AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

THE SCIENCE OF VOTING MACHINE TECHNOLOGY: ACCURACY, RELIABILITY AND SECURITY

HEARING

BEFORE THE

SUBCOMMITTEE ON TECHNOLOGY, INFORMATION POLICY, INTERGOVERNMENTAL RELATIONS AND THE CENSUS

OF THE

COMMITTEE ON GOVERNMENT REFORM

HOUSE OF REPRESENTATIVES

ONE HUNDRED EIGHTH CONGRESS

SECOND SESSION

JULY 20, 2004

Serial No. 108–258

Printed for the use of the Committee on Government Reform

Available via the World Wide Web: http://www.gpo.gov/congress/house
http://www.house.gov/reform

U.S. GOVERNMENT PRINTING OFFICE

98–208 PDF WASHINGTON : 2005

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2250 Mail: Stop SSOP, Washington, DC 20402–0001

COMMITTEE ON GOVERNMENT REFORM

TOM DAVIS, Virginia, *Chairman*

DAN BURTON, Indiana
CHRISTOPHER SHAYS, Connecticut
ILEANA ROS-LEHTINEN, Florida
JOHN M. MCHUGH, New York
JOHN L. MICA, Florida
MARK E. SOUDER, Indiana
STEVEN C. LATOURETTE, Ohio
DOUG OSE, California
RON LEWIS, Kentucky
JO ANN DAVIS, Virginia
TODD RUSSELL PLATTS, Pennsylvania
CHRIS CANNON, Utah
ADAM H. PUTNAM, Florida
EDWARD L. SCHROCK, Virginia
JOHN J. DUNCAN, JR., Tennessee
NATHAN DEAL, Georgia
CANDICE S. MILLER, Michigan
TIM MURPHY, Pennsylvania
MICHAEL R. TURNER, Ohio
JOHN R. CARTER, Texas
MARSHA BLACKBURN, Tennessee
PATRICK J. TIBERI, Ohio
KATHERINE HARRIS, Florida

HENRY A. WAXMAN, California
TOM LANTOS, California
MAJOR R. OWENS, New York
EDOLPHUS TOWNS, New York
PAUL E. KANJORSKI, Pennsylvania
CAROLYN B. MALONEY, New York
ELIJAH E. CUMMINGS, Maryland
DENNIS J. KUCINICH, Ohio
DANNY K. DAVIS, Illinois
JOHN F. TIERNEY, Massachusetts
WM. LACY CLAY, Missouri
DIANE E. WATSON, California
STEPHEN F. LYNCH, Massachusetts
CHRIS VAN HOLLEN, Maryland
LINDA T. SANCHEZ, California
C.A. "DUTCH" RUPPERSBERGER, Maryland
ELEANOR HOLMES NORTON, District of Columbia
JIM COOPER, Tennessee
BETTY MCCOLLUM, Minnesota

BERNARD SANDERS, Vermont (Independent)

MELISSA WOJCIAK, *Staff Director*
DAVID MARIN, *Deputy Staff Director/Communications Director*
ROB BORDEN, *Parliamentarian*
TERESA AUSTIN, *Chief Clerk*
PHIL BARNETT, *Minority Chief of Staff/Chief Counsel*

SUBCOMMITTEE ON TECHNOLOGY, INFORMATION POLICY, INTERGOVERNMENTAL RELATIONS AND THE CENSUS

ADAM H. PUTNAM, Florida, *Chairman*

CANDICE S. MILLER, Michigan
DOUG OSE, California
TIM MURPHY, Pennsylvania
MICHAEL R. TURNER, Ohio

WM. LACY CLAY, Missouri
STEPHEN F. LYNCH, Massachusetts

EX OFFICIO

TOM DAVIS, Virginia

HENRY A. WAXMAN, California

BOB DIX, *Staff Director*
URSULA WOJCIECHOWSKI, *Professional Staff Member*
JULIANA FRENCH, *Clerk*
DAVID MCMILLEN, *Minority Professional Staff Member*

CONTENTS

	Page
Hearing held on July 20, 2004	1
Statement of:	
Adler, Jim, founder and CEO, VoteHere, Inc.	101
Hite, Randolph C., Director, Information Technology Architecture and Systems, U.S. Government Accountability Office; Hratch G. Semerjian, Acting Director, National Institute of Standards and Technology, Technology Administration, U.S. Department of Commerce; and Terry Jarrett, general counsel for Hon. Matt Blunt, Missouri Secretary of State	17
Morganstein, Sanford J., president and founder, Populex Corp.	113
Rubin, Aviel, technical director, Information Security Institute, Department of Computer Science, Johns Hopkins University	91
Shamos, Michael, professor, Carnegie Mellon, director, Universal Library; co-director, Institute for E-Commerce	96
Letters, statements, etc., submitted for the record by:	
Adler, Jim, founder and CEO, VoteHere, Inc., prepared statement of	104
Clay, Hon. Wm. Lacy, a Representative in Congress from the State of Missouri, prepared statement of	9
Hite, Randolph C., Director, Information Technology Architecture and Systems, U.S. Government Accountability Office, prepared statement of	20
Holt, Hon. Rush D., a Representative in Congress from the State of New Jersey, prepared statement of	15
Jarrett, Terry, general counsel for Hon. Matt Blunt, Missouri Secretary of State, prepared statement of	75
Morganstein, Sanford J., president and founder, Populex Corp., prepared statement of	115
Putnam, Hon. Adam H., a Representative in Congress from the State of Florida, prepared statement of	4
Rubin, Aviel, technical director, Information Security Institute, Department of Computer Science, Johns Hopkins University, prepared statement of	94
Semerjian, Hratch G., Acting Director, National Institute of Standards and Technology, Technology Administration, U.S. Department of Commerce, prepared statement of	67
Shamos, Michael, professor, Carnegie Mellon, director, Universal Library; co-director, Institute for E-Commerce, prepared statement of	99

THE SCIENCE OF VOTING MACHINE TECHNOLOGY: ACCURACY, RELIABILITY AND SECURITY

TUESDAY, JULY 20, 2004

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON TECHNOLOGY, INFORMATION POLICY,
INTERGOVERNMENTAL RELATIONS AND THE CENSUS,
COMMITTEE ON GOVERNMENT REFORM,
Washington, DC.

The subcommittee met, pursuant to notice, at 10:07 a.m., in room 2247, Rayburn House Office Building, Hon. Adam Putnam (chairman of the subcommittee) presiding.

Present: Representatives Putnam and Clay.

Also present: Representatives Holt and Kaptur.

Staff present: John Hambel, senior counsel; Dan Daly, professional staff member/deputy counsel; Ursula Wojciechowski, professional staff member; Juliana French, clerk; Felipe Colon, fellow; Casey Welch and Jamie Harper, legislative assistants; Sean Hardgrove, intern; David McMillen, minority professional staff member; and Earley Green, minority chief clerk.

Mr. PUTNAM. The quorum being present, this Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census will come to order.

Good morning, everyone, and welcome to the subcommittee's hearing, "The Science of Voting Machine Technology: Accuracy, Reliability and Security."

An estimated 50 million voters representing nearly 30 percent of all voters are expected to cast their votes using some type of electronic voting technology this November. We have scheduled this oversight hearing to examine where we are today with the evolution of electronic voting technology, including the subject of access, utilization and the associated issues of reliability, ease of use, efficiency, accuracy and security.

The overriding goal of voting systems is to produce election results that accurately represent the will of the people. The historically close Presidential election of 2000 in Congress highlighted deficiencies of the voting process, especially in my State, that became the subject of many policy discussions at all levels of government. Since then many localities have sought to evaluate and improve their voting systems through the use of electronic voting technology, believing that such technology will improve the accuracy of vote recording and tabulation, decrease costs, and increase voter turnout.

The issues we will be examining today in the processes of balloting and tabulating the results of elections have been the subjects of discussions throughout our history. Deficiencies of one type or another have existed in virtually every process that has ever been utilized, yet today's existing and emerging technology offers greater opportunities for participation in the process of selecting our elected representatives, as well as the determination of other ballot questions.

The Federal Government had not historically set mandatory standards for voting systems, nor had it provided funding to State and local jurisdictions for the administration of elections. However, after November 2000, Congress considered and debated Federal election reform legislation, and the Help America Vote Act of 2002, or HAVA, was enacted. The act created a new Federal Government agency with election administration responsibilities, set requirements for voting and voter registration systems and provided Federal funding.

Beginning in January 2006, in accordance with HAVA, voting systems used in Federal elections must provide for error correction by voters, manual auditing, accessibility, alternative languages and Federal error rate standards. Systems must also maintain voter privacy and ballot confidentiality, and States must adopt uniform standards for what constitutes a vote on each system.

HAVA does not require any specific voting system, but it sets requirements that influence what systems election officials choose. HAVA's requirement for at least one handicapped-accessible voting system per polling place and other factors are expected to drive States toward adoption of touch-screen or direct recording electronic systems [DREs].

HAVA established a program to provide access to approximately $4 billion in Federal grants to States to modernize the voting systems currently in use. Accordingly, acquisitions of new voting systems technology are under way in a number of States and localities.

Currently five different voting systems are being used: hand-counted paper ballots, mechanical lever machines, computer punch cards, optical scan or marks forms, and DREs. Most States use more than one type of system. Each has advantages and disadvantages with respect to error rates, cost, speed, recounts, accessibility to the disabled and other characteristics. Differences in actual performances in elections are difficult to measure accurately and depend on a number of factors, such as the system design and condition, voter system familiarity, ballot complexity and design, local standards and practices, and the competence level of polling and training of polling place workers.

Since 2000, many electronic voting systems have been proposed. Today DREs, which present voters with choices on the video display and record votes electronically, are gaining favor. They offer improved user interfaces, facilitate voter confirmation, provide instant running tabulations, and potentially satisfy HAVA's requirement for at least one handicapped device per polling place.

There is concern how secure systems are from tampering by voters, elections officials or even manufacturers. There is also concern by some about the potential for software defects or other technical

failures that could interrupt the capability of the given system. There are disagreements among experts about both the seriousness of these concerns and what solutions to address them. While it is generally accepted that tampering is possible with any computer system given the time and resources, some experts believe that current security practices are sufficient. Others, naturally, disagree and believe that procedural and other safeguards can make DREs sufficiently safe from tampering, that the use of creating printed paper ballots would create too many problems. A number of these issues will be explored today.

As presently designed, many electronic voting systems do not produce a record that can be independently audited. For this reason and others, the prospect of electronic voting systems has been met with some skepticism in parts of the information technology community. Moreover, experience with large-scale technology deployment indicates that it takes time before the bugs in the system, including technology procedures and people associated with using and operating the technology, are shaken out or identified. So even communities that have deployed and used these systems will face the challenge of evaluating their performance.

Given the importance of the issue, in May I signed on to a bipartisan GAO request letter asking for a study examining the security of electronic voting systems, including DREs, optical scans and punch cards readers. We asked GAO to examine State, Federal and governmental use; identify significant issues and challenges; and report on best practices that can be implemented to improve the security and reliability of the electronic voting process.

Today's hearing will seek to further examine the technology of electronic voting systems: what are the lessons learned thus far; what are the most appropriate next steps, both short- and long-term, to ensure the integrity, reliability and accessibility of the security voting process that is such a vital ingredient to American democracy.

This is an election year, and as such it is often the case that both sides of the aisle attempt to score political points. That is not the purpose of this hearing. We are here to examine the technology that is available and learn from panels of experts what is and is not feasible in the current climate. Our goal is to further the discussion and debate on the technological advances that improve the manner in which our society conducts elections. My colleagues share my desire to conduct an informative oversight hearing, and I welcome their input and request for this hearing topic.

[The prepared statement of Hon. Adam H. Putnam follows:]

TOM LANTOS, CALIFORNIA
RANKING MINORITY MEMBER

ONE HUNDRED EIGHTH CONGRESS

Congress of the United States

House of Representatives

COMMITTEE ON GOVERNMENT REFORM

2157 RAYBURN HOUSE OFFICE BUILDING

WASHINGTON, DC 20515–6143

MAJORITY (202) 225-5074
FACSIMILE (202) 225-3974
MINORITY (202) 225-5051
TTY (202) 225-6852

www.house.gov/reform

HENRY A. WAXMAN, CALIFORNIA
RANKING MINORITY MEMBER

TOM LANTOS, CALIFORNIA
MAJOR R. OWENS, NEW YORK
EDOLPHUS TOWNS, NEW YORK
PAUL E. KANJORSKI, PENNSYLVANIA
CAROLYN B. MALONEY, NEW YORK
ELIJAH E. CUMMINGS, MARYLAND
DENNIS J. KUCINICH, OHIO
DANNY K. DAVIS, ILLINOIS
JOHN F. TIERNEY, MASSACHUSETTS
WM. LACY CLAY, MISSOURI
DIANE E. WATSON, CALIFORNIA
STEPHEN F. LYNCH, MASSACHUSETTS
CHRIS VAN HOLLEN, MARYLAND
LINDA T. SANCHEZ, CALIFORNIA
C.A. DUTCH RUPPERSBERGER, MARYLAND
ELEANOR HOLMES NORTON, DISTRICT OF COLUMBIA
JIM COOPER, TENNESSEE

BERNARD SANDERS, VERMONT,
INDEPENDENT

SUBCOMMITTEE ON TECHNOLOGY, INFORMATION POLICY, INTERGOVERNMENTAL RELATIONS AND THE CENSUS

Congressman Adam Putnam, Chairman

OVERSIGHT HEARING
STATEMENT BY ADAM PUTNAM, CHAIRMAN

Hearing topic: *"The Science of Voting Machine Technology: Accuracy, Reliability and Security."*

Wednesday, July 20, 2004
10:00 a.m.
Room 2247, Rayburn House Office Building

OPENING STATEMENT

Good morning and welcome to the Subcommittee's hearing on "The Science of Voting Machine Technology: Accuracy, Reliability and Security." An estimated 50 million registered voters, representing nearly 30 percent of all voters, are expected to cast their votes using some type of electronic voting technology this November. The Subcommittee scheduled this oversight hearing to examine where we are today with the evolution of electronic voting technology, including the subject of access, utilization and the associated issues of reliability, ease of use, efficiency, accuracy, and security.

The overriding goal of voting systems is to produce election results that accurately represent the will of the people. The Presidential election of 2000 highlighted deficiencies in the voting process that became the subject of many policy discussions at all levels of government. Since then, many localities have sought to evaluate and improve their voting systems through the use of electronic voting technology, believing that such technology will improve the accuracy of vote recording and tabulation, decrease costs, and increase voter turnout.

The issues we will be examining today in the processes of balloting and tabulating the results of elections, have been the subjects of discussion throughout our history. Deficiencies of one type or another have existed in virtually every process that has ever been utilized, yet today's

technology offers greater opportunities for participation in the important process of selecting our elected representatives as well as other ballot questions.

The federal government had not historically set mandatory standards for voting systems, nor had it provided funding to state and local jurisdictions for the administration of elections. However, after November 2000, Congress, the states, and various electoral commissions examined election procedures, voting technologies, whether national standards are necessary, along with the federal role in the election process. Congress considered and debated federal election reform legislation, and the Help America Vote Act of 2002 (P.L. 107-252) (HAVA) was enacted in October 2002. The act creates a new federal agency with election administration responsibilities, sets requirements for voting and voter-registration systems and certain other aspects of election administration, and provides federal funding.

I'd like to note for the record that both Polk and Hillsborough Counties in Florida, which I represent, had made significant investments in improving their voting machines and had touch-screens in place for the 2000 election.

HAVA established a program to provide access to approximately $4 billion in federal grants to states to modernize the voting systems currently in use. And acquisitions of new voting system technology are underway in a number of states and localities. HAVA does not require any particular voting system, but it sets requirements that will influence what systems election officials choose. HAVA's requirement for at least one handicapped accessible voting system per polling place and other factors are expected to drive states toward adopting touch-screen or direct recording electronic (DRE) machines.

Beginning January 2006, in accordance with HAVA, voting systems used in federal elections must provide for error correction by voters, manual auditing, accessibility, alternative languages, and federal error-rate standards. Systems must also maintain voter privacy and ballot confidentiality, and states must adopt uniform standards for what constitutes a vote on each system.

In general, it is desirable for voting systems, amongst other things, to:

- count votes accurately;
- prevent double voting;
- maintain voter privacy and anonymity;
- assure the voter that his or her vote has been counted toward the final tally without compromising anonymity;
- prevent vote tampering with results, both during and after the period during which polls are open, especially by anyone with authorized access to those results;
- provide for meaningful audits;
- maintain proper operation even in the face of power failures and other disasters; and
- support equal access to voting (including access for sub-populations such as non-English language voters and voters with various disabilities).

Currently five technologies are used: hand-counted paper-ballots, mechanical lever machines, computer punchcards, optical scan or marksense forms, and direct recording electronic systems. Most states use more than one kind of system. Each has advantages and disadvantages with respect to error rates, cost, speed, recounts, accessibility to disabled persons, and other characteristics. Differences in actual performances in elections are difficult to measure accurately and depend on many factors, such as the design and condition of the system, the familiarity of voters with it, the complexity and design of the ballot, local standards and practices, and the level of competence of polling place workers.

Since 2000, many electronic voting systems have been proposed. Today, DREs, which present voters with choices on a video display and record votes electronically, are gaining favor. They offer improved user interfaces, facilitate voter confirmation, provide instant running tabulations, and potentially satisfy HAVA's requirement for at least one handicapped accessible voting device per polling place.

There is currently some controversy about how secure these systems are from tampering by voters, election personnel, or even manufacturers. There is also concern by some about the potential for software defects or other technical failures that could interrupt the capability of a given system. There are disagreements among experts about both the seriousness of these concerns and what should be done to address them. While it is generally accepted that tampering is possible with any computer system given sufficient time and resources, some experts believe that current security practices are sufficient. Others believe that additional steps are needed.

Some experts believe that the problem is serious enough to require changes in the systems before they are more widely adopted, ranging from more sophisticated computer security to the printing of paper ballots that would be verified by the voter and hand-counted if the election results were contested. Others believe that procedural and other safeguards can make DREs sufficiently safe from tampering, that use of printing paper ballots would create too many problems, and that the controversy risks drawing attention away from the demonstrated utility of DREs in addressing known challenges of access to and usability of voting systems.

As presently designed, many electronic voting systems do not produce a record that can be independently audited. For this reason and others, the prospect of electronic voting systems has been met with some skepticism in parts of the information technology community. Moreover, experience with large-scale technology deployment indicates that it takes some time before the bugs in the system, the technology, procedures and people associated with using and operating the technology, are shaken out or even identified, and so even communities that have deployed and used these systems will face the challenge of how to evaluate their performance. Additionally, there continues to be questions about the maturity of the technology available to the market today, as well as the functional capabilities of access for the disabled community and the ability to conduct audits should that be necessary.

I look forward to the expert testimony from all our distinguished panelists that will provide a greater understanding of the fine points of voting machine technology. Today's hearing will seek to further examine the science and technology of electronic voting systems; what are the lessons learned thus far; and what are the most appropriate next steps, both short term and long term, to insure the integrity, reliability, accessibility, and security of the voting process that is such and important ingredient in American democracy and a justifiable expectation of the American people

This is an election year, and as such it is often the case that those on both sides of the aisle attempt to score political points. That is not the purpose of this hearing. We are here today to examine the technology that is available, and learn from panels of experts what is and is not feasible in the real world. Our goal is to further the discussion and debate on the technological advances that improve the manner in which our society conducts elections. I know that my colleagues share my desire to conduct an oversight hearing that is free from rancor and division.

#####

Mr. PUTNAM. Following Mr. Clay's opening statement, I would like to move directly to the witnesses' testimony, and request that other Members submit their opening statements for the record. Members, of course, will be invited to participate in the witness question-and-answer process.

I now yield to the distinguished ranking member of the subcommittee Mr. Clay for his opening remarks.

You are recognized, Mr. Clay.

Mr. CLAY. Mr. Chairman, first let me thank you for holding this hearing.

Florida and Missouri are both States with troubled voting histories. In the 2000 election, I had to go to court to keep the polls open so that everyone who wanted to vote could vote. The city had dropped thousands of voters from the rolls without ever telling the voter.

The issue before us is quite simple. I want to vote, and I want know that my vote is counted as I intended. With the paper ballot, my vote is before me, and I place it in the ballot box. The same holds true with punch cards and optical scans machines, although both of those are subject to mechanical error. Everyone in the country now knows what a hanging chad is. With lever machines and computerized voting, you have to take it on faith that your vote is counted as you intended.

The difference is one of scale. If a lever machine fails or is tampered with, it affects only that machine. If it's software, or computerized voting fails or is tampered with, it affects every machine running that program, and, therefore, the system fails the voter.

Last week the New York Times reported that in the March Florida primary, votes were not recorded for about 1 out of every 100 persons using the new machine. Some people, in defense of the new machines, point out that is about the same error rate as Florida experienced in the 2000 election. I don't think any of us want to use Florida 2000 as the standard, no offense against your State.

