But there are straightforward countermeasures that that will substantially reduce the most serious security risks presented by the three systems.

The Task Force's recommendations point the way for jurisdictions with the political will to protect their voting systems from attack. None of 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, conducting parallel testing – are particularly difficult or expensive to implement.[14] The Brennan Center urges election officials and policy makers to adopt the recommended security measures as soon as possible.

ENDNOTES

[1] NIST has informed the Brennan Center that the development of policy recommendations for voting systems is not within the agency's mission or institutional authority. Accordingly, the policy recommendations in the report should not be attributed to Task Force members who work for NIST.

[2] Tracy Campbell, DELIVER THE VOTE, at xvi (2005) (pointing to, among other things, a history of vote buying, ballot stuffing, and transposing of results).

[3] *Id.*

[4] Douglas W. Jones, *Threats to Voting Systems,* NIST Threat Analysis Workshop Presentation (Oct. 7, 2005), *available at* http://vote.nist.gov/threats/papers/threats_to_voting_systems.pdf (last visited May 25, 2006).

[5] *See, e.g.*, Brian Krebs, *Windows Security Flaw is 'Severe,'* Washington Post, Dec. 30, 2005, at D1 (publicizing a previously unknown flaw in Microsoft Windows).

[6] Ted Selker and Sharon Cohen, *An Active Approach to Voting Verification*, CalTech/MIT Voting Technology Project, Working Paper #28 (May 2005), *available at* http://vote.caltech.edu/media/documents/wps/vtp_wp28.pdf (last visited May 25, 2006).

[7] Lawrence Norden *et al.*, *Voting System Usability, in* THE MACHINERY OF DEMOCRACY (forthcoming July 2006) (original research by Prof. David Kimball).

[8] Maryland, which does not have a voter verified paper record requirement, also conducts parallel testing statewide. The 12 states that must conduct automatic audits of voter verified paper records are: AK, CA, CO, CT, HI, IL, MN, NM, NC, NY, WA, and WV.

[9] The 26 states are: AK, 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.

[10] Laws providing for inexpensive candidate-initiated recounts might also add security for voter verified paper. The Task Force did not examine such recounts as a potential countermeasure.

[11] 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. Among other reasons, a software attack program could be designed to re-activate any disabling of the wireless component.

[12] *See* RECOMMENDATIONS OF THE BRENNAN CENTER FOR JUSTICE AND THE LEADERSHIP CONFERENCE ON CIVIL RIGHTS FOR IMPROVING RELIABILITY OF DIRECT RECORDING ELECTRONIC VOTING SYSTEMS (2004), *available at* http://www.brennancenter.org/programs/downloads/voting_systems_final_ recommendations.pdf (last visited May 25, 2006) (recommending that jurisdictions hire independent security experts and create independent security oversight panels to implement and oversee security measures). Independent security experts and oversight panel members should be present during any forensic investigation, to increase its transparency.

[13] When a state determines that electronic records should be given a presumption of authority, the reverse process should be followed: first investigate the electronic records for tampering, then (if necessary) examine the paper records.

[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, Developer and 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 to Lawrence Norden, Associate Counsel, Brennan Center for Justice (February 25, 2006) (on file with the Brennan Center). Harvard L. Lomax, Registrar of Voters for Clark County, Nevada, estimates that a team 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 team 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 by Eric L. Lazarus and lawrence Norden 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, *Voting System Cost, in* THE MACHINERY OF DEMOCRACY (forthcoming July 2006).

BRENNAN CENTER FOR JUSTICE
BOARD OF DIRECTORS AND OFFICERS

BRENNAN CENTER

FOR JUSTICE

AT NYU SCHOOL OF LAW

161 Avenue of the Americas

12th Floor

New York, NY 10013

212-998-6730

www.brennancenter.org

BRENNAN CENTER

FOR JUSTICE

AT NYU SCHOOL OF LAW

161 Avenue of the Americas

12th Floor

New York, NY 10013

212-998-6730

www.brennancenter.org