Advocates for computerized voting tell us to trust the system. My experience says trust but verify. That is why I believe, as do 130 of my colleagues who have cosponsored Congressman Holt's bill, who happens to be with us today, that the computerized machines that are out there today are inadequate. They offer no way to verify my vote. The certification process is inadequate. As we have seen in California, some manufacturers bypass certification.

After the vote is cast, the issue is counting the vote. Again, I say trust, but verify. With paper ballots, a recount is a straightforward matter. Recounting punch cards and optical scan ballots is also straightforward. There is no recount for computerized voting. That is not verification. That is trusting that the software performed as promised.

I believe we all have had enough experience with software to know that trusting it to work correctly 100 percent of the time is a foolish concept. Some suggest that the internal audit trail and the computerized machines would be sufficient for a recount. I don't know if that is true, but I do know that the audit trail is subject to the same weaknesses as all software. It is invisible to the voter, and its reliability must be taken on faith.

California ran a parallel monitoring system during its March primary, where live machines were set aside for testing. In that case the machine worked as intended, but parallel testing doesn't work to check the machines. What do you do if you find at the end of the day that the machine failed to test? Do you throw out the whole precinct? Do you throw out all votes cast on that kind of machine?

I am a man of faith, and I have great trust in my fellow man, but when it comes to voting, faith and trust are not the building blocks for a secure system. If we are to earn the voters' trust, we must provide them with voting opportunities that are simple and direct. We must provide them with machines that allow the voter to see his or her vote.

Computerized voting machines are wonderful inventions for those that run elections. They make the job of counting and transmitting the vote about as simple as can be. As a bonus, they make recounts a thing of the past. But we don't run elections for the convenience of election boards or election officials, we run elections to provide the public with the opportunity to participate in their government. We must provide the public with the most transparent voting system possible. Computerized voting does not accomplish that.

Two months ago the Secretary of State of California issued stringent security measures that counties had to meet before electronic voting machines could be used. Last week the Secretary of State of Ohio, one of the outspoken advocates of electronic voting, halted the deployment of those machines in Ohio. Several of the flaws identified last December still had not been corrected.

Last week in Maryland, participants in the Computer Ate My Vote rally said that electronic voting machines are poorly programmed and prone to hackers. At that rally, Barbara Simons, a former president of the Association for Computing Machinery, told those gathered, "If I had a single message, that message would be, wait, there is better technology on the way."

I look forward to working with the Election Assistance Commission and my fellow Members of Congress to reassure the American voter that their votes are safe and will be counted. In this debate that should be everyone's goal and objective. I thank you, Mr. Chairman for this hearing today.

Mr. PUTNAM. I thank you, Mr. Clay.

[The prepared statement of Hon. Wm. Lacy Clay follows:]

STATEMENT OF THE HONORABLE WM. LACY CLAY

July 20, 2004

Mr. Chairman, thank you for holding this hearing. Florida and Missouri are both states with troubled voting histories. In the 2000 election I had to go to court to keep the polls open so that everyone who wanted to vote could vote. The city had dropped thousands of voters from the rolls without ever telling the voter.

The issue before us is quite simple. I want to vote, and I want to know that my vote is counted as I intended. With a paper ballot, my vote is there in front of me, and I place it in the ballot box. The same is true of punch cards and optical scan machines, although both of those are subject to mechanical error -- everyone in the country now knows what a hanging chad is. With lever machines and computerized voting, you have to take it on faith that your vote is counted as you intended. The difference is one of scale. If a lever machine fails or is tampered with, it affects only that machine. If the software for

computerized voting fails or is tampered with, it affects every machine running that program, and therefore the system fails the voter.

Last week, the *New York Times* reported that in the March Florida primary, votes were not recorded for about one out of every 100 persons using the new machines. Some people, in defense of the new machines, point out that that is about the same error rate as Florida experienced in the 2000 election. I don't think any of us want to use Florida 2000 as the standard.

Advocates for computerized voting tell us to trust the system. My experience says trust but verify. That is why I believe, as do 130 of my colleagues who have co-sponsored Congressman Holt's bill, that the computerized machines that are out there today are inadequate. They offer no way to verify my vote. The certification process is inadequate, and as we have seen in California, some manufacturers bypass certification.

After the vote is cast, the issue is counting the votes. Again I say, trust but verify. With paper ballots, a recount is a

straightforward matter. Recounting punch cards and optical scan ballots is also straightforward. There is no recount for computerized voting. That is not verification. That is trusting that the software performed as promised. I believe we all have had enough experience with software to know that trusting it to work correctly 100% of the time is foolish.

Some suggest that the internal audit trail in the computerized machines would be sufficient for a recount. I don't know if that is true, but I do know that the audit trail is subject to the same weaknesses as all software -- it is invisible to the voter, and its reliability must be taken on faith.

California ran a parallel monitoring system during its March primary where live machines were set aside for testing. In that case, the machines worked as intended, but parallel testing doesn't work to check the machines. What do you do if you find at the end of the day that the machine failed the test? Do you throw out the whole precinct? Do you throw out all votes cast on that kind of machine?

I am a man of faith, and I have great trust in my fellow man. But when it comes to voting, faith and trust are not the building blocks for a secure system. If we are to earn the voter's trust, we must provide them with voting opportunities that are simple and direct. We must provide them with machines that allow the voter to see his or her vote.

Computerized voting machines are wonderful inventions for those that run elections. They make the job of counting and transmitting the vote about as simple as can be. As a bonus, they make recounts a thing of the past. But we don't run elections for the convenience of election boards or election officials. We run elections to provide the public with the opportunity to participate in their government. We must provide the public with the most transparent voting system possible. Computerized voting does not accomplish that.

Two months ago, the Secretary of State issued stringent security measures that counties had to meet before electronic voting machines could be used. Last week, the Secretary of State of Ohio, one of the outspoken advocates of electronic

voting, halted the deployment of those machines in Ohio. Several of the flaws identified last December still had not been corrected. Last week in Maryland, participants in "The Computer Act My Vote" rally said that electronic voting machines are poorly programmed and prone to hackers. At that rally, Barbara Simmons, a former president of the Association for Computing Machinery, told those gathered "If I had a single message…that message would be Wait. There is better technology on the way."

I look forward to working with the Election Assistance Commission and my fellow members of Congress to reassure the American voter that their votes are safe and will be counted. In this debate, that should be everyone's goal and objective.

Mr. PUTNAM. Mr. Clay requested this hearing, and I am delighted to work with him to put it together, and we appreciate your interest. It's very important.

We have been joined by Mr. Holt, a gentleman from New Jersey. Without objection, I would like to insert your opening statement into the record and also ask unanimous consent that you sit on the panel and join us, despite not being a member of the committee.

Mr. HOLT. Thank you.

[The prepared statement of Hon. Rush D. Holt follows:]

Statement of Representative Rush Holt to
The Committee on Government Affairs Subcommittee on Technology, Information Policy, Intergovernmental Relations, and the Census
July 20, 2004

The process of voting must be fair, accessible and verifiable. While I have always supported increases in fairness and accessibility in the voting system, today I am focused on the verifiability, that is the auditability, of the voting system. I believe the auditability of our electoral system has not been given due attention, and has unjustifiably been treated as mutually exclusive to accessibility. We must take pains to uphold all three principles.

Voting is the foundation of democracy, and votes are inherently valuable. Anything valuable, such as bank records, or property records, must be auditable. We wouldn't have it any other way. The same absolutely must be true of our votes.

The process of voting in a democracy was always intended to belong strictly to the voter, who makes his or her decision and casts the ballot, and the election official, who counts it. A system such as this is "publicly" auditable, as it should be in a democracy – with the voters alone verifying that their intentions are properly recorded and the election officials alone verifying the accuracy of the tally. If a voter casts a vote on an electronic voting machine, verifying nothing but what is for a transitory moment in time reflected on the screen, how can the record of that vote be meaningfully audited? Can any election official, computer scientist, or voting system vendor reconstruct what that voter intended? No. The voter votes in secret. Because of the secret ballot, only the voter can verify that his or her intention is recorded correctly. That is why a hard copy of each vote – verified by the voter him or herself – must be required of all voting systems.

Voting systems that include hard copy paper ballots have been found to be among the most accurate of any voting system. The 2001 Caltech MIT study, "*Voting, What is, What Could Be*" reported that over the twelve-year period surveyed (1988-2000) "[o]ptically scanned paper and hand-counted paper ballots have consistently shown the best average performance. Scanners have the lowest rate of uncounted, unmarked, and spoiled ballots in presidential races and in Senate and gubernatorial races . . . Hand-counted paper has shown similarly low residual vote rates." The statistics reported were as follows: in presidential races, the residual vote rate as a percentage of all ballots cast was 1.8% for paper ballots, 1.5% for optically scanned paper ballots, and 2.3% for touch screen (DRE) machines. In Senate and gubernatorial races, the rates were 3.3%, 3.5% and 5.9%, respectively.

Besides having a worse residual vote rate than optically scanned and hand-counted paper-ballots, touch screen machines in their current form are not meaningfully auditable. This is fundamental. Better machines, better programmers, better procedures will not remove

(continued)

this problem. The report continued "[i]n the 2000 presidential election, the state of Florida conducted an enormous audit of its voting machines . . . . It is extremely important to be able to conduct such an audit. . . . Paper ballots have the highest degree of auditability. . . . The votes cast on a broken machine can never be reclaimed . . . Most new electronic machines produce an internal paper tape (like a cashiers tape) and an electronic recording of every voting session. . . . While this is an improvement over [older DRE] machines, it is not a direct recording of the voter's intention. If the machine fails between the touch screen and the tape, the voter's stated intentions are still lost. We feel that new voting standards must require a minimum level of auditability."

The touchscreen machines currently in use, which produce no voter verified paper trail, may count as many as 50 million ballots this November. Is there a possibility that the votes cast on those machines will be manipulated? Is it possible that the manipulation will go undetected? Of course it is. Numerous news accounts in recent years have reported irregularities in the results produced on electronic voting machines. The cause of each of those irregularities will always remain a matter of some speculation. But the bottom line is, inspection, testing and certification – all of which had been conducted on all of the machines in question – did not prevent those incidents. The integrity of those votes counts has been lost forever.

It is critical that all votes be independently auditable, which is only possible with systems that incorporate a voter verified paper audit trail. In the absence of an independent audit mechanism, the vote count will no longer be publicly owned. The voters will no longer verify the accuracy of their own ballots. No one else can. Because the software of virtually all electronic voting systems is protected by trade secret agreements, the American public is left to simply trust that, at the end of the day, the machines have given them the right answer. That is simply not acceptable in a democracy.

###

Mr. PUTNAM. Without objection, we would welcome you to the subcommittee and certainly encourage you to participate in the dialog, and we move directly to the witness testimony.

Before doing so I would ask that the witnesses please rise, and anyone who would be accompanying who will be helping you in answering the questions, and raise your right hands.

[Witnesses sworn.]

Mr. PUTNAM. I would note for the record that all the witnesses responded in the affirmative.

We will move to our first witness, Mr. Randolph Hite. Mr. Hite is the Director of Information Technology Architecture and Systems Issues at the U.S. Government Accountability Office, formally the GAO, still the GAO, but new G and A. During his 25-year career with GAO, he has directed reviews of major Federal investments and information technology, such as IRS's tax systems modernization and DOD's business systems modernization. Mr. Hite is the principal author of several information technology management guides, including GAO's system guides on systems testing. He frequently testifies before Congress on such topics and is an ex officio member of the Federal CIO Council. He received a number of awards throughout his career and was a 2003 Federal 100 Award winner.

Welcome to the subcommittee. You are recognized for 5 minutes.

STATEMENTS OF RANDOLPH C. HITE, DIRECTOR, INFORMATION TECHNOLOGY ARCHITECTURE AND SYSTEMS, U.S. GOVERNMENT ACCOUNTABILITY OFFICE; HRATCH G. SEMERJIAN, ACTING DIRECTOR, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, TECHNOLOGY ADMINISTRATION, U.S. DEPARTMENT OF COMMERCE; AND TERRY JARRETT, GENERAL COUNSEL FOR HON. MATT BLUNT, MISSOURI SECRETARY OF STATE

Mr. HITE. Thank you, Mr. Chairman. It seems like only yesterday that hanging chads and butterfly ballots were the focus of attention. Now almost 4 years later, the focus is on verifiable audit trails and code tampering as they relate to the modern ATM-like voting devices, which in many jurisdictions have replaced the more venerable voting machine that gave rise to the 2000 election debate.

In the wake of this debate in 2000, we issued a series of reports in 2001 on election administration and voting technology. We made a number of recommendations for reform. In my view, the gist of what we said then still applies today, which I will summarize by making four points.

Point one, although voting systems play a major role in elections, they are but one facet of a complex, highly decentralized, multidimensional elections process in which each dimension demands on the interplay of people, processes and technology. As such, when I think of the, "voting system," I think of the inseparable triad of the equipment itself, the individuals who interact with the equipment and the rules that govern this interaction.

Point two, although security has taken center stage in the debates surrounding some electronic voting systems, other interrelated performance characteristics, such as accuracy, ease of use

and cost, are also important. For example, the commonly called DREs have been criticized because they lack a paper record. At the same time these DREs offer ease of use advantages because they are more accommodating to voters with disabilities, and they protect against certain voter errors, such as overvoting, which can affect how accurately voter intent is captured. On the other hand, optical scan voting systems have a lower capital cost than DREs, and they offer a paper record. However, they are relatively more challenging for voters with certain disabilities to use.

Point three, voting system performance can be traced to two key variables. The first is the quality of the standards that the system is designed to meet, which includes, in my view, the quality of the development and testing that was performed to ensure that the system, in fact, meets the standards.

Second is how well the system, as it has been designed, developed and tested, is used in an operational setting, which includes the effectiveness of the procedures that are followed concerning system maintenance, setup, use and operation, combined with the know-how of the people who are interacting with the system. If either of these variables is lacking, system performance can suffer.

Point four, local jurisdictions face challenges in effectively leveraging modern voting technology this year and for years to come. For this year, jurisdictions need to maximize the performance and minimize the risk associated with the systems that they have, whether electronic or not electronic, which is a particularly important point given that three-quarters of the voters in 2004 are expected to vote the same way that they did in 2000.

To accomplish this, it is important for jurisdictions to make sure that they perform the requisite testing and maintenance activities, and, in doing so, they treat the people, the processes and the technology as a triad; in effect, as the voting system.

Other challenges are more long-term, and they relate to the need for jurisdictions to make informed decisions about whether to change their voting equipment, and our work in 2001 showed that voting jurisdictions were not consistently addressing all of these challenges.

In closing, let me emphasize electronic voting technology is a critical link in the election chain, and while this link by itself cannot make an election, it can break one if not designed, tested, maintained, implemented and maintained properly. The concerns being surfaced with this technology highlight the potential for election problems if jurisdictions do not effectively address the challenges that I just mentioned.

I believe HAVA recognizes these challenges as does the Election Assistance Commission, so I say let's give them a chance to do what they were established to do. In this regard, although the Commission only recently began operations, and is not yet at full strength, I believe that it has hit the ground running to inform and educate jurisdictions and voters about electronic voting systems and promote the interplay of people, process and technology in the November 2004 election.

Beyond this, the Commission, with the assistance of NIST and others, will need to examine opportunities for strengthening these voting standards and the testing that's associated with enforcing

the standards. Critical to accomplishing their roles under HAVA will be ensuring that they have the resources they need to do their jobs, and that they proceed in an open and transparent manner.

Mr. Chairman, that concludes my statement. I will be happy to answer any questions.

Mr. PUTNAM. Thank you very much, Mr. Hite.

[The prepared statement of Mr. Hite follows:]

United States Government Accountability Office

GAO

Testimony

Before the Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census, Committee on Government Reform, House of Representatives

For Release on Delivery
Expected at 10:00 a.m. EDT
Tuesday, July 20, 2004

ELECTIONS

Electronic Voting Offers Opportunities and Presents Challenges

Statement of Randolph C. Hite, Director
Information Technology Architecture and Systems

GAO-04-975T

July 20, 2004

GAO
Accountability · Integrity · Reliability

Highlights

Highlights of GAO-04-975Ta testimony before the Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census, Committee on Government Reform, House of Representatives

ELECTIONS

Electronic Voting Offers Opportunities and Presents Challenges

Why GAO Did This Study

The technology used to cast and count votes is one aspect of the multifaceted U.S. election process. GAO examined voting technology, among other things, in a series of reports that it issued in 2001 following the problems encountered in the 2000 election. In October 2002, the Congress enacted the Help America Vote Act, which, among other things, established the Election Assistance Commission (EAC) to assist in the administration of federal elections. The act also established a program to provide funds to states to replace older punch card and lever machine voting equipment. As this older voting equipment has been replaced with newer electronic voting systems over the last 2 years, concerns have been raised about the vulnerabilities associated with certain electronic voting systems.

Among other things, GAO's testimony focuses on attributes on which electronic voting systems can be assessed, as well as design and implementation factors affecting their performance. GAO also describes the immediate and longer term challenges confronting local jurisdictions in using any type of voting equipment, particularly electronic voting systems.

www.gao.gov/cgi-bin/getrpt?GAO-04-975T.

To view the full product, including the scope and methodology, click on the link above. For more information, contact Randolph C. Hite at (202) 512-3439 or hiter@gao.gov.

What GAO Found

An electronic voting system, like other automated information systems, can be judged on several bases, including how well its design provides for security, accuracy, ease of use, and efficiency, as well as its cost. For example, direct recording electronic systems offer advantages in ease of use because they can have features that accommodate voters with various disabilities, and they protect against common voter errors, such as overvoting (voting for more candidates than is permissible); a disadvantage of such systems is their capital cost and frequent lack of an independent paper audit trail. Advantages of optical scan voting equipment (another type of electronic voting system) include capital cost and the enhanced security associated with having a paper audit trail; disadvantages include lower ease of use, such as limited ability to accommodate voters with disabilities.

One important determinant of voting system performance is how it is designed and developed, including the testing that determines whether the developed system performs as designed. In the design and development process, a critical factor is the quality of the specified system requirements as embodied in applicable standards or guidance. For voting technology, these voluntary standards have historically been problematic; the EAC has now been given responsibility for voting system guidelines, and it intends to update them. The EAC also intends to strengthen the process for testing voting system hardware and software. A second determinant of performance is how the system is implemented. In implementing a system, it is critical to have people with the requisite knowledge and skills to operate it according to well-defined and understood processes. The EAC also intends to focus on these people and process factors in its role of assisting in the administration of elections.

In the upcoming 2004 national election and beyond, the challenges confronting local jurisdictions in using electronic voting systems are similar to those facing any technology user. These challenges include both immediate and more long term challenges, as shown in the table.

Challenges in Using Electronic Voting Systems

Time frame	Challenge
Near term	• Performing those security, testing, and maintenance activities needed to adequately ensure that the system operates as intended.
	• Managing the system, the people who interact with the system, and the processes that govern this interaction as interrelated and interdependent parts.
Long term	• Having reliable measures and objective data to know whether the system is meeting the needs of the user community (both voters and those who administer the elections).
	• Making choices about future system changes in light of whether a given system will provide benefits over its useful life that are commensurate with life cycle costs, and ensuring that these costs are affordable.

Source: GAO.

Mr. Chairman and Members of the Subcommittee:

I appreciate the opportunity to participate in today's hearing on electronic voting systems.[1] In light of concerns associated with the voting systems used in the 2000 election, we produced a series of reports, issued in 2001,[2] in which we examined virtually every aspect of the election process, including types of voting technology. As we reported in 2001, the particular technology used to cast and count votes is a critical part of this process, but it is only one facet of a multifaceted election process. Other facets include the people who implement and use the technology and the processes that govern its implementation, among which are the standards used to define the characteristics and performance of the technology. Accordingly, we recognized that no voting technology, however well designed, can be a magic bullet that will solve all the problems that can arise in the election process. At the same time, we also recognized that if not properly managed, this one facet of the election process can significantly undermine the integrity of the whole.

As requested, my testimony today will focus on electronic voting systems, and in doing so I will address (1) the role of these systems within the larger election process, (2) attributes that can be used to examine these systems' capabilities, (3) the importance of both system design and implementation to the performance of these systems, and (4) the challenges confronting local jurisdictions in using any type of voting equipment, particularly electronic voting systems.

In preparing for this testimony, we drew extensively from our published work on the election process. We augmented this work

[1] In this testimony, the term *electronic voting system* is used generically, to refer both to optical scan systems and direct recording electronic systems, both of which depend on electronic technology. Each type of system is described more fully in the Background section of this testimony.

[2] For example, U.S. General Accounting Office, *Elections: Perspectives on Activities and Challenges across the Nation*, GAO-02-3 (Washington, D.C.: Oct. 15, 2001); *Elections: Status and Use of Federal Voting Equipment Standards*, GAO-02-52 (Washington, D.C.: Oct. 15, 2001); and *Elections: A Framework for Evaluating Reform Proposals*, GAO-02-90 (Washington, D.C.: Oct. 15, 2001).

with reviews of more recent studies of electronic voting systems and other relevant documents. In addition, we interviewed commissioners of the newly appointed Election Assistance Commission (EAC) regarding its efforts to date and its plans, and we attended EAC and other commission hearings on electronic voting systems. Our follow-up work was performed from February to July 2004 in Washington, D.C. All the work on which this testimony is based was performed in accordance with generally accepted government auditing standards.

Results in Brief

Electronic voting systems play a vital role in elections, but they are only one component in a multidimensional process. The people, processes, and technology that make up these various dimensions all contribute to the success of the overall election process. From a national perspective, this overall process involves many levels of government, including over 10,000 jurisdictions with widely varying characteristics and requirements. For example, the size of a jurisdiction and the languages spoken by voters are significant variables in local election processes, as is the performance of the particular voting system used.

The performance of an electronic voting system, like any type of automated information system, can be judged on several bases, including how well its design provides for security, accuracy, ease of use, and efficiency, as well as cost. For example, direct recording electronic systems have advantages in ease of use because they can have features that accommodate persons with various disabilities, and they provide features that protect against common voter errors; disadvantages of such systems are their cost and their frequent lack of an independent paper audit trail. Advantages of optical scan voting equipment, which is another type of electronic voting system, include cost and the enhanced security associated with having a paper audit trail; disadvantages include lower ease of use, such as their limited ability to accommodate voters with disabilities.

Voting system performance is a function of two very important activities: system design and development—including the testing

that determines whether the developed system performs as designed—and system implementation. One critical input to the design and development process is the quality of the specified system requirements as embodied in applicable standards. For voting technology, these standards have historically been problematic, and they are now a focus of the EAC. Critical inputs to the system implementation process are having people with the requisite knowledge and skills to operate and use the system, and having well-defined and understood processes governing this operation and use. Both are also areas of focus by the commission.

Looking toward to the upcoming 2004 national election and beyond, the challenges confronting local jurisdictions in using electronic voting systems are not unlike those facing any technology user. These challenges include (1) performing those security, testing, and maintenance activities needed to minimize risk and adequately ensure that the system operates as intended; (2) managing the system, the people who interact with the system, and the processes that govern this interaction as interrelated and interdependent parts; (3) having reliable measures and objective data to know whether the system is meeting the needs of the jurisdiction's user community (both the voters and the persons who administer the elections); and (4) making choices about future system changes in light of whether a given system will provide benefits over its useful life commensurate with life-cycle costs, and ensuring that these costs are affordable.

Background

Following the 2000 national elections, we performed a comprehensive series of reviews covering our nation's election process, in which we identified a number of challenges. These reviews culminated in a capping report that summarized this work and provided the Congress with a framework for considering options for election administration reform.[3] Our reports and

[3] U.S. General Accounting Office, *Elections: A Framework for Evaluating Reform Proposals*, GAO-02-90 (Washington, D.C.: Oct. 15, 2001).

framework were among the resources that the Congress drew on in enacting the Help America Vote Act (HAVA) of 2002,[4] which provided guidance for fundamental election administration reform. Among other things, the act authorizes $3.86 billion in funding over several fiscal years for programs to replace punch card and mechanical lever voting equipment, improve election administration, improve accessibility, train poll workers, and perform research and pilot studies. It also created the EAC to oversee the election administration reform process. Since the act's passage, a number of voting jurisdictions have replaced their older voting equipment with direct recording electronic systems. At the same time, concerns have been raised about the use of these systems; some have reported that these systems have serious security vulnerabilities and that the embedded controls are not sufficient to ensure the integrity of the election process. The EAC, which began operations in January 2004, held a public hearing in May 2004 at which a major topic was the security and reliability of electronic voting devices.

GAO Work Following the 2000 Elections Provided a Framework for Election Administration Reform

At the request of congressional leaders, committees, and members, we conducted an extensive body of work in the wake of the 2000 elections, which culminated in seven reports addressing a range of election-related topics.

First, we reviewed the constitutional framework for the administration of elections, as well as major federal statutes enacted in this area.[5] We reported that the constitutional framework for elections includes both state and federal roles. States are responsible for the administration of both their own elections and federal elections, but the Congress has enacted laws in several major areas of the voting process, including the timing of federal

[4] Pub. L. No. 107-252.

[5] U.S. General Accounting Office, *Elections: The Scope of Congressional Authority in Election Administration*, GAO-01-470 (Washington, D.C.: Mar. 13, 2001).

elections, voter registration, and absentee voting requirements. Congressional authority to legislate in this area derives from various constitutional sources, depending upon the type of election. For federal elections, the Congress has constitutional authority over both congressional and presidential elections.

Second, we examined voting assistance for military and overseas voters.[6] We reported that although tools are available for such voters, many potential voters were unaware of them, and many military and overseas voters believed it was challenging to understand and comply with state requirements and local procedures for absentee voting. In addition, although information was not readily available on the precise number of military and overseas absentee votes that were disqualified in the 2000 general election and the reasons for disqualification, we found through a national telephone survey that almost two-thirds of the disqualified absentee ballots were rejected because of lateness or errors in completion of the envelope or form accompanying the ballot. We recommended that the Secretaries of Defense and State improve (1) the clarity and completeness of service guidance, (2) voter education and outreach programs, (3) oversight and evaluation of voting assistance efforts, and (4) sharing of best practices. The Departments of Defense and State agreed with our overall findings and recommendations, and as of May 2004, the recommendations had largely been implemented.

Third, we investigated whether minorities and disadvantaged voters were more likely to have their votes not counted because the voting method they used was less reliable than that of affluent white voters.[7] According to our results, the state in which counties were located had more effect on the number of uncounted presidential votes than did counties' demographic characteristics or voting method. State differences accounted for 26 percent of the total

[6] U.S. General Accounting Office, *Elections: Voting Assistance to Military and Overseas Citizens Should Be Improved*, GAO-01-1026 (Washington, D.C.: Sept. 28, 2001).

[7] U.S. General Accounting Office, *Elections: Statistical Analysis of Factors That Affected Uncounted Votes in the 2000 Presidential Election*, GAO-02-122 (Washington, D.C.: Oct. 15, 2001).

variation in uncounted presidential votes across counties.[8] County demographic characteristics accounted for 16 percent of the variation (counties with higher percentages of minority residents tended to have higher percentages of uncounted presidential votes, while counties with higher percentages of younger and more educated residents tended to have lower percentages of uncounted presidential votes), and voting equipment accounted for 2 percent of the variation.

Fourth, in a review of voting accessibility for voters with disabilities,[9] we found that all states had provisions addressing voting by people with disabilities, but these provisions varied greatly. Federal law requires that voters with disabilities have access to polling places for federal elections, with some exceptions.[10] All states provided for one or more alternative voting methods or accommodations intended to facilitate voting by people with disabilities. In addition, states and localities had made several efforts to improve voting accessibility for voters with disabilities, such as modifying polling places, acquiring new voting equipment, and expanding voting options, but state and county election officials surveyed cited various challenges to improving access. We concluded that given the limited availability of accessible polling places, other options that could allow more voters with disabilities to vote at a polling place on election day include reassigning them to other, more accessible polling places or creating accessible superprecincts in which voters from more than one precinct could all vote in the same building.

Fifth, we reported on the status and use of voting equipment standards developed by the Federal Election Commission (FEC).[11]

[8] State differences may have included such factors as statewide voter education efforts, state standards for determining what is a valid vote, the use of straight party ballots, the number of candidates on the ballot, the use of provisional ballots, and the extent to which absentee or early voting occurred.

[9] U.S. General Accounting Office, *Voters with Disabilities: Access to Polling Places and Alternative Voting Methods*, GAO-02-107 (Washington, D.C.: Oct. 15, 2001).

[10] 42 U.S.C. Sec. 1973ee-1.

[11] U.S. General Accounting Office, *Elections: Status and Use of Federal Voting Equipment Standards*, GAO-02-52 (Washington, D.C.: Oct. 15, 2001).

These standards define minimum functional and performance requirements, as well as minimum life-cycle management processes for voting equipment developers to follow, such as quality assurance. At the time of our review, no federal agency had explicit statutory responsibility for developing the standards; however, the FEC developed voluntary standards for computer-based systems in 1990,[12] and the Congress provided funding for this effort. Similarly, no federal agency was responsible for testing voting systems against the federal standards. Instead, the National Association of State Election Directors accredited independent test authorities to test voting systems against the standards. We noted, however, that the FEC standards had not been updated since 1990 and were consequently out of date. We suggested that the Congress consider assigning explicit federal authority, responsibility, and accountability for the standards, including their proactive and continuous update and maintenance; we also suggested that the Congress consider what, if any, federal role is appropriate regarding implementation of the standards, including the accreditation of independent test authorities and the qualification of voting systems. Both of these matters were addressed in the Help America Vote Act, which, among other things, set up the EAC to take responsibility for voluntary voting system guidelines. We also made recommendations to the FEC aimed at improving the guidelines. Before the EAC became operational, the FEC continued to update and maintain the guidelines, issuing a new version in 2002.

Sixth, we issued a report on election activities and challenges across the nation.[13] In this report, we described the operations and challenges associated with each stage of the election process, including voter registration; absentee and early voting;[14] election day administration; and vote counts, certification, and recounts. The report also provided analyses on issues associated with voting

[12] *Performance and Test Standards for Punchcard, Marksense, and Direct Recording Electronic Voting Systems* (January 1990).

[13] U.S. General Accounting Office, *Elections: Perspectives on Activities and Challenges across the Nation,* GAO-02-3 (Washington, D.C.: Oct. 15, 2001);

[14] Absentee and early voting allows eligible persons to vote in person or by mail before election day.

systems that were used in the November 2000 elections and the potential use of the Internet for voting. Among other things, we pointed out that each of the major stages of an election depends on the effective interaction of people (the election officials and voters), processes (or internal controls), and technology (registration systems, election management systems, and voting systems). We also enumerated the challenges facing election officials at all stages of the election process.

Finally, we issued a capping report that included a framework for evaluating election administration reform proposals.[16] Among other things, we observed that the constitutional and operational division of federal and state authority to conduct elections had resulted in great variability in the ways that elections are administered in the United States. We concluded that given the diversity and decentralized nature of election administration, careful consideration needed to be given to the degree of flexibility and the planned time frames for implementing new initiatives. We also concluded that in order for election administration reform to be effective, reform proposals must address all major parts of our election system—its people, processes, and technology—which are interconnected and significantly affect the election process. And finally, we provided an analytical framework for the Congress to consider in deciding on changes to the overall election process.

The Help America Vote Act Was Enacted to Strengthen the Overall Election Process

Enacted by the Congress in October 2002, the Help America Vote Act of 2002 addressed a range of election issues, including the lack of explicit federal (statutory) responsibility for developing and maintaining standards for electronic voting systems and for testing voting systems against standards.

With the far-reaching goal of improving the election process in every state, the act affects nearly every aspect of the voting process, from voting technology to provisional ballots, and from voter registration to poll worker training. In particular, the act established a program

[16] U.S. General Accounting Office, *Elections: A Framework for Evaluating Reform Proposals*, GAO-02-90 (Washington, D.C.: Oct. 15, 2001).

to provide funds to states to replace punch card and lever machine voting equipment,[16] established the EAC to assist in the administration of federal elections and provide assistance with the administration of certain federal election laws and programs, and established minimum election administration standards for the states and units of local government that are responsible for the administration of federal elections. In January 2004, the Congressional Research Service reported that disbursements to states for the replacement of older equipment and election administration improvements totaled $649.5 million.[17]

The act specifically tasked the EAC to serve as a national clearinghouse and resource for compiling election information and reviewing election procedures; for example, it is to conduct periodic studies of election administration issues to promote methods of voting and administration that are most convenient, accessible, and easy to use for all voters. Other examples of EAC responsibilities include

- developing and adopting voluntary voting system guidelines, and maintaining information on the experiences of states in implementing the guidelines and operating voting systems;
- testing, certifying, decertifying, and recertifying voting system hardware and software through accredited laboratories;
- making payments to states to help them improve elections in the areas of voting systems standards, provisional voting and voting information requirements, and computerized statewide voter registration lists; and
- making grants for research on voting technology improvements.

According to the act, reporting to the EAC will be the Technical Guidelines Development Committee, which will make

[16] The General Services Administration (GSA) is responsible for administering grants to the states to replace punch card systems and lever machines in qualifying states, including providing payments for general election administration improvements to states that apply for funds to replace voting equipment.

[17] Kevin J. Coleman and Eric A. Fischer, *Elections Reform: Overview and Issues,* Congressional Research Service RS20898 (Washington, D.C.: Jan. 21, 2004).

recommendations on voluntary voting system guidelines. The National Institute of Standards and Technology (NIST) will provide technical support to the development committee, and the NIST Director will serve as its chairman.

In December 2003, the EAC commissioners were appointed, and the EAC began operations in January 2004. According to the commission chairman, the EAC's fiscal year 2004 budget is $1.2 million, and its near-term plans focus on complying with requirements established in HAVA. In that regard, the EAC issued its first annual report to the Congress in April of this year on the status of election administration reform. The EAC also plans to issue best practices guidelines in July 2004 to increase the reliability of voting equipment and systems for the November 2004 elections. The guidelines also include guidance on recruiting and training poll workers. The commission's longer term plans include updating the voluntary voting system guidelines and improving the process for independent testing of voting systems. Toward this end, the EAC's Technical Guidelines Development Committee recently held its first meeting to develop a plan to update voluntary voting system guidelines. According to some commissioners, current operations are constrained by a lack of persons in key staff positions, including the Executive Director, General Counsel, and Inspector General.

Electronic Voting Systems Fall into Two Primary Categories

In the United States today, most votes are cast and counted by one of two types of electronic voting systems: optical scan and direct recording electronic (DRE). Two older voting technologies were also used in the 2000 elections: punch card equipment (used by about 31 percent of registered voters in 2000 and expected to be used by 19 percent in 2004) and mechanical lever voting machines (used by about 17 percent of registered voters in 2000 and expected to be 13 percent in 2004).[18] These equipment types are being

[18] Figures for the 2000 and 2004 elections are according to Election Data Services, Inc. Election Data Services, Inc., is a political consulting firm specializing in redistricting, election administration, and the analysis and presentation of census and political data.

replaced as required by provisions established in HAVA.[19] In addition, for a small minority of registered voters, votes are cast and counted manually on paper ballots.[20]

Optical Scan Systems

Optical scan voting systems use electronic technology to tabulate paper ballots. Although optical scan technology has been in use for decades for such tasks as scoring standardized tests, it was not applied to voting until the 1980s. In 2000, about 31 percent of registered voters voted on optical scan systems. In the 2004 election, according to Election Data Services, Inc., about 32 percent of registered voters will use optical scan voting equipment.

For voting, an optical scan system is made up of computer-readable ballots, appropriate marking devices, privacy booths, and a computerized tabulation device. The ballot, which can be of various sizes, lists the names of the candidates and the issues. Voters record their choices using an appropriate writing instrument to fill in boxes or ovals, or to complete an arrow next to the candidate's name or the issue. The ballot includes a space for write-ins to be placed directly on the ballot.

Optical scan ballots are tabulated by optical-mark-recognition equipment (see fig. 1), which counts the ballots by sensing or reading the marks on the ballot. Ballots can be counted at the polling place—this is referred to as precinct-count optical scan[21]—or

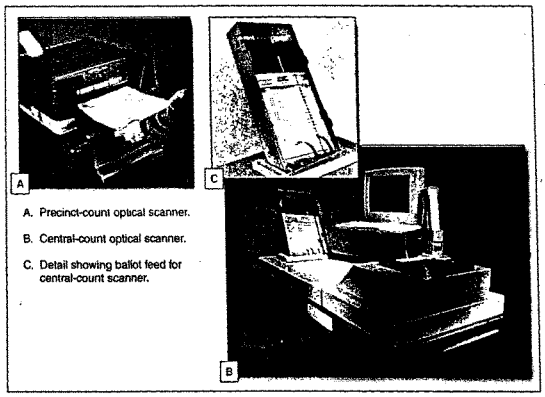
[19] Pub. L. 107-252, Sec. 102, provides federal funds to states for the systematic removal and replacement of punch card voting systems and lever voting systems in time for the regularly scheduled general election for federal offices to be held in November 2004; states that receive a certified waiver may extend their replacement time frame until the first election for federal office after January 1, 2006.

[20] We reported that about 1 percent of registered voters used manually counted paper ballots in the 2000 elections. Election Data Services, Inc., reports that about 0.6 percent will use this method in the 2004 elections.

[21] Precinct-count optical scan equipment sits on a ballot box with two compartments for scanned ballots—one for accepted ballots (i.e., those that are properly filled out) and one for rejected ballots (i.e., blank ballots, ballots with write-ins, or those accepted because of a forced override). In addition, an auxiliary compartment in the ballot box is used for storing ballots if an emergency arises (e.g., loss of power or machine failure) that prevents the ballots from being scanned.

at a central location. If ballots are counted at the polling place, voters or election officials put the ballots into the tabulation equipment, which tallies the votes; these tallies can be captured in removable storage media that are transported to a central tally location, or they can be electronically transmitted from the polling place to the central tally location. If ballots are centrally counted, voters drop ballots into sealed boxes, and election officials transfer the sealed boxes to the central location after the polls close, where election officials run the ballots through the tabulation equipment.

Figure 1: Precinct-Count Optical Scan Tabulator and Central-Count Optical Scan Tabulator



A. Precinct-count optical scanner.

B. Central-count optical scanner.

C. Detail showing ballot feed for central-count scanner.

Source: Equipment vendors.

Software instructs the tabulation equipment to assign each vote (i.e., to assign valid marks on the ballot to the proper candidate or issue). In addition to identifying the particular contests and candidates, the software can be configured to capture, for example, straight party voting and vote-for-no-more-than-N contests. Precinct-based optical scanners can also be programmed to detect overvotes (where the voter votes for two candidates for one office, for example,

invalidating the vote) and undervotes (where the voter does not vote for all contests or issues on the ballot) and to take some action in response (rejecting the ballot, for instance). In addition, optical scan systems often use vote-tally software to tally the vote totals from one or more vote tabulation devices.

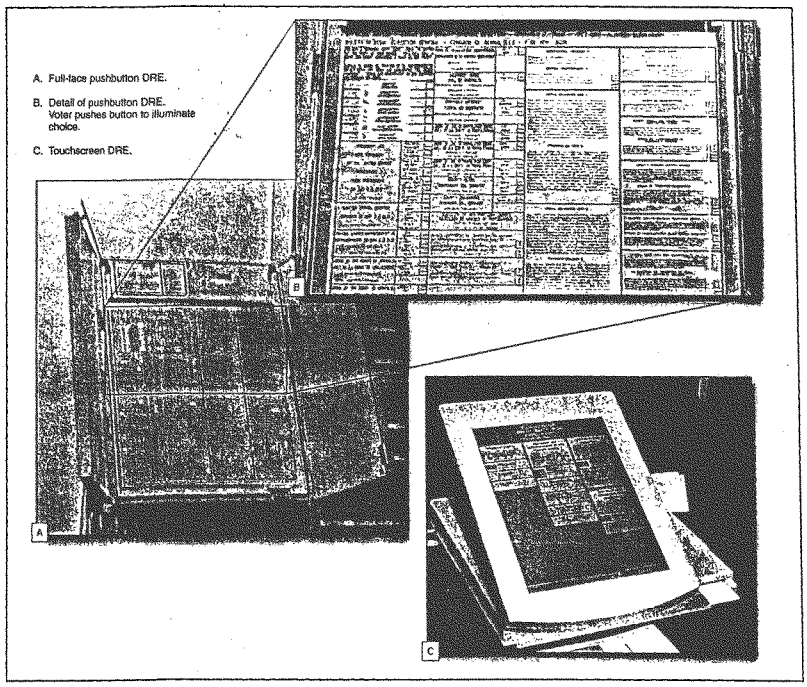
If election officials program precinct-based optical scan systems to detect and reject overvotes and undervotes, voters can fix their mistakes before leaving the polling place. However, if voters are unwilling or unable to correct their ballots, a poll worker can manually override the program and accept the ballot, even though it has been overvoted or undervoted. If ballots are tabulated centrally, voters do not have the opportunity to correct mistakes that may have been made.

Direct Recording Electronic Systems

First introduced in the 1970s, DREs capture votes electronically, without the use of paper ballots. In the 2000 election, about 12 percent of voters used this type of technology. In the 2004 election, according to Election Data Services, Inc., about 29 percent of registered voters will use this voting technology.

DREs come in two basic types, pushbutton or touchscreen, the pushbutton being the older technology; during the 2000 elections, pushbutton DREs were the most prevalent of the two types. The two types vary considerably in appearance (see fig. 2). Pushbutton DREs are larger and heavier than touchscreens.

Figure 2: DRE Pushbutton and DRE Touchscreen



Source: Local election officials and equipment vendor.

Pushbutton and touchscreen units also differ significantly in the way they present ballots to the voter. With the pushbutton, all ballot information is presented on a single "full-face" ballot. For example,

a ballot may have 50 buttons on a 3 by 3 foot ballot, with a candidate or issue next to each button. In contrast, touchscreen DREs display the ballot information on an electronic display screen. For both pushbutton and touchscreen types, the ballot information is programmed onto an electronic storage medium, which is then uploaded to the machine. For touchscreens, ballot information can be displayed in color and can incorporate pictures of the candidates. Because the ballot space on a touchscreen is much smaller than on a pushbutton machine, voters who use touchscreens must page through the ballot information. Both touchscreen and pushbutton DREs can accommodate multilingual ballots.

Despite the differences, the two types have some similarities, such as how the voter interacts with the voting equipment. For pushbuttons, voters press a button next to the candidate or issue, which then lights up to indicate the selection. Similarly, voters using touchscreens make their selections by touching the screen next to the candidate or issue, which is then highlighted. When voters are finished making their selections on a touchscreen or a pushbutton DRE, they cast their votes by pressing a final "vote" button or screen. Until they hit this final button or screen, voters can change their selections. Both types allow voters to write in candidates. While most DREs allow voters to type write-ins on a keyboard, some pushbutton types require voters to write the name on paper tape that is part of the device.

Although DREs do not use paper ballots, they do retain permanent electronic images of all the ballots, which can be stored on various media, including internal hard disk drives, flash cards, or memory cartridges. According to vendors, these ballot images, which can be printed, can be used for auditing and recounts.

Some of the newer DREs use smart card technology as a security feature. Smart cards are plastic devices—about the size of a credit card—that use integrated circuit chips to store and process data, much like a computer. Smart cards are generally used as a means to open polls and to authorize voter access to ballots. For instance, smart cards on some DREs store program data on the election and are used to help set up the equipment; during setup, election workers verify that the card received is for the proper election. Other DREs are programmed to automatically activate when the

voter inserts a smart card; the card brings up the correct ballot onto the screen. In general, the interface with the voter is very similar to that of an automatic teller machine.

Like optical scan devices, DREs require the use of software to program the various ballot styles and tally the votes, which is generally done through the use of memory cartridges or other media. The software is used to generate ballots for each precinct within the voting jurisdiction, which includes defining the ballot layout, identifying the contests in each precinct, and assigning candidates to contests. The software is also used to configure any special options, such as straight party voting and vote-for-no-more-than-N contests. In addition, for pushbutton types, the software assigns the buttons to particular candidates and, for touchscreens, the software defines the size and location on the screen where the voter makes the selection. Vote-tally software is often used to tally the vote totals from one or more units.

DREs offer various configurations for tallying the votes. Some contain removable storage media that can be taken from the voting device and transported to a central location to be tallied. Others can be configured to electronically transmit the vote totals from the polling place to a central tally location.

DREs are designed not to allow overvotes; for example, if a voter selects a second choice in a two-way race, the first choice is deselected. In addition to this standard feature, different types offer a variety of options, including many aimed at voters with disabilities, that jurisdictions may choose to purchase. In our 2001 work, we cited the following features as being offered in some models of DRE:

- *A "no-vote" option.* This option helps avoid unintentional undervotes. This provides the voter with the option to select "no vote (or abstain)" on the display screen if the voter does not want to vote on a particular contest or issue.
- *A "review" feature.* This feature requires voters to review each page of the ballot before pressing the button to cast the vote.
- *Visual enhancements.* Visual enhancements include color highlighting of ballot choices, candidate pictures, etc.

- *Accommodations for voters with disabilities.* Examples of options for voters who are blind include Braille keyboards and audio interfaces.[22] At least one vendor reported that its DRE accommodates voters with neurological disabilities by offering head movement switches and "sip and puff" plug-ins.[23] Another option is voice recognition capability, which allows voters to make selections orally.
- *An option to recover spoiled ballots.* This feature allows voters to recast their votes after their original ballots are cast. For this option, every DRE at the poll site would be connected to a local area network. A poll official would void the original "spoiled" ballot through the administrative workstation that is also connected to the local area network. The voter could then cast another ballot.
- *An option to provide printed receipts.* In this case, the voter would receive a paper printout or ballot when the vote is cast. This feature is intended to provide voters and/or election officials with an opportunity to check what is printed against what is recorded and displayed. It is envisioned that procedures would be in place to retrieve the paper receipts from the voters so that they could not be used for vote selling. Some DREs also have an infrared "presence sensor" that is used to control the receipt printer in the event the voter is allowed to keep the paper receipt; if the voter leaves without taking the receipt, the receipt is pulled back into the printer.

Expanded Use of Electronic Voting Systems Has Raised Concerns

As older voting equipment has been replaced with newer electronic voting systems over the last 2 years, the debate has shifted from hanging chads and butterfly ballots to vulnerabilities associated with DREs. Problems with these devices in recent elections have arisen in various states. For example:

[22] According to spokespersons for national advocacy groups for people with disabilities, only a small percentage of blind people have the Braille proficiency needed to vote using a Braille ballot.

[23] Using a mouth-held straw, the voter issues switch commands—hard puff, hard sip, soft puff, and soft sip—to provide signals or instructions to the voting machine.

- Six DRE units used in two North Carolina counties lost 436 ballots cast in early voting for the 2002 general election because of a software problem, according to a February 9, 2004, report in *Wired News*. The manufacturer said that problems with the firmware of its touchscreen machines led to the lost ballots. The state was trying out the machines in early voting to determine if it wanted to switch from the optical scan machines it already owned to the new touchscreen systems.
- According to a January 2004 report in *Wired News*, blank ballots were recorded for 134 voters who signed in and cast ballots in Broward County, Florida. These votes represented about 1.3 percent of the more than 10,000 people who voted in the race for a state house representative.
- *USA Today* reported that four California counties suffered from problems with DREs in a March 2004 election, including miscounted ballots, delayed polling place openings, and incorrect ballots. In San Diego County, about one-third of the county's polling places did not open on time because of battery problems caused by a faulty power switch.

Additionally, serious questions are being raised about the security of DREs. Some state that their use could compromise the integrity of the election process and that these devices need auditing mechanisms, such as receipt printers that would provide a paper audit trail and allow voters to confirm their choices.[24] Among these critics are computer scientists, citizens groups, and legislators.

For example, computer scientists from Johns Hopkins and Rice Universities released a security analysis of software from a DRE of a major vendor, concluding that the code had serious security flaws that could permit tampering.[25] Other computer scientists, while

[24] Stanford University computer science professor David Dill was reported as saying "All of this just underscores the need for voting machines to have a paper trail." Dill runs Verified Voting, a group that is urging election officials and legislators to mandate voter-verified paper ballots as audit tools.

[25] Tadayoshi Kohno, Adam Stubblefield, Aviel D. Rubin, and Dan S. Wallach, *Analysis of an Electronic Voting System*, Johns Hopkins University Information Security Institute, TR-2003-19 (July 2003).

agreeing that the code contained security flaws, criticized the study for not recognizing how standard election procedures can mitigate these weaknesses. Following the Johns Hopkins and Rice study, the State of Maryland contracted with both SAIC and RABA Technologies to study the same DRE equipment. The SAIC study found that the equipment, as implemented in Maryland, poses a security risk.[26] Similarly, RABA identified vulnerabilities associated with the equipment.[27] An earlier Caltech/MIT study[28] noted that despite security strengths of the election process in the United States,[29] current trends in electronic voting are weakening those strengths and introducing risks; according to this study, properly designed and implemented electronic voting systems could actually improve, rather than diminish, security.

Citizen advocacy groups are also taking action. For example, according to an April 21, 2004, press release from the Campaign for Verifiable Voting in Maryland, the group filed a lawsuit against the Maryland State Board of Elections to force election officials to decertify the DRE machines used in Maryland until the manufacturer remedies security vulnerabilities and institutes a paper audit trail.

Legislators and other officials are also responding to the issues. In at least 20 states, according to the Associated Press, legislation has been introduced requiring a paper record of every vote cast.[30] Following the problems in California described above, the California

[26] Science Applications International Corporation, *Risk Assessment Report*, SAIC-6099-2003-261 (Sept. 2, 2003).

[27] RABA Technologies, LLC, *Trusted Agent Report* (Jan. 20, 2004).

[28] Caltech/MIT Voting Technology Project, *Voting: What Is, What Could Be* (July 2001). (http://www.vote.caltech.edu/Reports/2001report.html)

[29] These strengths include the openness of the election process, which permits observation of counting and other aspects of election procedure; the decentralization of elections and the division among different levels of government and groups of people; equipment that produces "redundant trusted recordings" of votes; and the public nature and control of the election process.

[30] Rachel Konrad, *Legislators Wary of Electronic Voting*, The Associated Press (Apr. 24, 2004).

Secretary of State banned the use of one model of touchscreen DREs and conditionally decertified other similar models. According to the *New York Times*, these models represented 14,000 and 28,000 units, respectively.[31] The Secretary recommended that the state Attorney General consider taking civil and criminal action against the manufacturer for "fraudulent actions." The decision followed the recommendations of the state's Voting Systems and Procedures Panel, which urged the Secretary of State to prohibit the four counties that experienced difficulties from using their touchscreen units in the November 2004 election. The panel reported that the manufacturer did not obtain federal approval of the model used in the four affected counties and installed software that had not been approved by the Secretary of State. It also noted that problems with the systems prevented an unspecified number of voters from casting ballots. In addition, two California state senators drafted a bill to prohibit the use of any DRE voting system without a paper trail in the 2004 general election; they planned to introduce the bill if the Secretary of State did not act.[32] In June 2004, the Secretary of State proposed standards for the creation and testing of paper trails for electronic voting systems.

At the federal level, several bills have been introduced in response to concerns about electronic voting technology. One of the bills,[33] the Voter Confidence and Increased Accessibility Act of 2003 (H.R. 2239), if enacted, would require that voting machines used in elections for federal office produce paper audit trails so that voters and election officials can check accuracy.[34] Among other provisions,

[31] John Schwartz, "High-Tech Voting Is Banned in California," *New York Times* (May 1, 2004).

[32] Tim Reiterman, Stuart Pfeifer, and Jean O. Pasco, "State Is Urged to Ban Vote Machine," *Los Angeles Times* (Apr. 24, 2004).

[33] Other related measures include S 1986, Protecting American Democracy Act of 2003; S 2045, Secure and Verifiable Electronic Voting Act of 2004; S2313, Restore Elector Confidence in Our Representative Democracy Act of 2004; and S 2437, Voting Integrity and Verification Act of 2004.

[34] A companion to this bill in the Senate is S 1980.

the bill would also ban the use of undisclosed software[35] and wireless communications devices in voting systems.

Some of the concerns regarding DREs were raised at a public hearing held by the EAC on May 5, 2004. The purpose of the hearing was to permit the EAC to receive information on the use, security, and reliability of electronic voting devices. It included panels of technology and standards experts, vendors of voting systems, state election administrators, and citizen advocacy groups. One expert testified that electronic voting systems are flawed because they do not permit voters to verify that their votes were recorded correctly and they do not permit a public vote count. Others stated that the systems can be made secure only by the addition of a voter-verifiable paper ballot. On the other hand, the election administrators on the panel described positive experiences with DREs, and representatives of voters with disabilities supported the use of DREs because of their accessibility features.[36]

Despite Their Vital Role, Voting Systems Are Only One Aspect of the Larger Election Process

Electronic voting systems represent one of many important components in the overall election process. This process is made up of several stages, with each stage consisting of key people, process, and technology variables. Many levels of government are involved, including over 10,000 jurisdictions with widely varying characteristics.

[35] The bill states that any voting system containing or using software shall disclose the source code of that software to the EAC, and the EAC shall make that source code available for inspection, upon request, to any citizen.

[36] Following this hearing, which focused on DRE voting systems, the EAC held a second hearing on June 3, 2004, to focus on three other voting technologies: punch card and lever machines and optical scan voting equipment. The hearing addressed best practices, problems, and transitional issues associated with these systems. A major emphasis of the hearing was to identify practices that could be published and used by local election officials in preparation for the election of November 2, 2004.

In the U.S. election process, all levels of government share responsibility. At the federal level, the Congress has authority under the Constitution to regulate presidential and congressional elections and to enforce prohibitions against specific discriminatory practices in all elections—federal, state, and local.[37] It has passed legislation affecting the administration of state elections that addresses voter registration,[38] absentee voting,[39] accessibility provisions for the elderly and handicapped,[40] and prohibitions against discriminatory practices.[41] The Congress does not have general constitutional authority over the administration of state and local elections.

At the state level, the states are responsible for the administration of both their own elections and federal elections. States regulate the election process, including, for example, adoption of voluntary voting system guidelines, testing of voting systems, ballot access, registration procedures, absentee voting requirements, establishment of voting places, provision of election day workers, and counting and certification of the vote. In fact, the U.S. election process can be seen as an assemblage of 51 somewhat distinct election systems—those of the 50 states and the District of Columbia.

Further, although election policy and procedures are legislated primarily at the state level, states typically have decentralized this process so that the details of administering elections are carried out at the city or county levels, and voting is done at the local level. As we reported in 2001, local election jurisdictions number more than 10,000, and their size varies enormously—from a rural county with

[37] For more information on the role of the federal government in the administration of elections, see U.S. General Accounting Office, *Elections: The Scope of Congressional Authority in Election Administration*, GAO- 01-470 (Washington, D.C.: Mar. 13, 2001).

[38] National Voter Registration Act of 1993, commonly known as the "Motor Voter" Act; 42 U.S.C. 1973gg to 1973gg-10.

[39] Uniformed and Overseas Citizens Absentee Voting Act (1986); 42 U.S.C. 1973ff to 1973ff-6.

[40] Voting Accessibility for the Elderly and Handicapped Act (1984); 42 U.S.C. 1973ee to 1973ee-6.

[41] Voting Rights Act of 1965, 42 U.S.C. 1973 to 1973bb-1.

about 200 voters to a large urban county such as Los Angeles County, where the total number of registered voters for the 2000 elections exceeded the registered voter totals in 41 states.

The size of a voting jurisdiction significantly affects the complexity of planning and conducting the election, as well as the method used to cast and count votes. In our 2001 work, we quoted the chief election official in a very large voting jurisdiction: "the logistics of preparing and delivering voting supplies and equipment to the county's 4,963 voting precincts, recruiting and training 25,000 election day poll workers, preparing and mailing tens of thousands of absentee ballot packets daily and later signature verifying, opening and sorting 521,180 absentee ballots, and finally, counting 2.7 million ballots is extremely challenging."

The specific nature of these challenges is affected by the voting technology that the jurisdiction uses. For example, jurisdictions using DRE systems may need to manage the electronic transmission of votes or vote counts; jurisdictions using optical scan technology need to manage the paper ballots that this technology reads and tabulates. Jurisdictions using optical scan technology may also need to manage electronic transmissions if votes are counted at various locations and totals are electronically transmitted to a central tally point.

Another variable is the diversity of languages within a jurisdiction. In November 2000, Los Angeles County, for instance, provided ballots in Spanish, Chinese, Korean, Vietnamese, Japanese, and Tagalog, as well as English. No matter what technology is used, jurisdictions may need to provide ballot translations; however, the logistics of printing paper materials in a range of languages, as would be required for optical scan technology, is different from the logistics of programming translations into DRE units.

Some states do have statewide election systems so that every voting jurisdiction uses similar processes and equipment, but others do not. For instance, we reported in 2001 that in Pennsylvania, local election officials told us that there were 67 counties and

consequently 67 different ways of handling elections.[42] In some states, state law prescribes the use of common voting technology throughout the state, while in other states local election officials generally choose the voting technology to be used in their precincts, often from a list of state-certified options.

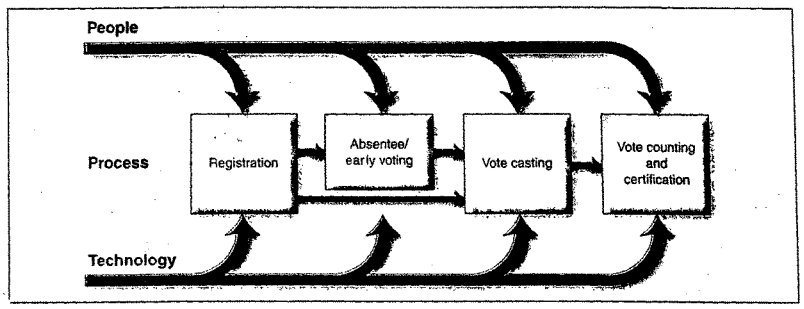
Whatever the jurisdiction and its specific characteristics, administering an election is a year-round activity, involving varying sets of people to carry out processes at different stages. These stages generally consist of the following:

- *Voter registration.* Among other things, local election officials register eligible voters and maintain voter registration lists, including updates to registrants' information and deletions of the names of registrants who are no longer eligible to vote.
- *Absentee and early voting.* This type of voting allows eligible persons to vote in person or by mail before election day. Election officials must design ballots and other systems to permit this type of voting, as well as educating voters on how to vote by these methods.
- *The conduct of an election.* Election administration includes preparation before election day, such as local election officials arranging for polling places, recruiting and training poll workers, designing ballots, and preparing and testing voting equipment for use in casting and tabulating votes, as well as election day activities, such as opening and closing polling places and assisting voters to cast votes.
- *Vote counting.* At this stage, election officials tabulate the cast ballots; determine whether and how to count ballots that cannot be read by the vote counting equipment; certify the final vote counts; and perform recounts, if required.

As shown in figure 3, each stage of an election involves people, processes, and technology.

[42] GAO-02-3.

Figure 3: Stages of Election Process



Source: GAO analysis.

Electronic voting systems are primarily involved in the last two stages, during which votes are cast and counted. However, the type of system that a jurisdiction uses may affect earlier stages. For example, in a jurisdiction that uses optical scan systems, paper ballots like those used on election day may be mailed in the absentee voting stage. On the other hand, a jurisdiction that uses DRE technology would have to make a different provision for absentee voting.

Electronic Voting Systems' Performance Can Be Judged on Several Attributes

Although the current debate concerning electronic voting systems primarily relates to security, other factors affecting election administration are also relevant in evaluating these systems. Ensuring the security of elections is essential to public confidence and election integrity, but officials choosing a voting system must also consider other performance factors, such as accuracy, ease of use, and efficiency, as well as cost. Accuracy refers to how frequently the equipment completely and correctly records and counts votes; ease of use refers to how understandable and

accessible the equipment is to a diverse group of voters and to election workers; and efficiency refers to how quickly a given vote can be cast and counted. Finally, equipment's life-cycle cost versus benefits is an overriding practical consideration.

Security

In conducting elections, officials must be able to assure the public that the confidentiality of the ballot is maintained and fraud prevented. In providing this assurance, the people, processes, and technology involved in the election system all play a role: the security procedures and practices that jurisdictions implement, the security awareness and training of the election workers who execute them, and the security features provided by the systems.

Election officials are responsible for establishing and managing privacy and security procedures to protect against threats to the integrity of elections.[43] These security threats include potential modification or loss of electronic voting data; loss, theft, or modification of physical ballots; and unauthorized access to software and electronic equipment. Physical access controls are required for securing voting equipment, vote tabulation equipment, and ballots; software access controls (such as passwords and firewalls[44]) are required to limit the number of people who can access and operate voting devices, election management software, and vote tabulation software. In addition, election processes are designed to ensure privacy by protecting the confidentiality of the vote: physical screens are used around voting stations, and poll workers are present to prevent voters from being watched or coerced while voting.

[43] We have described an effective security program as including, at a minimum, (1) assigning responsibility for security, (2) assessing security risks and vulnerabilities and implementing both manual and technology-based security measures to prevent or counter these risks, and (3) periodically reviewing the controls to ensure their appropriateness. For more information, see U.S. General Accounting Office, *Executive Guide: Information Security Management*, GAO/AIMD-98-68 (Washington, D.C.: May 1998).

[44] A firewall is a hardware or software component that protects computers or networks from attacks by outside network users by blocking and checking all incoming traffic.

Examples of security controls that are embedded in the technology include the following:

- *Access controls.* Election workers may have to enter user names and passwords to access voting systems and software, so that only authorized users can make modifications. On election day, voters may need to provide a smart card or token[45] to DRE units.
- *Encryption.* To protect the confidentiality of the vote, DREs use encryption technology to scramble the votes cast so that the votes are not stored in the same order in which they were cast. In addition, if vote totals are electronically transmitted, encryption is used to protect the vote count from compromise by scrambling it before it is transmitted over telephone wires and unscrambling it once it is received.
- *Physical controls.* Hardware locks and seals protect against unauthorized access to the voting device once it has been prepared for the election (e.g., once the vote counter is reset, the unit is tested, and ballots are prepared).
- *Audit trails.* Audit trails provide documentary evidence to recreate election day activity, such as the number of ballots cast (by each ballot configuration or type) and candidate vote totals for each contest. Audit trails are used for verification purposes, particularly in the event that a recount is demanded. With optical scan systems, the paper ballots provide an audit trail. Since not all DREs provide a paper record of the votes, election officials may rely on the information that is collected by the DRE's electronic memory. Part of the debate over the assurance of integrity that DREs provide revolves around the reliability of this information.
- *Redundant storage.* Redundant storage media in DREs provide backup storage of votes cast or vote counts to facilitate recovery of voter data in the event of power or system failure.

The particular features offered by DRE and optical scan equipment differ by vendor make and model as well as the nature of the technology. DREs generally offer most of the features, but there is

[45] In security systems, a token is small device that displays a constantly changing identification code; smart cards may perform a similar function.

debate about the implementation of these features and the adequacy of the access controls and audit trails that this technology provides. If DREs use tokens or smart cards to authenticate voters, these tokens must also be physically protected and may require software security protection. For optical scan systems, redundant storage media may not be required, but software and physical access controls may be associated with tabulation equipment and software, and if vote tallies are transmitted electronically, encryption may also be used. In addition, since these systems use paper ballots, the audit trail is clearer, but physical access to ballots after they are cast must be controlled. The physical and process controls used to protect paper ballots include ballot boxes as well as the procedures implemented to protect the boxes if they need to be transported, to tabulate ballots, and to store counted ballots for later auditing and possible recounts.

Accuracy

Ensuring that votes are accurately recorded and tallied is an essential attribute of any voting equipment. Without such assurance, both voter confidence in the election and the integrity and legitimacy of the outcome of the election are at risk. The importance of an accurate vote count increases with the closeness of the election. Both optical scan and DRE systems are claimed to be highly accurate. In 2001, our vendor survey showed virtually no differences in vendor representations of the accuracy of DRE and optical scan voting equipment, measured in terms of how accurately the equipment counted recorded votes.[46] Vendors of optical scan equipment reported accuracy rates of between 99 and 100 percent, with vendors of DREs reporting 100 percent accuracy.

As we reported in 2001, although 96 percent of local election jurisdictions were satisfied with the performance of their voting equipment during the 2000 election, according to our mail survey, only about 48 percent of jurisdictions nationwide collected data on

[46] GAO-02-3.

the accuracy of their voting equipment for the election.[47] Further, it was unclear whether jurisdictions actually had meaningful performance data. Of those local election jurisdictions that we visited that stated that their voting equipment was 100 percent accurate, none was able to provide actual data to substantiate these statements. Similarly, according to our mail survey, only about 51 percent of jurisdictions collected data on undervotes, and about 47 percent collected data on overvotes for the November 2000 election.[48]

Although voting equipment may be designed to count votes as recorded with 100 percent accuracy, how frequently the equipment counts votes as intended by voters is a function not only of equipment design, but also of the interaction of people and processes. These people and process factors include whether, for example,

- technicians have followed proper procedures in testing and maintaining the system,
- voters followed proper procedures when using the system,
- election officials have provided voters with understandable procedures to follow, and
- poll workers properly instructed and guided voters.

As indicated earlier, various kinds of errors can lead to voter intentions not being captured when ballots are counted. Avoiding or compensating for these errors may involve solutions based on technology, processes, or both. For example, DREs are designed to prevent overvoting; however, overvoting can also be prevented by a procedure to check optical scan ballots for overvotes before the voter leaves the polls, which can be accomplished by a precinct-based tabulator or by other means.

[47] GAO-02-3. Confidence intervals were calculated at the 95 percent confidence level. Unless otherwise noted, all estimates from GAO's mail survey have a confidence interval of plus or minus 4 percentage points or less; all estimates from GAO's telephone survey have a confidence interval of plus or minus 11 percentage points or less.

[48] DREs do not allow overvotes, so the figure for overvotes does not include jurisdictions that used DREs.

Ease of Use

Like accuracy, ease of use (or user friendliness) largely depends on how voters interact with the voting system, physically and intellectually. This interaction, commonly referred to as the human/machine interface, is a function of the system design, the processes established for its use, and user education and training. Among other things, how well jurisdictions design ballots and educate voters on the use of voting equipment affects how easy voters find the system to use. In the 2000 elections, for example, ballots for some optical scan systems were printed on both sides, so that some voters failed to vote one of the sides. This risk could be mitigated by clear ballot design and by explicit instructions, whether provided by poll workers or voter education materials. Thus, ease of use affects accuracy (i.e., whether the voter's intent is captured), and it can also affect the efficiency of the voting process (confused voters take longer to vote).

Accessibility to diverse types of voters, including those with disabilities, is a further aspect of ease of use. As described earlier, DREs offer more options for voters with disabilities, as they can be equipped with a number of aids to voters with disabilities. However, these options increase the expense of the units, and not all jurisdictions are likely to opt for them. Instead of technological solutions, jurisdictions may establish special processes for voters with disabilities, such as allowing them to be assisted to cast their votes; this workaround can, however, affect the confidentiality of the vote.

Efficiency

Efficiency—the speed of casting and tallying votes—is an important consideration for jurisdictions not only because it influences voter waiting time and thus potentially voter turnout, but also because it affects the number of voting systems that a jurisdiction needs to acquire and maintain, and thus the cost.

Efficiency can be measured in terms of the number of people that the equipment can accommodate within a given time, how quickly the equipment can count votes, and the length of time that voters need to wait. With DREs, the vote casting and counting functions are virtually inseparable, because the ballot is embedded in the

voting equipment. Accordingly, for DREs efficiency is generally measured in terms of the number of voters that each machine accommodates on election day. In 2001, vendors reported that the number of voters accommodated per DRE ranges from 200 to 1,000 voters per system per election day.

With optical scan systems, in contrast, vote casting and counting are separate activities, since the ballot is a separate medium—a sheet of paper or a computer card—which once completed is put into the vote tabulator. As a result, the efficiency of optical scan equipment is generally measured in terms of the speed of count (i.e., how quickly the equipment counts the votes on completed ballots). Complicating this measurement is the fact that efficiency differs depending on whether central-count or precinct-based tabulators are used. Central-count equipment generally counts more ballots per hour because it is used to count the ballots for an entire jurisdiction, rather than an individual polling site. For central-count optical scan equipment, 10 vendors reported speed of count ranges from 9,000 to 24,000 ballots per hour. For precinct-count optical scan equipment, vendors generally did not provide specific speed of count data, but they stated that one machine is generally used per polling site.

Generalizations about the effect of technology on wait times are difficult. In 2001, our mail survey found that 84 percent of jurisdictions nationwide were satisfied with the amount of voter wait time at the polling place during the November 2000 election, but that 13 percent of jurisdictions considered long lines at the polling places to be a major problem.[49] However, we estimated that only 10 percent of jurisdictions nationwide collected information on the average amount of time that it took voters to vote. We were told by some jurisdictions that the length of time voters must wait is affected by ballots that include many races and issues. Some jurisdictions reported that their ballots were so long that it took voters a long time in the voting booth to read them and vote. As a result, lines backed up, and some voters had to wait for over an hour to cast their votes. Officials in one jurisdiction said that their voters experienced long wait times in part because redistricting caused

[49] GAO-02-3.

confusion among voters, who often turned up at the wrong polling places. As these examples show, the voting system used is not always a major factor in voter wait times. However, processes that do depend on the system may affect the time that a voter must spend voting. For example, in precincts that use precinct-level counting technology for optical scan ballots, voters may place their ballots in the automatic feed slot of the tabulator. This process can add to voting time if the tabulator is designed to reject ballots that are undervoted, overvoted, or damaged, and the voter is given the opportunity to correct the ballot.

Cost

Generally, buying DRE units is more expensive than buying optical scan systems. For a broad picture, consider the comparison that we made in 2001 of the costs of purchasing new voting equipment for local election jurisdictions based on three types of equipment: central-count optical scan equipment, precinct-count optical scan equipment, and touchscreen DRE units.[50] Based on equipment cost information available in August 2001, we estimated that purchasing optical scan equipment that counted ballots at a central location would cost about $191 million.[51] Purchasing an optical scan counter for each precinct that could notify voters of errors on their ballots would cost about $1.3 billion. Purchasing touchscreen DRE units for each precinct, including at least one unit per precinct that could accommodate blind, deaf, and paraplegic voters, would cost about $3 billion.

For a given jurisdiction, the particular cost involved will depend on the requirements of the jurisdiction, as well as the particular equipment chosen. Voting equipment costs vary among types of voting equipment and among different manufacturers and models of the same type of equipment. For example, in 2001, DRE touchscreen unit costs ranged from $575 to $4,500. Similarly, unit costs for precinct-count optical scan equipment ranged from $4,500 to $7,500. Among other things, these differences can be attributed to

[50] GAO-02-3.

[51] Cost estimates include capital costs only.

differences in what is included in the unit cost as well as differences in the characteristics of the equipment.

In addition to the equipment unit cost, an additional cost for jurisdictions is the software that operates the equipment, prepares the ballots, and tallies the votes (and in some cases, prepares the election results reports). Our vendor survey showed that although some vendors included the software cost in the unit cost of the voting equipment, most priced the software separately. Software costs for DRE and optical scan equipment could run as high as $300,000 per jurisdiction. The higher costs were generally for the more sophisticated software associated with election management systems. Because the software generally supported numerous equipment units, the software unit cost varied depending on the number of units purchased or the size of the jurisdiction.

Other factors affecting the acquisition cost of voting equipment are the number and types of peripherals required. In general, DREs require more peripherals than do optical scan systems, which adds to their expense. For example, some DREs require smart cards, smart card readers, memory cartridges and cartridge readers, administrative workstations, and plug-in devices (for increasing accessibility for voters with disabilities). Touchscreen DREs may also offer options that affect the cost of the equipment, such as color versus black and white screens. In addition, most DREs and all optical scan units require voting booths, and most DREs and some precinct-based optical scan tabulators offer options for modems. Precinct-based optical scan tabulators also require ballot boxes to capture the ballots after they are scanned.

Once jurisdictions acquire the voting equipment, they must also incur the cost to operate and maintain it, which can vary considerably. For example, in 2001, jurisdictions that used DREs reported a range of costs from about $2,000 to $27,000. Similarly, most jurisdictions that used optical scan equipment reported that operations and maintenance costs ranged from about $1,300 to $90,000. The higher ends of these cost ranges generally related to the larger jurisdictions. In fact, one large jurisdiction that used optical scan equipment reported that its operating costs were $545,000. In addition, the jurisdictions reported that these costs generally included software licensing and upgrades, maintenance

contracts with vendors, equipment replacement parts, and supply costs.

For decisions on whether to invest in new voting equipment, both initial capital costs (i.e., cost to acquire the equipment) and long-term support costs (i.e., operation and maintenance costs) are relevant. Moreover, these collective costs (i.e., life-cycle costs) need to be viewed in the context of the benefits the equipment will provide over its useful life. It is advisable to link these benefits directly to the performance characteristics of the equipment and the needs of the jurisdiction.

Electronic Voting System Performance Depends on System Design and Implementation

The performance of any information technology system, including electronic voting systems, is heavily influenced by a number of factors, not the least of which is the quality of the system's design and the effectiveness with which the system is implemented in an operational setting. System design and implementation, in turn, are a function of such things as how well the system's requirements are defined, how well the system is tested, and how well the people that operate and use the system understand and follow the procedures that govern their interaction with it. Our work in 2001 raised concerns about the FEC's voting system standards, and showed that practices relative to testing and implementation of voting systems varied across states and local jurisdictions.

Voting Systems Should Be Designed, Built, and Tested against Well-Defined Standards

Like that of any information technology product, the design of a voting system starts with the explicit definition of what the system is to do and how well it is to do it. These requirements are then translated into design specifications that are used to develop the system. Organizations such as the Department of Defense and the Institute of Electrical and Electronics Engineers have developed guidelines for various types of systems requirements and for the processes that are important to managing the development of any system throughout its life cycle. These guidelines address types of

product requirements (e.g., functional and performance), as well as documentation and process requirements governing the production of the system.

In the case of voting systems, the FEC had assumed responsibility for issuing standards that embodied these requirements, a responsibility that HAVA has since assigned to the EAC. The FEC standards are nevertheless still the operative standards until the EAC updates them. These FEC-issued standards apply to system hardware, software, firmware, and documentation,[52] and they span prevoting,[53] voting,[54] and postvoting activities.[55] They also address, for example, requirements relating to system security; system accuracy and integrity; system auditability; system storage and maintenance; and data retention and transportation. In addition to these standards, some states and local jurisdictions have specified their own voting system requirements.

In 2001, we cited a number of problems with the FEC-issued voting system standards, including missing elements of the standards. Accordingly, we made recommendations to improve the standards. Subsequently, the FEC approved the revised voting system standards on April 30, 2002. According to EAC commissioners with whom we spoke, the commission has inherited the FEC standards, but it plans to work with NIST to revise and strengthen them.

To ensure that systems are designed and built in conformance with applicable standards, our work in 2001 found that three levels of

[52] Systems are all those intended for preparing the voting system for use in an election; producing the appropriate ballot formats; testing that the voting system and ballot materials have been properly prepared and are ready for use; recording and counting votes; consolidating and reporting results; displaying results on site or remotely; and maintaining and producing audit trail information.

[53] Prevoting operations include ballot preparation; the preparation of election-specific software or firmware; the production of ballots or ballot pages; the installation of ballots and ballot counting software or firmware; and system and equipment tests.

[54] Voting operations include all operations conducted at the polling place by voters and officials, including the generation of status messages.

[55] Postvoting operations include closing the polling place; obtaining reports by voting machine, polling place, and precinct (for central-count systems); obtaining consolidated reports; and obtaining reports of audit trails.

tests are generally performed: qualification tests, certification tests, and acceptance tests. For voting systems, the FEC-issued standards called for qualification testing to be performed by independent testing authorities. According to the standards, this testing is to ensure that voting systems comply with both the FEC standards and the systems' own design specifications. State standards define certification tests, which the states generally perform to determine how well the systems conform to individual state laws, requirements, and practice.[56] Finally, state and local standards define acceptance testing, performed by the local jurisdictions procuring the voting systems. This testing is to determine whether the equipment, as delivered and installed, satisfies all the jurisdiction's functional and performance requirements. Beyond these levels of testing, jurisdictions also perform routine maintenance and diagnostic activities to further ensure proper system performance on election day.

Our 2001 work found that the majority of states (38) had adopted the FEC standards then in place,[57] and thus these states required that the voting systems used in their jurisdictions passed qualification testing.[58] In addition, we reported that qualified voting equipment had been used in about 49 percent (±7 percentage points) of jurisdictions nationwide that used DREs and about 46 percent (±7 percentage points) of jurisdictions nationwide that used optical scan technology. However, about 46 percent (±5 percentage points) reported that they did not know whether their equipment had been qualified.

[56] States and local jurisdictions may use the standards to baseline the minimum functional and performance requirements but may also impose other requirements to meet their needs (such as the type and number of languages that equipment should support, how a ballot needs to appear on a DRE screen, or options that allow persons with various types of disabilities to vote).

[57] As of April 2004, the District of Columbia and 42 out of 50 states have regulations that require voting systems to meet federal standards, according to the Election Reform Information Project of the University of Richmond.

[58] However, because the standards were not published until 1990 and the qualification testing program was not established until 1994, we judged in 2001 that many jurisdictions were probably using voting equipment that did not undergo qualification testing.

As we reported in 2001, 45 states and the District of Columbia told us that they had certification testing programs, and we estimate from our mail survey that about 90 percent of jurisdictions used state-certified voting equipment in the 2000 national election.[55] In addition, we reported that most of the jurisdictions that had recently bought new voting equipment had conducted some form of acceptance testing. However, the processes and steps performed and the people who performed them varied. For example, in one jurisdiction that purchased DREs, election officials stated that testing consisted of a visual inspection, power-up, opening of polls, activation and verification of ballots, and closing of polls. In contrast, officials in another jurisdiction stated that they relied entirely on the vendor to test their DREs. In jurisdictions that used optical scan equipment, acceptance testing generally consisted of running decks of test cards. For example, officials from one jurisdiction stated that they tested each unit with the assistance of the vendor using a vendor-supplied test deck.

Our 2001 work found that the processes and people involved in routine system maintenance, diagnostic, and pre-election day checkout activities varied from jurisdiction to jurisdiction. For example, about 90 percent of jurisdictions nationwide using DRE and optical scan technology had performed routine or manufacturer-suggested maintenance and checkout before the 2000 national election. However, our visits to 27 local election jurisdictions revealed variations in the frequency with which jurisdictions performed such routine maintenance. For example, some performed maintenance right before an election, while others performed maintenance regularly throughout the year. For example, officials in one jurisdiction that used DREs stated that they tested the batteries monthly.

Voting Systems Should Be Properly Implemented

Proper implementation of voting systems is a matter of people knowing how to carry out appropriately designed processes to ensure that the technology performs as intended in an operational

[55] GAO-02-3.

setting. According to the EAC commissioners, one of their areas of focus will be election administration processes and the people who carry out these processes. Examples include ballot preparation, voter education, recruiting and training poll workers, setting up the polls, running the election, and counting the votes.

Ballot preparation. Whether ballots are electronic or paper, they need to be designed in a way that promotes voter understanding when they are actually used. Designing both optical scan and DRE ballots requires consideration of the different types of human interaction entailed and the application of some human factors expertise. For DREs, programming skills need to be applied to create the ballot and enter the ballot information onto an electronic storage medium, which is then uploaded to the unit. For optical scan systems, paper ballots need to be designed and printed in specified numbers for distribution to polling places; they may also be used for absentee balloting, usually in combination with printed mailing envelopes. Electronic "ballots" in DRE units do not require distribution separate from the distribution of the voting equipment itself; however, the use of DREs means that a separate technique is necessary for absentee ballots—generally paper ballots. Thus, the use of these units generally requires a mixed election system.

Voter education. Implementation of any voting method requires that voters understand how to vote—that is, what conventions are followed. For optical scan systems, voters need to understand how to mark the ballots, they need to know what kinds of marker (type of pen or pencil) can be used, they need to be informed if a ballot must be marked on both sides, and so on. For DRE systems, voters need to understand how to select candidates or issues and understand that their votes are not cast until the cast vote button is pressed; for touchscreens, they need to know how to navigate the various screens presented to them.

Voters also need to understand the procedure for write-in votes. In 2001, one jurisdiction had an almost 5 percent overvote rate because voters did not understand the purpose of the ballot section permitting write-in votes. Voters selected a candidate on the ballot and then wrote the candidate's name in the write-in section of the ballot, thus overvoting and spoiling the ballot. In addition to voter education, how the system is programmed to operate can also

address this issue. For example, precinct-count optical scan equipment can be programmed to return a voter's ballot if the ballot is overvoted or undervoted and allow the voter to make changes.

Poll worker recruitment and training. Poll workers need implementation training. They need to be trained not only in how to assist voters to use the voting system, but also in how to use the technology for the tasks poll workers need to perform. These tasks can vary greatly from jurisdiction to jurisdiction. When more sophisticated voting systems are used at polling sites, jurisdictions may find it challenging to find poll workers with the skills to implement and use newer technologies. In 2001, we quoted one election official who said that "it is increasingly difficult to find folks to work for $6 an hour. We are relying on older retired persons—many who can't/won't keep up with changes in the technology or laws. Many of our workers are 70+."

Setting up the polls. Proper setup of polling places raises a number of implementation issues related to the people, processes, and technology involved. For DREs, the need for appropriate power outlets and possibly network connections limits the sites that can be used as polling places. In addition, setting up, initializing, and sometimes networking DRE units are technically challenging tasks. Technicians and vendor representatives may be needed to perform these tasks or to assist poll workers with them. In addition, with DREs, computer security issues come into play that are different from those associated with the paper and pencil tools that voters use in optical scan systems. Besides the units themselves, many DRE systems use cards or tokens that must be physically secured. With optical scan equipment, the ballots must be physically secured. Further, if precinct-based tabulation is used with an optical scan system, the tabulation equipment must be protected from tampering.

Running the election. Many implementation issues associated with running the election are associated with the interaction of voters with the technology. Although both DREs and optical scan systems are based on technologies that most voters will have encountered before, general familiarity is not enough to avoid voter errors. With optical scan, voter errors are generally related to improperly marked ballots: the wrong marking device, stray marks, too many marks

(overvotes), and so on. As described already, DRE equipment is designed to minimize voter error (by preventing overvotes, for example), but problems can also occur with this voting method. For example, many DREs require the voter to push a cast vote button to record the vote. However, some voters forget to push this button and leave the polling place without doing so. Similarly, after pressing the final cast vote button, voters cannot alter their votes. In some cases, this button may be pressed by mistake—for example, a small child being held by a parent may knock or kick the final vote button before the parent has completed the ballot.

The technology is not the only factor determining the outcome in these situations, as different jurisdictions have different rules and processes concerning such problems. In 2001, we reported that when voters forgot to press the cast vote button, one jurisdiction required that an election official reach under the voting booth curtain and push the cast vote button without looking at the ballot. However, another jurisdiction required that an election official invalidate the ballot and reset the machine for a new voter.

Counting the votes. Finally, implementation of the processes for counting votes is affected both by the technology used and by local requirements. With DREs, votes are collected within each unit. Some contain removable storage media that can be taken from the voting unit and transported to a central location to be tallied. Others can be configured to electronically transmit the vote totals from the polling place to a central tally location. As described earlier, optical scan systems also vary in the way votes are counted, depending on whether precinct-based or centralized tabulation equipment is used. For optical scan systems, officials follow state and local regulations and processes to determine whether and how to count ballots that cannot be read by the tabulation equipment. Counting such ballots may involve decisions on how to judge voter intent, which are also generally governed by state and local regulations and processes.

In addition, depending on the type of voting technology used, ways to perform recounts may differ. For optical scan devices, recounts can be both automatic and manual; as in the original vote counting, officials make decisions on counting ballots that cannot be read by the tabulation equipment and on voter intent. With DREs there is no separate paper ballot or record of the voter's intention, and

therefore election officials rely on the information recorded in the machine's memory: that is, permanent (read only) electronic images of each of the "marked" ballots. The assurance that these images are an accurate record of the vote depends on several things, including the proper implementation of the processes involved in designing, maintaining, setting up, and using the technology.

Jurisdictions Face Immediate and Longer Term Challenges in Leveraging Voting Technologies

In 2001, we identified four key challenges confronting local jurisdictions in effectively using and replacing voting technologies. These challenges are not dissimilar to those faced by any organization seeking to leverage modern technology to support mission operations. The first two challenges are particularly relevant in the near term, as jurisdictions look to position themselves for this year's national elections. The latter two are more relevant to jurisdictions' strategic acquisition and use of modern voting systems.

Ensuring that Necessary Security, Testing, and Maintenance Activities Are Performed

Maximizing the performance of the voting systems that jurisdictions have and plan to use in November 2004 means taking proactive steps between now and then to best ensure that systems perform as intended. These steps include activities aimed at securing, testing, and maintaining these systems. We reported in 2001 that although the vast majority of jurisdictions performed security, testing, and maintenance activities in one form or another, the extent and nature of these activities varied among jurisdictions and depended on the availability of resources (financial and human capital) committed to them. The challenge facing all voting jurisdictions will be to ensure that these activities are fully and properly performed, particularly in light of the serious security concerns that have been reported with DREs.

Managing the People, Processes, and Technology as Components of the Overall Process

As previously discussed in this testimony, jurisdictions need to manage the triad of people, processes, and technology as interrelated and interdependent parts of the total voting process. Given the amount of time that remains between now and the November 2004 elections, jurisdictions' voting system performance is more likely to be influenced by improvements in poll worker system operation training, voter education about system use, and vote casting procedures than by changes to the systems themselves.[60] The challenge for voting jurisdictions is thus to ensure that these people and process issues are dealt with effectively.

Having Reliable System Performance Measures and Objective Data

Reliable measures and objective data are needed for jurisdictions to know whether the technology being used is meeting the needs of the user communities (both the voters and the officials who administer the elections). In 2001, we reported that the vast majority of jurisdictions were satisfied with the performance of their respective technologies in the November 2000 elections. However, this satisfaction was mostly based not on objective data measuring performance, but rather on the subjective impressions of election officials. Although these impressions should not be discounted, informed decisionmaking on voting technology investment requires more objective data. The challenge for jurisdictions is to define measures and begin collecting data so that they can definitely know how their systems are performing.

Ensuring That Technology Cost Is Commensurate with Benefits

Jurisdictions must be able to ensure that the technology will provide benefits over its useful life that are commensurate with life-cycle costs (acquisition as well as operations and maintenance) and that these collective costs are affordable and sustainable. In 2001, we reported that the technology type and configuration that jurisdictions employed varied depending on each jurisdiction's unique circumstances, such as size and resource constraints, and

[60] Some system changes may be feasible, such as connecting DREs to printers.

that reliable data on life-cycle costs and benefits were not available. The challenge for jurisdictions is to view and treat voting systems as capital investments and to manage them as such, including basing decisions on technology investments on clearly defined requirements and reliable analyses of quantitative and qualitative return on investment.

In closing, I would like to say again that electronic voting systems are an undeniably critical link in the overall election chain. While this link alone cannot make an election, it can break one. The problems that some jurisdictions have experienced and the serious concerns being surfaced by security experts and others highlight the potential for difficulties in the upcoming 2004 national elections if the challenges that we cited in 2001 and reiterate in this testimony are not effectively addressed. Although the EAC only recently began operations and is not yet at full strength, it needs to remain vigilant in its efforts to ensure that jurisdictions and voters are educated and well-informed about the proper implementation and use of electronic voting systems, and to ensure that jurisdictions take the appropriate steps—related to people, process, and technology—that are needed regarding security, testing, and maintenance. More strategically, the EAC needs to move swiftly to strengthen the voluntary voting system guidelines and the testing associated with enforcing these guidelines. Critical to the commission's ability to do this will be the adequacy of resources at its disposal and the degree of cooperation it receives from entities at all levels of government.

Mr. Chairman, this concludes my statement. I would be pleased to answer any questions that you or other Members of the Subcommittee may have at this time.

Contact and Acknowledgements

For further information, please contact Randolph C. Hite at (202) 512-6256 or by e-mail at hiter@gao.gov. Other key contributors to this testimony were Barbara S. Collier, Deborah A. Davis, Richard B. Hung, John M. Ortiz, Jr., Maria J. Santos, and Linda R. Watson.

Mr. PUTNAM. Our next witness is Dr. Hratch Semerjian, serving as Acting Director of NIST. He has served as Deputy Director of NIST since July 2003. In this position Dr. Semerjian is responsible for the overall operation of the Institute, including financial management, human resource management, facilities and information technology systems, effectiveness of NIST's technology programs, and interactions with international organizations.

He received his master's and Ph.D. Degrees in engineering from Brown. In 1977, he joined the National Bureau of Standards, now known as NIST, where he served director of the chemical science and laboratory from April 1992 through July 2002.

Welcome to the subcommittee, sir. You are recognized.

Dr. SEMERJIAN. Thank you, Mr. Chairman and Ranking Member Clay and Mr. Holt. I appreciate this opportunity to testify today.

As you pointed out, major changes are taking place in the way we conduct elections. The trusty old ballot box is being replaced by a host of new technology such as optical scanners or touch-screen systems. As a result of these changes, Congress enacted the Help America Vote Act and mandated specific roles for the National Institute of Standards and Technology [NIST].

Many of the issues we are examining today are all directly related to standards and guidelines. Congress understood the importance of standards in voting technologies and specifically gave the Director of NIST the responsibility of chairing the Technical Guidelines Development Committee [TGDC], a committee reporting to the Election Assistance Commission [EAC] under HAVA.

The TGDC is charged with making recommendations to the EAC with regard to voluntary standards and guidelines for election-related technologies that have an impact on many of the issues we are discussing today.

While we have considerable experience in standards development, NIST understands that, as a nonregulatory agency, our role is limited, and we need to understand the needs of the community. To that end, NIST staff have started to meet with members of the election community.

Also, at the request of Congress and the National Association of State Election Directors, NIST organized and hosted a symposium last December on Building Trust and Confidence in Voting Systems. Over 300 attendees from the election community attended the seminar to begin discussion, collaboration and consensus on voting reform issues.

As required under HAVA, earlier this year NIST delivered to the EAC a report entitled "Improving the Usability and Accessibility of Voting Systems and Products." The EAC delivered the report to Congress on April 30th. The specific recommendations of the report are included in my written testimony.

NIST views as a top priority accomplishing its responsibilities mandated under HAVA in partnership with the EAC. These mandates include the recommendation of voluntary voting system standards to the EAC through its Technical Guidelines Development Committee. The first set of voluntary standards is due 9 months after the appointment of the 14 members by the EAC.

TGDC held its first meeting on July 9th, just a couple of weeks ago. Fourteen of the fifteen appointed members of the Technical

Guidelines Development Committee participated in the first plenary meeting. At that meeting the TGDC agreed on a procedural roadmap for standards development as well as a preliminary work plan. In addition, the TGDC adopted a resolution that established three working subcommittees to address issues related to one, security and transparency; two, human factors and privacy; and three, core requirements and testing.

Another important role for NIST under HAVA is to develop a formal accreditation program for laboratories that test voting system hardware and software for conformance to current voting system standards.

On June 23rd, NIST announced in the Federal Register the establishment of a laboratory accreditation program for voting systems. NVLAP, the National Voluntary Laboratory Accreditation Program at NIST, will conduct a public workshop on August 17th to review its accreditation criteria as well as receive comments and feedback from the participating laboratories and other interested parties. Only after a laboratory has met all of the NVLAP criteria for accreditation will it be presented to the Election Assistance Commission for its approval to test voting systems. The EAC may impose requirements on the laboratories in addition to the NVLAP accreditation.

Finally, NIST has compiled best security practices relevant to election security from current Federal Information Processing Standards [FIPS]. These standards are available now on the NIST Website as well as the EAC Website. This compilation is intended to help State and local election officials with their efforts to better secure voting equipment before the November 2004 elections.

NIST realizes how important it is for voters to have trust and confidence in voting systems, even as new technologies are introduced. Increasingly, computer technology touches all aspects of the voting process, voter registration, vote recording and vote tallying. NIST believes that rigorous standards, guidelines and testing procedures will enable U.S. industry to produce products that are high-quality, reliable, interoperable and secure, thus enabling the trust and confidence that citizens require and at the same time preserving room for innovation and change.

Thank you for the opportunity to testify on behalf of NIST, and I will be happy to answer any questions.

Mr. PUTNAM. Thank you, sir.

[The prepared statement of Dr. Semerjian follows:]

Statement of

Dr. Hratch G. Semerjian
Acting Director

National Institute of Standards and Technology
Technology Administration
U.S. Department of Commerce

Before the

House of Representatives
Committee on Government Reform
Subcommittee on Technology, Information Policy, Intergovernmental Relations
and the Census

"The Science of Voting Machine Technology: Accuracy, Reliability, and Security"

July 20, 2004

Chairman Putnam, Ranking Member Clay, and members of the Subcommittee thank you for the opportunity to testify today on "The Science of Voting Machine Technology: Accuracy, Reliability and Security." Major changes are taking place in the way we conduct elections. Our trusty old ballot boxes often are being replaced by a host of new technologies. Citizens are now much more likely to encounter optical scanners or touch screen systems at the polling place than a wooden box with a sturdy lock. As a result of these changes, Congress enacted the Help America Vote Act, commonly known as HAVA, and mandated specific research and development roles for the National Institute of Standards and Technology (NIST).

Many of the issues we are examining today are all directly related to standards and guidelines. As we like to say at NIST, if you have a good standard, you can have a good specification, and with proper testing you will be assured that the equipment performs as required. Congress understood the importance of standards in voting technologies and specifically gave the Director of NIST the responsibility of chairing the Technical Guidelines Development Committee (TGDC), a committee reporting to the EAC under HAVA. This committee is charged with making recommendations to the Election Assistance Commission (EAC) with regard to voluntary standards and guidelines for election-related technologies that have an impact on many of the issues we are discussing.

While we have considerable experience in "standards development", NIST understands that as a non-regulatory agency our role is limited and has started to meet with members of the "elections community", – ranging from disability advocacy groups, voting advocacy groups, researchers, state and local election officials, and vendors – to learn about their concerns. Ultimately, in coordination with the EAC and the broader "elections community" we want to apply our "standards development" experience to election-related technologies so that, when voting is complete, the vote tally will be accurate and done in a timely manner.

NIST is by no means a newcomer to the issues related to electronic voting. Previous to the HAVA, NIST's involvement in studying voting machine technology resulted in the publication of two technical papers in 1975 and 1988. NIST's recent activities related to voting system technology have been preparatory to the implementation of HAVA and fulfilling the initial mandates of the law.

At the request of Congress and the National Association of State Election Directors, NIST organized and hosted a *Symposium on Building Trust and Confidence in Voting Systems* in December of 2003 at its Gaithersburg headquarters. Over three hundred attendees from the election community attended the seminar to begin discussion, collaboration and consensus on voting reform issues. Symposium participants included state and local election officials; vendors of voting equipment and systems, academic researchers; representatives of the cyber-security and privacy community; representatives from the disability community, standards organizations and independent testing authorities, as well as newly appointed U.S. Election Assistance Commissioners. Representative stakeholders participated with NIST scientists in panels addressing:

- Testability, Accreditation and Qualification in Voting Systems;

- Security and Openness in Voting Systems; and
- Usability and Accessibility in Voting Systems.

Attendees agreed that they all shared the goals of:

- Practical, secure elections, with every vote being important;
- The importance of looking at the voting system end-to-end;
- The need for good procedures & best practices in physical & cyber security;
- The need to improve current testing & certification procedures;
- The need to separately address both short-term and long-term challenges; and
- The benefits of the election community working as a team.

As required under HAVA, earlier this year NIST recently delivered to the EAC a report "which assesses the areas of human factors research and human-machine interaction, which feasibly could be applied to voting products and systems design to ensure the usability of and accuracy of voting products and systems, including methods to improve access for individuals with disabilities (including blindness) and individuals with limited proficiency in the English Language and to reduce voter error and the number of spoiled ballots in elections". The EAC delivered the report to Congress on April 30, 2004.

The report titled "Improving the Usability and Accessibility of Voting Systems and Products," assesses human factors issues related to the process of a voter casting a ballot as he or she intends. The report's most important recommendation is for the development of a set of usability standards for voting systems that are performance-based. Performance-based standards address results rather than equipment design. Such standards would leave voting machine vendors free to develop a variety of innovative products if their systems work well from a usability and accessibility standpoint. Additionally, the report emphasizes developing the standards in a way that would allow independent testing laboratories to test systems to see if they conform to the usability standards. The labs would employ objective tests to decide if a particular product met the standards.

In total the report makes 10 recommendations to help make voting systems and products simpler to use, more accurate and easily available to all individuals – including those with disabilities, language issues and other impediments to participating in an election. The recommendations highlight the need to:

1) Develop voting system standards for usability that are performance-based, relatively independent of the voting technology, and specific (i.e., precise).

2) Specify the complete set of user-related functional requirements for voting products in the voting system standards.

3) Avoid low-level design specifications and very general specifications for usability.

4) Build a foundation of applied research for voting systems and products to support the development of usability and accessibility standards.

5) To address the removal of barriers to accessibility, the requirements developed by the Access Board, the current VSS (Voting System Standards), and the draft IEEE (Institute of Electrical and Electronics Engineers) standards should be reviewed, tested, and tailored to voting systems and then considered for adoption as updated VSS standards. The feasibility of addressing both self-contained, closed products and open architecture products should also be considered.

6) Develop ballot design guidelines based on the most recent research and experience of the visual design communities, specifically for use by election officials and in ballot design software.

7) Develop a set of guidelines for facility and equipment layout; develop a set of design and usability testing guidelines for vendor- and state-supplied documentation and training materials.

8) Encourage vendors to incorporate a user-centered design approach into their product design and development cycles including formative (diagnostic) usability testing as part of product development.

9) Develop a uniform set of procedures for testing the conformance of voting products against the applicable accessibility requirements.

10) Develop a valid, reliable, repeatable, and reproducible process for usability conformance testing of voting products against the standards described in recommendation 1) with agreed upon usability pass/fail requirements.

NIST views as a top priority accomplishing its impending responsibilities mandated in the HAVA in partnership with the EAC. These mandates include the recommendation of voluntary voting system standards to the EAC through its Technical Guidelines Development Committee. The first set of voluntary standards is due nine months after the appointment of the fourteen members by the EAC.

The TGDC held its first meeting on July 9, 2004. Fourteen of the fifteen appointed members of the Technical Guidelines Development Committee participated in the first plenary meeting. Dr. Arden Bement NIST's Director serving as chairman, set as a goal for the meeting to agree on a procedural road map for standards development as well as a preliminary work plan.

Specifically, the chair recommended the committee strive for five distinct deliverables to the EAC in the next nine months:

1) A list of publicly vetted requirements for voluntary voting system standards;
2) Recommendations for standards that currently exist with changes if necessary;

3) An assessment of best practices that can be made available to the election community for use in the 2006 election cycle;
4) A recognition and statement thereof of those areas where there are no current standards under development; and
5) A prioritized calendar for future standards development relative to each of the four previous deliverables.

In addition the TGDC adopted a resolution that established three working subcommittees to address security and transparency, human factors and privacy, and core requirements and testing. Dr. Bement and the members of the TGDC believe that his goal for the initial plenary session was indeed met. Our current plans call for the next plenary session on or about January 2005 with public meetings between now and then to gather data, and subcommittee meetings to analyze the data and form initial resolutions.

Another important role for NIST under HAVA is to develop a formal accreditation program to laboratories that test voting system hardware and software for conformance to the current Voting System Standards. On June 23, 2004, NIST announced in the Federal Register the establishment of a Laboratory Accreditation Program for Voting Systems. NIST will carry out the accreditation of these laboratories through the National Voluntary Laboratory Accreditation Program (NVLAP), which is administered by NIST. NVLAP is a long-established laboratory accreditation program that is recognized both nationally and internationally. NVLAP accreditation criteria are codified in the Code of Federal Regulations (CFR, Title 15, Part 285).

NVLAP will conduct a public workshop on August 17th to review its accreditation criteria, as well as receive comments and feedback from the participating laboratories and other interested parties. After the workshop, NVLAP will finalize specific technical criteria for testing laboratories and make the necessary logistical arrangements to begin the actual assessment of the laboratories. NVLAP must identify, contract, and train technical expert assessors; laboratories must complete the NVLAP application process; rigorous onsite assessments must be conducted; and laboratories undergoing assessment must resolve any identified nonconformities before accreditation can be granted. It is our intention that laboratories will be able to formally apply to NVLAP and initiate the assessment process in early 2005 if not sooner.

Simply stated, laboratory accreditation is formal recognition that a laboratory is competent to carry out specific tests. Expert technical assessors conduct a thorough evaluation of all aspects of laboratory operation that affect the production of test data, using recognized criteria and procedures. General criteria are based on the international standard ISO/IEC 17025, *General requirements for the competence of testing and calibration laboratories*, which is used for evaluating laboratories throughout the world. Laboratory accreditation bodies use this standard specifically to assess factors relevant to a laboratory's ability to produce precise, accurate test data, including the technical competency of staff, validity and appropriateness of test methods, testing and quality assurance of test and calibration data. Laboratory accreditation programs usually also specify field-specific technical criteria that laboratories must meet, in addition to demonstrating general technical competence.

Laboratory accreditation thus provides a means of evaluating the competence of laboratories to perform specific types of testing, measurement and calibration. It also allows a laboratory to determine whether it is performing its work correctly and to appropriate standards.

Laboratories seeking accreditation to test voting system hardware and software will be required to meet the NVLAP criteria for accreditation which include: ISO/IEC 17025, the 2002 Voting System Standards, and any other criteria deemed necessary by the Election Assistance Commission (EAC). To ensure continued compliance, all NVLAP-accredited laboratories undergo an onsite assessment before initial accreditation, during the first renewal year, and every two years thereafter to evaluate their ongoing compliance with specific accreditation criteria.

Only after a laboratory has met all NVLAP criteria for accreditation will it be presented to the Election Assistance Commission for its approval to test voting systems. The EAC may impose requirements on the laboratories in addition to NVLAP accreditation.

Finally, NIST has compiled best security practices relevant to election security from current Federal Information Processing standards (FIPS). These standards are available on the NIST website (http://vote.nist.gov/securityrisk.pdf) and will be available on EAC's website (http://www.fec.gov/pages/vssfinal/vss.html). This compilation is intended to help state and local election officials with their efforts to better secure voting equipment before the November 2004 election.

NIST realizes how important it is for voters to have trust and confidence in voting systems even as new technologies are introduced. Increasingly, computer technology touches all aspects of the voting process – voter registration, vote recording, and vote tallying. NIST believes that rigorous standards, guidelines, and testing procedures will enable U.S. industry to produce products that are high quality, reliable, interoperable, and secure thus enabling the trust and confidence that citizens require and at the same time preserving room for innovation and change.

Thank you for the opportunity to testify. I would be happy to answer any questions the Committee might have.

Mr. PUTNAM. Our next witness will be introduced by his fellow Missourian, Missourian or Missourian.

Mr. CLAY. Missourian.

Mr. PUTNAM. Missourian.

You are recognized, sir. You have the floor, sir.

Mr. CLAY. Thank you, Mr. Chairman.

Mr. Terry Jarrett is the general counsel to Secretary of State Matt Blunt. He received his J.D. in 1996 from the University of Missouri Columbia School of Law. While in law school, Mr. Jarrett was editor-in-chief of the Missouri Law Review. From 1996 to 1997, he served as a judicial law clerk to the Honorable Duane Benton, judge of the Supreme Court of Missouri.

Prior to joining the Secretary of State, Mr. Jarrett practiced law as a private attorney in Jefferson City. He is a member of the Missouri Bar, the Cole County Bar Association and the American Bar Association. Mr. Jarrett also serves as a first lieutenant in the Judge Advocate General's Court of the U.S. Army Reserve. He represents the Missouri Secretary of State Matt Blunt.

Welcome to the committee. Thank you for being here.

Mr. JARRETT. Thank you, Mr. Chairman, Ranking Member Clay and Mr. Holt.

It is an honor to have the opportunity to testify at today's hearing. I am here on behalf of Missouri Secretary of State Matt Blunt, whose schedule would not allow him to be here today, and he asked me to express his regrets. Secretary Blunt specifically asked that I thank the distinguished member of this subcommittee, Congressman William Lacy Clay from our home State of Missouri, who has been a leader in reform efforts in the city of St. Louis. He has been particularly interested in the city's compliance with the consent decree between St. Louis City and the Department of Justice related to the handling of the city's inactive voter list. Secretary Blunt shares his concern and appreciates his efforts to improve elections in St. Louis.

Secretary Blunt has asked me to address the security of direct recording electronic voting machines, specifically whether to require DREs to produce a voter-verified paper ballot. Secretary Blunt has worked over the past 3 years to ensure that our elections are above reproach and that our citizens have confidence in the process. That is why he decided earlier this year that he would only certify DRE voting machines that produce a voter-verified paper ballot. This will provide voters with the peace of mind they deserve by enabling them to review their ballots prior to casting them and to ensure that paper ballots are available for review should a recount be necessary or an election result challenged.

One of Secretary Blunt's first acts as Secretary of State was to appoint and convene a bipartisan commission of election experts to recommend improvements in our election laws and procedures. The commission met several times and conducted a series of public hearings where over 125 Missourians voiced their opinions in oral and written testimony. In addition many Missourians have submitted their thoughts by e-mail, fax and regular mail.

Out of this very open process came many recommendations for improvements that have since been implemented in Missouri. One of the commission's recommendations was to allow for the use of

touch-screen voting systems, so long as safeguards are in place to ensure the integrity of votes cast and create a paper audit trail in case of a contested election.

Secretary Blunt heard from many Missourians who expressed their preference that touch-screen voting machines produce a paper ballot so that they can verify their votes before they are cast. At this point in time, Secretary Blunt is convinced that a voter-verified paper ballot is the only paper audit trail that can provide voters with a reasonable assurance that their vote will not be lost, destroyed or otherwise not counted.

Computers have opened up a whole new array of technical possibilities for voting. Manufacturers are moving quickly to embrace innovation. Technology can and should be used by government to improve efficiency, as well as provide cost savings for taxpayers. This new technology promises to open up voting to people who have not been able to participate fully in the voting process, namely the disabled voter. Yet in our urgency to improve and upgrade voting systems, we must not certify equipment that has the potential to cast doubt on the integrity of an election. Effective security standards and procedures must be considered and implemented.

Secretary Blunt has also heard from a number of local election officials, and I want to say a word about them. They eagerly await the opportunity to provide voters with the benefits that technology can provide. Local election officials are on the front lines of voting, and I urge this subcommittee to seek their input as it addresses the important issues raised by today's hearing.

There is a growing consensus of computer science experts, election officials, voter advocacy groups and political leaders that touch-screen voting systems should produce a verified voter ballot so that voters can inspect their ballots before they are cast. Almost daily, reports in the newspaper and other media outlets support this view. A voter-verified paper ballot providing local election officials with access to actual ballots for recounts if necessary is just as important.

Perhaps at some point in the future, technological advances will be such that electronic voting system security can be assured without voter-verified paper ballots. However, that does not appear to be the case today. Until we can be positive that electronic voting systems are secure, a voter-verified paper ballot is the best way to make voters feel confident in legitimacy of elections.

I appreciate that this subcommittee recognizes the importance of this issue by having this public hearing. Thank you again for the opportunity to share Secretary Blunt's views with this subcommittee, and I would be happy to answer any questions. Thank you.

Mr. PUTNAM. Thank you very much.

[The prepared statement of Mr. Jarrett follows:]

Written Testimony of Terry Jarrett
General Counsel to the Honorable Matt Blunt, Missouri Secretary of State
Before the
House Committee on Government Reform
Subcommittee on Technology, Information Policy,
Intergovernmental Relations and the Census
July 20, 2004

Thank you Mr. Chairman and distinguished members of the Subcommittee. It is an honor to have the opportunity to testify at today's hearing on "The Science of Voting Machine Technology: Accuracy, Reliability and Security." I am Terry Jarrett, General Counsel to Missouri Secretary of State Matt Blunt. Secretary Blunt's schedule would not allow him to be here today, and he asked me to express his regrets. He wants me to convey to this Subcommittee his appreciation in allowing me to testify on his behalf. Secretary Blunt specifically asked that I thank a distinguished member of this Subcommittee—Congressman William Lacy Clay from our home state of Missouri—who has been a leader in election reform efforts in the City of St. Louis. He has been particularly interested in the City's compliance with a Consent Decree between St. Louis City and the Department of Justice relating to the handling of the City's inactive voter list. Secretary Blunt appreciates his concern and his efforts to ensure that the 2004 elections in St. Louis will be free from many of the problems that occurred during the November 2000 election.

Secretary Blunt has asked me to address the security of Direct Recording Electronic (DRE) voting machines – also known as "touch screen" machines – specifically, whether to require DREs to produce a voter verified paper ballot. Secretary

Blunt has worked over the past three years that he has been Missouri's Secretary of State to ensure that our elections are above reproach, and that our citizens have confidence in the process and, most importantly, the results. That is why he decided earlier this year that he would only certify DRE voting machines that produce a voter verified paper ballot. This will provide voters with the peace of mind they deserve on Election Day by enabling them to review their ballots prior to casting them and ensure that paper ballots are available for review should a recount be necessary or an election result challenged.

One of Secretary Blunt's first acts as Secretary of State was to appoint and convene a bipartisan commission of election experts to recommend changes and improvements in our elections laws and procedures. The commission met several times and conducted a series of public hearings in which 18 Missouri communities participated. During the hearings, over 125 Missourians voiced their opinions with many also providing written testimony. In addition, many Missourians submitted their thoughts on the election process via e-mail, fax and regular U.S. mail. Out of this very open process came many recommendations for improvements that have since been implemented in Missouri. One of the commission's recommendations was to amend Missouri law to allow for the use of touch screen voting systems so long as safeguards are in place to ensure the integrity of votes cast and create a paper audit trail in case of a contested election. Secretary Blunt heard from many Missourians who expressed their preference that touch screen voting machines produce a paper ballot so that they can verify their votes before they are cast. At this point in time Secretary Blunt is convinced that a voter

verified paper ballot is the only "paper audit trail" that can provide voters with a reasonable assurance that their vote will not be lost, destroyed or otherwise not counted.

Computers have opened up a whole new array of technical possibilities for the casting and counting of votes. Manufacturers are moving quickly to embrace innovation. Secretary Blunt believes that technology can and should be used by government to improve efficiency and service as well as provide cost savings for taxpayers. This new technology promises to open up voting to people who have not been able to participate fully in the voting process—the disabled. Yet, in our urgency to improve and upgrade voting systems, we must not certify equipment and systems that have the potential to cast doubt on the integrity of an election. Effective security standards and procedures must be considered and implemented.

Secretary Blunt has also heard from a number of local election officials, and I want to say a word about them. They eagerly await the opportunity to provide voters with the benefits that technology can provide. Local election officials are on the "front lines" of voting, and I urge this subcommittee to seek their input as it addresses the important issues raised by today's hearing.

There is a growing consensus of computer science experts, elections officials, voter advocacy groups and political leaders that touch screen voting systems should produce a voter verified paper ballot so voters can inspect their ballots before they are cast to ensure they were marked as intended. Almost daily, reports in the newspaper and other media outlets support this view. For example, recently the following events have occurred:

- On May 5, 2004, the Election Assistance Commission held a public hearing on the present status of computerized voting systems.
- On April 30, 2004, California Secretary of State Kevin Shelley banned the use of touch screen voting systems in four counties and decertified all touch screen systems in California until they could produce a voter-verified paper trail.
- On April 22, 2004, a lawsuit was filed in Maryland challenging use of certain DREs that do not create a voter verified paper trail. On June 25, the plaintiffs in that case filed a motion for preliminary injunction barring Maryland from using certain DREs in the November 2004 election.

A voter verified paper ballot providing local election officials and the courts with access to actual ballots for recounts if one is necessary or in the event that the electronic equipment is damaged or malfunctions would be just as important. There are bills now pending in Congress that would require a voter verified paper ballot for electronic voting systems. Representative Clay is a co-sponsor of just such a bill, H.R. 2239, the Voter Confidence and Increased Accessibility Act. Perhaps at some point in the future technological advances will be such that electronic voting system security can be assured without voter verified paper ballots. However, that does not appear to be the case today. Until we can be positive that electronic voting systems are secure, a voter verified paper ballot is the best way to make voters feel confident in the legitimacy of elections.

I appreciate that this Subcommittee recognizes the importance of this issue by having this public hearing. Thank you again for the opportunity to share Secretary Blunt's views with the Subcommittee.

Mr. PUTNAM. We are going to do a 5-minute round of questions, get through everyone, and then do another round if we so desire. Considering the number of committee members who are here, I think we will certainly have time to do that.

Technology changes rapidly. Obviously local governments don't have the luxury of changing election systems with every cycle, but a number of these new systems are new. I mean, they are new concepts, they are new approaches.

Mr. Hite, if you would, evaluate these newer models, optical scan and the DREs, for us and rank them in terms of accuracy, security and access for those who traditionally have not had good access to the ballot.

Mr. HITE. I would be happy to, but I would like to preface it with addressing the question on two levels. You can talk about the types of equipment in general, but it really also requires getting down to specific make and model, because while DREs, for example, commonly offer certain features with respect to accuracy or with respect to security, how they are actually implemented in the system, and then how they are actually implemented within the jurisdiction, will determine how well they perform.

So, with that preface, I will make a couple of comments based on our 2001 work, where we surveyed vendors and we surveyed jurisdictions with respect to these characteristics of performance. As a general rule, when it came to ease of use and efficiency, how quickly they can capture and count, and the costs associated with doing that, DREs generally had a higher rating than the other types of voting equipment. With regard to security based on features, notwithstanding how they have been implemented, that with regard to security, DREs and optical scan were roughly the same. And then with regard to accuracy across all types of equipment, whether it is jurisdictions or vendors, they basically viewed the accuracy of the systems to be somewhat the same.

Now, I would add another qualification with that with regard to the jurisdictions, and that is when we followed up with certain jurisdictions to see what data are actually collected and are behind these impressions, we learned that is exactly what they are, they are impressions or viewpoints on performance.

The data are pretty sparse in terms of what are collected relative to the performance of any of the types of systems, which is one of the long-term challenges that we have laid out that needs to be addressed. If we are going to make strategic, long-term, informed decisions about what kind of technology to use, you have to base it on some good data, and in terms of a performance standpoint out there across the jurisdictions, that data basically are not being captured.

Mr. PUTNAM. Dr. Semerjian, do you want to field that as well?

Dr. SEMERJIAN. Well, I basically agree with the comments made by Mr. Hite. I think the DREs can improve their performance with the appropriate standards and testing protocols. I think that is really where we still have a perception that these systems are not tested properly. We don't have national standards; implementation is varied from State to State, from precinct to precinct. I think with the proper establishment of proper standards and testing procedures, I think DREs can improve our ability to provide secure, pri-

vate voting ability and accuracy. And also, I think it was pointed out by Mr. Hite, it can improve in terms of enabling voters with disabilities. That's something that perhaps the other systems do not. I think that is something we need to keep in mind.

Mr. PUTNAM. Mr. Jarrett, how many different voting systems are employed throughout Missouri?

Mr. JARRETT. In Missouri we have three types. We do some counties that still operate under the paper ballot system. We have punch card systems and also optical scan systems.

Mr. PUTNAM. And the decision on which type to deploy is made by whom?

Mr. JARRETT. That is made by the local election officials in every county.

Mr. PUTNAM. And how many of those are there? How many different counties do you have?

Mr. JARRETT. We have 116 election authorities. The urban areas such as St. Louis, Kansas City, St. Louis County and Jackson County have boards of election commissioners that are appointed by the Governor, and they run elections in those areas. The rest are run by county clerks.

Mr. PUTNAM. Has there been a high turnover since 2000?

Mr. JARRETT. Of county clerks?

Mr. PUTNAM. No, of technology.

Mr. JARRETT. Oh, I'm sorry.

Mr. PUTNAM. Changes in the method of electioneering.

Mr. JARRETT. Well, Missouri is the ShowMe State, so we have been sort of taking a wait-and-see attitude.

Mr. PUTNAM. Wait on Florida to show you the way, right?

Mr. JARRETT. Yes, that's right. We have had eight counties that moved from the punch card to the optical scan for this election. Several of the counties are waiting, looking at the DREs very closely, and, of course, some of the counties that had optical scan had the central count, and they are moving toward the precinct counters, so not much turnover. Again, we are sort of adopting the wait-and-see approach.

Mr. PUTNAM. My time expired. I will yield to Mr. Clay also. Boy, 5 minutes goes by pretty fast.

Mr. CLAY. Yes, it does. You were having fun, Mr. Chairman.

Mr. Hite, in your testimony you communicate that certain voting machines pose a certain risk. Do you have a certain set of recommendations for local election officials to minimize those risks?

Mr. HITE. The short answer is no, sir, I don't have a set of recommendations handy for those jurisdictions. I would observe, however, that this is one of the things that the Election Assistance Commission was set up to do, and I believe they are on brink of releasing best practices for the local jurisdictions to employ in the 2004 elections.

Mr. CLAY. You know, the Election Assistance Commission has a budget of $1.5 million for fiscal year 2004. Is that adequate for them to meet their obligations for the 2004 elections?

Mr. HITE. I know, in talking to the Commission Commissioners, that they do not believe that it is adequate, and I believe they are in the best position to make a judgment as to whether or not it is adequate or not. I know under HAVA they were authorized up to

$10 million a year, and I would only submit, from my viewpoint, that their role in this, as is the role of NIST, is extremely important and worthy of adequate funding to ensure that they can do what they were set up to do under HAVA.

Mr. CLAY. Does certification guarantee that the software is free of malicious code, and, if so, how is that accomplished?

Mr. HITE. No sir, the answer to your question is no, it does not guarantee that. There is no system that offers a guarantee of that.

Mr. CLAY. Does it guarantee that the machine cannot be tampered with during the election?

Mr. HITE. No sir.

Mr. CLAY. No. OK. Thank you for your responses.

Dr. Semerjian, it is my understanding that the work at NIST on standards for computerized voting machines was halted this year because of a lack of funding; is that correct?

Dr. SEMERJIAN. Well, things slowed down, let's say, but, in fact, let me make it clear that the standards are not going to be set by NIST. They will be set eventually by TGDC. So TGDC just got started. So we have done, as I pointed out, some of the background work on human factors and on security issues, but as far as setting standards and guidelines, TGDC had to do that, which did not get going until 2 weeks ago.

Mr. CLAY. Let me ask you, what was your budget request for election work for 2004, and what will be your request for 2005?

Dr. SEMERJIAN. There was no request in the 2004 budget. For 2005, the EAC has requested a budget of $10 million for NIST, not for 1 year, but basically for the entire work to be done, which will probably be done over a 3-year period. But I think if that $10 million is provided, we feel that is adequate funding for NIST to get the job done.

Mr. CLAY. OK. NIST has a responsibility under the Help America Vote Act with regard to the development of technical standards for voting systems. When do you think these standards will be ready? And I heard you say in your testimony you have had the initial meeting?

Dr. SEMERJIAN. Right. Basically HAVA legislation requires us to make the first set of recommendations within 9 months after the formation of TGDC. So the clock just started running.

Mr. CLAY. OK. Thank you for those answers.

Mr. CLAY. Mr. Jarrett, the Secretary of State in Missouri has declared that no electronic voting machines will be used in Missouri that do not provide a voter verification paper trail. Has any electronic voting equipment been certified for use in Missouri, and, if so, will any be used in the St. Louis area?

Mr. JARRETT. The answer to that is no, none have been certified. In Missouri, State statute requires that before the Secretary of State can certify equipment for use in Missouri, that it has to be certified to the current standards by an independent testing authority. And as of this date, no vendor has submitted that ITA certification to the Secretary of State, so there will be none used in Missouri this year.

Mr. CLAY. During the debate at the Election Assistance Commission hearing in May, there was a concerned voice by the disability community that computerized voting machines with verified paper

ballots would be a step backward for the visually impaired. In research done by your office, how have you addressed that problem?

Mr. JARRETT. Well, we have looked at, of course, that's a very serious problem, and it is one that I know Secretary Blunt takes very seriously. We have looked at a written opinion from the Department of Justice on that issue that talks about DREs that produce paper ballots; as long as they produce a similar experience for disabled voters, that it complies with HAVA and the Americans with Disabilities Act. And in Missouri, Secretary Blunt has appointed a committee, an equipment certification committee, where we have a representative from a disability advocacy group that's a member, and we also have two members from the blind community that are on the committee. And they have been very helpful in educating the rest of the committee on the disability issues, and they will certainly be very important in certifying. And Secretary Blunt will consider their input before he certifies equipment to make sure that it is accessible to the disabled.

Mr. CLAY. Thank you for your answer.

My time is up, Mr. Chairman.

Mr. PUTNAM. Mr. Holt.

Mr. HOLT. Thank you very much, Mr. Chairman, and I appreciate the opportunity to join you here, and I certainly like the Florida orange juice. That's a nice touch. We all extol the contributions of Florida in the orange juice field.

Mr. PUTNAM. We have to have something positive to say about Florida this morning.

Mr. HOLT. Well, indeed, in 2000, we all got an education. Americans got an education in voting. Many of us who had been involved in the business knew it is complex. As one who won a reelection by less than 1 vote per precinct, I certainly had paid attention to the mechanisms and as well as the technology of voting.

But for most Americans, it was previously thought to be very simple, and I think we have all learned a lot. I think we have learned that we have to hold up the principles that voting will be fair, that it will be accessible, and that it will be verifiable, and it is that latter principle that I wanted to talk about today.

I noticed your hearing calls for technology, accuracy, reliability and security. I would add another, auditability or verifiability, as what we should be looking at today.

And my first question, actually, I guess, is probably for Mr. Hite and for Mr. Semerjian. Considering that it is a secret ballot, is it possible for anyone other than the voter, be it the manufacturer, vendor or election official—is it possible for anyone other than a voter to verify whether the voter's intentions have been appropriately recorded?

Mr. HITE. I have never pondered that question before, so that is why I pause.

Mr. HOLT. I think it is the fundamental question here.

Mr. HITE. My quick response to that is I don't think it is possible for anyone other than the voter to know the voter's intent and be able to verify the voter's intent. You would have to require some element of the voter's interaction to do that.

Mr. HOLT. Dr. Semerjian.

Dr. SEMERJIAN. Well, let me perhaps answer a different and related question.

Mr. HOLT. OK.

Dr. SEMERJIAN. That is the fact that the paper ballot is verified does not necessarily mean that the computer-recorded vote is verified. I mean, they are related, but they are two different things. So I think we need to make sure that we should not be satisfied simply by saying the paper ballot, the paper ballot is the intent of the voters.

We need to make sure that the computer-recorded vote records properly the intent of the voter, and I think that's done through a proper testing, through providing proper security and data integrity measures.

Mr. HOLT. Well, let me follow on that point, Mr. Semerjian. In your testimony you talk about performance-based standards. I take that to mean you like to look at the outcome in an applied way, where it is actually used in the field, to see whether the result is correct, rather than relying on procedures that the room is locked, and that no one else has access to the software or whatever training and procedural steps one takes. So, given that, with performance-based standards, how can you know whether a machine has an error in it, perhaps in a software, perhaps unintentional, perhaps hacked? How can you know that on a performance basis?

Dr. SEMERJIAN. Well, that's normally done by subjecting the equipment that is being tested to certain inputs. Statistically——

Mr. HOLT. But that's beforehand. That's not performance-based. As I understand what you mean by performance-based standards, you want to know whether, as it is used in the field, whether the numbers match up with some independent measurement.

Dr. SEMERJIAN. The idea of the performance-based standard is not to simply say you have to do this and that and the other thing, but to simply say, OK, if applied, if I use that equipment the way it is supposed to be used. Then does the machine, at the end, produce the exact input as an output? That's really what is meant by performance standard—and with what level of accuracy? I mean, is there a discrepancy at the 1 percent level, or what is our expectation; is 1 percent acceptable, or 5 percent?

Those are the kinds of standards we can accept, not telling vendors that you have to do this, you have to save the data this way, etc. I think we want to leave the creativity, the innovation part to the vendor, but require them to deliver an equipment, the machine, that provides 100 percent accurate performance.

Mr. HOLT. Well, the time is up. I am not sure I got an answer to how do you know whether the machine has been hacked or not, but time has expired, so thank you.

Thank you, Mr. Chairman.

Mr. PUTNAM. Thank you.

Mr. Hite or Dr. Semerjian, do you know how many individual election units there are in this country, how many precincts there are in this country?

Mr. HITE. The numbers I have seen on the precincts, are on the order of 193,000.

Mr. PUTNAM. 193,000 precincts, and presumably some of them in very rural areas might just have one or two machines, and another might have a couple of dozen?

Mr. HITE. I was speaking to precincts, polling places, in terms of jurisdictions, voting jurisdictions, there's only on the order of 10,000. Each of these precincts have multiple polling places associated with them.

Mr. PUTNAM. So there are 193,000 polling places?

Mr. HITE. Correct, where you go to vote, the local school, church.

Mr. PUTNAM. Right. Each of which may have one or two machines or private little areas where you go do your paper ballot, pull the paper ballot or lever or whichever it may be, up to a dozen at each precinct, something like that.

Mr. HITE. Configurations go by equipment and size.

Mr. PUTNAM. But we are talking about a lot?

Mr. HITE. Yes.

Mr. PUTNAM. It could be several hundred thousand starting at a baseline of almost 200,000?

Mr. HITE. Yes.

Mr. PUTNAM. So, let me just say something about Florida, because I think it is important. Anyone could have been Florida in 2000, and, in my opinion, we haven't passed any regulation that will prevent another Florida in 2004. Nothing we have done, nothing we will talk about, nothing we can do will prevent a close election, which is really what happened.

I mean, when you talk about what happened in Florida, you had a close election, and it was not the first time that it had happened. Even in my short time, county commissioners have been elected and then unelected because the outcome of a vote turned by five votes or three votes, because there were human beings involved and somebody forgot to—the deputy who delivered the boxes of ballots to the central accounts location thought he had unloaded all the ballots and found another box in his car the next morning, or the very well-meaning, well-trained coworkers just picked up three paper ballots, and they thought they only had one, fed it into the machine, and so the top one was red, the bottom two were not.

When you get down to several hundred thousand machines counting millions of votes, there will be errors, because humans are involved. So let me just ask what the HAVA act will do to prevent the same errors, the same oversights, the same mistakes that were made in 2000. What has changed as a result of that legislation?

Mr. HITE. I don't believe that the HAVA act will fundamentally change that for the 2004 election. The HAVA act has in it provisions for long-term improvement in this area, as well as short-term, because steps have already been taken by the EAC in a relatively short amount of time to recognize and inform and educate the jurisdictions about where improvements can be made in the near term to minimize the chance of those errors. We are never going to get rid of them. That's what we are trying to do is minimize them. And whether similar problems will surface in 2004, I would be shocked if they didn't, and particularly because the whole election process is going to be under such a microscope now and going forward. But what we are talking about, what HAVA does,

and what we are talking about doing near term and long term, is to reduce the probabilities of this happening.

Mr. PUTNAM. Is there a margin of error in every voting process and voting technology that is deployed today?

Mr. HITE. There is a margin of error in every process involved in any type of business or government activity, including air traffic control, for example, where you want accuracy down to five nines, so it is inevitable.

Mr. PUTNAM. Over the long term, is a paper trail the way to go? Is a paper trail the best, most effective way to audit the results of an election?

Mr. HITE. I believe a paper trail can offer a layer of security with respect to DREs. Now, it all depends on how you use that paper trail. Just having the paper receipt and having the voter look at it in and of itself doesn't give you a whole lot. But if you implement it in a way where you have some means to know whether or not the machine is capturing the vote as it is on the paper receipt, now you have added a level of security.

As with any decision about security capabilities, you have to make those decisions in the context of risk. What is the threat, what are my vulnerabilities, and how much am I willing to pay to reduce the risks associated with those two variables? And so you have to make decisions about that. You don't just throw money at something. You make good, fact-based decisions.

Mr. PUTNAM. And I would submit that time is also a factor, because it becomes a deterrent to voting, depending on how long it takes for all this verification to occur.

Dr. Semerjian, I want you to answer that question, and then we will yield to Mr. Clay.

Dr. SEMERJIAN. Well, I agree with what was said. I don't think I have anything to add. There is an uncertainty with every process. And the whole point is, how do you reduce that uncertainty to an acceptable level? So whether you expect 100 percent accuracy, which is almost unattainable, or whether 99.9 percent is acceptable or whether it is 95 percent, I think we certainly want to set standards that push that level, that level of certainty, or reduce the level of uncertainty as much as possible. And that can be done through proper testing and setting the proper standards to start with.

Mr. Chairman, may I answer, sir, the question that Mr. Holt asked that I could not answer?

Mr. PUTNAM. Sure.

Dr. SEMERJIAN. Regarding hacking, how do we know that it's hacked?

Mr. HOLT. Or error of any sort.

Dr. SEMERJIAN. Well, this is work in progress. As I said, TGDC had the first meeting. But one of the issues that they already addressed is this issue: How do we know that the software on a particular machine is not hacked or modified or changed by mistake? And we do have a National Software Reference Laboratory at NIST that we use for this kind of applications. We haven't used them for the voting process, but we have used it where at different stages of a process you can actually check the integrity or the signature of a particular software package, so that once you have established this referenced initial certified version of a software, you can check

against that at different stages so that there are no mistakes made in duplication, or, changes by mistake, so that you can verify the integrity of that software from the very beginning of the process to the very end where it is loaded to individual machines.

So we haven't worked out all the details, but I think that the technology is there to be able to say that this particular software package is not what it was at the beginning of the process, that something has changed, and alert the officials that some action needs to be taken.

Mr. PUTNAM. Mr. Holt, how about if I just go ahead and recognize you for your second wave of questions?

Mr. HOLT. Well, just following on that point. In fact, that is right; the way you test software is you see whether it gives the right answer. In other words, you audit it. You compare it against another approach to that same calculation to see if it gives the same result. And you do that at each stage along the way. You also check the software to see whether it is robust in various ways.

Dr. SEMERJIAN. May I say something?

Mr. HOLT. Yes.

Dr. SEMERJIAN. This is not only substantiating the result of the computation, because the program can give you the same result but in the meantime could produce some output of some other source. Here, the idea is to check the integrity of the entire software package.

Mr. HOLT. That is right. Step by step, you audit it.

Dr. SEMERJIAN. Well, it is more than that.

Mr. HOLT. And you compare each operation to see whether that operation does what you think it does.

Dr. SEMERJIAN. It is more than that. If any kind of a statement is changed in that software—which may still give the same answer—if any code is changed, the signature of the code will be changed. So even two codes that give the same answer may be slightly modified. And this kind of technology will detect that.

Mr. HOLT. That is external hacking. That might or might not find an embedded problem, an embedded bug that has been in there since it was written or since it left the package.

Dr. SEMERJIAN. That is where the certification process comes in.

Mr. HOLT. But, anyway, my point is the way you know anything, the way anything of value should be subject to audit—and my point is, if in fact the answer to my first question is that only the voter can verify his or her intentions are properly recorded, then the only audit that makes sense is to compare the result against what the voter has verified. But let me go on to a couple of other questions.

Mr. Hite, what do you think—you say in your testimony that we have to make sure that the people who work with these devices are well trained and have the requisite knowledge. What is the requisite knowledge to operate today's BREs? Is it more or less than the knowledge to maintain, say, keeping track of optical scan paper for the election workers?

Mr. HITE. What I can offer there as part of our survey of jurisdictions, in 2001 we asked local jurisdictions about whether or not DREs versus optical scans, etc., how difficult they were for operators, poll workers to use, or for voters to use, or how difficult it was to correct somebody's vote who made a mistake versus the different

types of technology. And in general, DREs were easier to operate than the optical scan and the other types of voting systems.

Specifically in terms of the training that is needed for a given poll worker, a given maintenance individual, anyone who has to interact with that system, that is going to vary by jurisdiction and by type of system because there's different rules and standards that govern how these elections are conducted—and we can use Missouri as an example of that.

Mr. HOLT. So if there are 50 million people this year who will be asked to vote on electronic machines, maybe 30 million will actually show up and vote. For those 30 million votes this year, what would you recommend is the best near-term solution to protect the integrity?

Mr. HITE. Coming from an organization where we don't make rash decisions or take or quick positions on things, I'd go back to what I said before. It requires a level of understanding and visibility into those systems—make and model of those systems—to know how they behave and know what their strengths and weaknesses are. I just don't have that because I haven't done that type of analysis on a system-by-system basis. And so my position would be that is the kind of decision that you want to make with the long-term focus in mind. You want to base it on some good data that talks about what are the vulnerabilities of those systems and what is the best way to implement paper receipts if you choose to do that. I am just not in a position to give you the answer that you are looking for. I don't have that kind of knowledge.

Mr. HOLT. And with my time expired, I just want to thank the Show Me State and Secretary Blunt for his, I think, intelligent approach to this and his leadership.

And thank you, Mr. Chairman.

Mr. PUTNAM. Mr. Clay.

Mr. CLAY. Thank you, Mr. Chairman.

Mr. PUTNAM. And I will note for the record the presence of the gentlelady from Ohio, Ms. Kaptur. Without objection, you are certainly welcome to join us, and we are delighted to have you here and certainly hope that should you wield the gavel in your appropriations subcommittee, that I will be accorded the same treatment when you all are——

Ms. KAPTUR. Yes.

Mr. PUTNAM. Thank you.

Mr. Clay.

Mr. CLAY. Thank you.

Mr. Hite, the California Secretary of State has established a set of safety criteria that, if met by election officials, will allow the recertification of the computerized voting machines. Would you comment on the adequacy of those recommendations?

Mr. HITE. Yes, sir. I am aware, as you say, that there are these 23 conditions. I am not, unfortunately, familiar with those 23 conditions so that I can offer an informed opinion on it. So I apologize for that.

Mr. CLAY. In your full written testimony, you state that current touch-screen electronic voting machines can produce images that can be printed, but explain that this is according to vendors. Did

GAO investigate whether the machines currently in use do in fact have this potential?

Mr. HITE. No sir, we did not. We have done no code reviews or any testing or evaluation of specific make and models to determine what features are implemented and whether or not they have been implemented properly. I believe that other witnesses at this hearing have much more in-depth knowledge about the specific make and models.

Mr. CLAY. Thank you.

Dr. Semerjian, when the new standards are ready, what do you suggest that States do if they have already purchased voting machines with HAVA funds and then find out that the new machines are not HAVA compliant? What should they do?

Dr. SEMERJIAN. I am not quite sure how to answer that question.

Mr. CLAY. I want to hear your answer.

Dr. SEMERJIAN. I think this is exactly the issue they are struggling with. They feel that they are between a rock and a hard place, because they need to make some changes perhaps, and yet the information that they need to make informed decisions regarding purchases is not available. So, I mean, I really feel for them, but unfortunately the timing was such that these standards could not be provided in time certainly to affect this year's elections, but we hope that they will be for the 2006 elections.

Mr. CLAY. So some States got ahead of everyone else because of HAVA, and now that may come back to bite them?

Dr. SEMERJIAN. Well, I mean, this is strictly conjecture on my part. But I mean, it sort of depends on what the changes needed will be. I mean, if there are software changes, they certainly can be made relatively inexpensively. But if there are going to be major hardware changes, obviously they will be more costly.

Mr. CLAY. Let me also ask, whose job is it to assure that electronic voting machines are free of malicious code and actually register the votes as intended? Whose job would that be?

Dr. SEMERJIAN. Elections are run, to the best of my knowledge, by local officials. So it is their responsibility to ensure the integrity of the voting process. The EAC, TGDC, and other organizations try to provide them with the information, knowledge, and the tools, technology tools to make that job as tenable as possible. But at the end of the day, it is the local officials' responsibility to ensure the integrity of the voting process.

Mr. CLAY. Thank you for those responses.

Mr. Jarrett, it is my understanding that none of the touch-screen machines now on the market have been certified to the 2002 standards. Is that correct?

Mr. JARRETT. That is my understanding as well.

Mr. CLAY. Did the lack of certification play a role in the Missouri Secretary of State's decision to defer the use of computerized voting machines in Missouri?

Mr. JARRETT. Yes. Again, our State statute requires that anytime that the Secretary of State certifies equipment, it has to be certified by an ITA to the current standards, which are the FEC 2002 standards currently, d will be the EAC standards when the Standards Board and the TGDC sets those standards. So, yes, it played the major role, as a matter of fact.

Mr. CLAY. I thank you for your response and the entire panel being here.

Mr. Chairman, I yield back the balance of my time.

Mr. PUTNAM. Thank you, sir.

Ms. Kaptur.

Ms. KAPTUR. Yes, Mr. Chairman. Thank you so much for allowing us to participate in your important hearing this morning and also for the Florida orange juice. I now had that for breakfast and for lunch, and appreciate the work that the people of your State do for the rest of the world.

Thank you very much. And I wanted to thank the witnesses for producing this excellent report this morning. This is a topic on which we in Ohio are very, very focused, and appreciate your diligence.

I think more oversight is better than less oversight. I know that Congressman Clay in our conversations has been trying to receive information from those of us not on this subcommittee, not on this full committee, in the important area of voting technology and reform. And I just thought I would state for the record, and I will put the full information in the record, that in Ohio, about a year ago, five technologies that were being considered were displayed at our Statehouse in Columbus, OH. And at that time, not being a computer technology expert, I asked three of our major universities to select the best people they had, and they chose the people in charge of their computer security to go down and review the technologies on display. And I won't read you their full report, but I will read you some of the conclusions:

No technology currently under consideration had attributes that made it both secure and readily accessible for use. All of the technologies had serious shortcomings in these two major elements:

None of the security mechanism force of the voting systems that remained in consideration in Ohio could sufficiently prevent fraud or abuse.

The integrity of the voting process as well as voter confidence could be compromised through the absence of an auditible paper trail at each precinct. Without rigorous testing by multiple outside agencies with appropriate technical expertise, assurance of a secure era of tamper-proof electronic election system cannot be obtained. Levels of computer proficiency among the electorate vary and tend to disfavor the elderly, minorities, and the economically disadvantaged.

And we saw that in the election called the test election, which was held last year in which the technologies were employed.

And, finally, while electronic voting is a viable option that can be successfully implemented, it must use secure disciplines to gain the public's confidence.

After that information came to me, it got my attention, and particularly because our State was trying to get our local counties to purchase equipment and to sign contracts. And after my family and I voted in November, I sent a letter to our Secretary of State, November 10, 2003—and I am placing this in the record—to which I have received no response. But I would ask you if you are capable to answer any of these questions.

I explained in the letter that when we voted at our polling place, we actually chose the paper ballot rather than using the electronic device that was also an option. When we completed the paper ballot, we gave it over to the election official who put it in an optical scan. And our ballots, when it went through the scan, were physically stored in the back of the machine and at the end of the day the physical ballots could be tallied against the totals provided by the scanner. And, thus, we felt confident that our votes had been counted and that, if necessary, an auditible trail would be present at the precinct level, which is how we vote in Ohio. We count at the precinct level.

The people, however, who in that same precinct chose to use the electronic device, I would ask the question, how would their votes be counted? Where exactly is their vote in that machine? That is the first question. How and where were their votes counted at the end of the day? Will the touch-screen system produce an auditable paper trail of votes at the precinct level? And, if not, what happens to the votes on the disk once those votes leave the precinct? Who controls the disk? And is any tally left at the precinct level?

To date, our Secretary of State has not chosen to answer this letter. I am just curious, how would you go about perhaps, if you can, answering any of the questions that I have asked?

Mr. PUTNAM. Did you write all that down?

Mr. HITE. Well, actually, I didn't need to write it down because, unfortunately, the answer to the question is, it depends. And it is going to depend on the specific make and model of the equipment that is being used there and the set of procedures that are being employed to govern the extraction of those votes and the transportation of those votes, whether it is on disk or electronically. So there is so many things that are peculiar to your situation that we don't have privy to and are not in a position to answer, but certainly your Secretary of State should be in a position to answer.

Mr. PUTNAM. Anybody else want a crack at that?

Mr. JARRETT. Certainly in Missouri, Secretary Blunt has said that he is not going to certify any DREs unless they do provide a voter-verified paper ballot. So, in Missouri, that will be the standard. There will be a paper backup.

Ms. KAPTUR. And that paper backup would be at the precinct level? Do you count the votes at the precinct level in Missouri?

Mr. JARRETT. No. They are counted back at the central office. But, yeah, that will be available at the precinct level. I think Secretary Blunt envisioned a system where the paper ballot would either be behind glass and where the voter couldn't touch it, it would simply drop into the ballot box. Or, even where the voter would get the ballot, paper ballot, and put it in a ballot box so that the voter could see it before they hit the final button casting their ballot to make sure that it is what they intended.

Mr. PUTNAM. The gentlelady's time has expired.

The subcommittee will accept any final comments that the first panel would like to make, if you have any. If there are some last words, a question you wish you had been asked, something you would like to answer, this is your opportunity. And then we will recess and set up the second panel. Any final comments from the

first panel? Very good. The subcommittee will stand in recess. We will arrange the witness table for the second panel.

[Recess.]

Mr. PUTNAM. The subcommittee will reconvene. The witnesses will please rise for the administration of the oath.

[Witnesses sworn.]

Mr. PUTNAM. I would note for the record that all the witnesses responded in the affirmative. We will move directly to witness testimony.

The first witness is Dr. Aviel Rubin. Dr. Rubin is professor of computer science and technical director of the Information Security Institute at Johns Hopkins University. Prior to joining Johns Hopkins, he was a research scientist at AT&T labs. Dr. Rubin has authored and coauthored several books on Internet security. He serves on the board of directors of the UFE&IX Association and on the DARPA Information Science and Technology Study Group. Dr. Rubin is coauthor of a report showing security flaws in a widely used electronic voting system that focused a national spotlight on the issue.

In January of this year, Baltimore Magazine named him Baltimorean of the year for his work in safeguarding the integrity of our election process, and he is also a recipient of the 2004 Electronic Frontiers Foundation Pioneer Award. Weather to the subcommittee. You are recognized for 5 minutes.

STATEMENT OF AVIEL RUBIN, TECHNICAL DIRECTOR, INFORMATION SECURITY INSTITUTE, DEPARTMENT OF COMPUTER SCIENCE, JOHNS HOPKINS UNIVERSITY

Mr. RUBIN. Thank you, Mr. Chairman, Mr. Clay, Mr. Holt, and Ms. Kaptur. In addition to all of that, I just want to introduce that I served as an election judge on Super Tuesday in March, in Baltimore County, to gain experience with actually helping to run an election.

My belief, after studying the code in the Diebold DREs is that the DREs that are in use right now and that will be in use in November are poorly designed, insecure, and that they should not be used. The Secretaries of State of California and Ohio—and, I now learned, Missouri as well—have come out with statements backing this opinion.

I have two major concerns, and to some degree they are mutually exclusive. Let me describe the first concern.

The first concern is that something very bad will happen in November in the election due to the insecure machines. They could fail in a catastrophic way. They could get a result that is obviously wrong. And what would we do? There would be no ballots to recount. They could fail in a way that is wrong, that could get a result that is wrong but not obvious. We don't know how likely that outcome is.

Let me talk about my second concern. My second concern is that nothing bad will happen, and that will be used as an argument to say that the machines are secure. Some people already are saying that the machines are secure because we have had no failures in the past. This would give them more ammunition to continue to say that the machines are secure. The lack of an obvious failure

does not mean that the machines are secure. We have a vulnerability here. We have fully computerized machines that can be read, they can be read without anyone even knowing it, and even if the machines are open source. Just because this software is available for inspection does not mean there isn't something hidden inside of it that cannot be found. I do not believe it is possible to find all of the problems that could exist in software, even by really good experts.

Let me give an analogy. You might drive without a seat belt, and if a bad accident happens to you and you get really hurt, there is no consolation in me saying, I told you so. But if there is no accident, that does not mean that it was safe.

On November 2nd, 30 percent of American voters will be driving without a seat belt. If there is no apparent incident, that does not mean it was safe to do so.

My primary concerns with today's DREs are that there is no way for voters to verify that their votes were recorded correctly. There is no way to publicly count the votes, no way to count the votes so that people can watch and be sure that the counting is legitimate. In the case of a controversial election, a meaningful recount is not possible. The machines must be completely trusted not to fail, not to have been programmed maliciously in the first place, and not to have been tampered with. In Diebold's machines we found gross design and implementation errors when we looked at the code.

The current certification process resulted in these machines being approved for use and are being used in elections.

I am often asked, how do the other vendors compare to Diebold? And I have to say, I don't know; nobody will let me look at that their system.

We often find ourselves in these kinds of hearings, and election officials will pull out—and I just learned we are going to have a similar demonstration today—a 10-foot long ribbon that shows what a paper ballot might look like. And I would say, yes, if you designed the absolute worst paper ballot that you could think of, it would look like that. Why don't we start with something like the absentee ballots that they are using, and show that is what a ballot could look like? In fact, that absolutely worst possible design of a paper ballot probably includes all of the choices that were not made by the voters as well.

I don't think that this is an insurmountable problem. I believe that we can design voting systems that are accessible to the disabled, that provide voter verifiability to the voters, and that raise the bar in security past the threshold that I need to be past, and we are way below that threshold right now.

In conclusion, accessibility and security are not mutually exclusive. They should not be portrayed that way. We need to develop systems that do not require completely trusting the vendor with the outcome. We need to develop systems that are auditable, including the ability to perform a recount that is recounting the voter's intent. Systems where voters know that their completed ballots

are recorded correctly need to be developed, and we need to develop a transparent process without secret code. Today's DREs have none of those properties. Thank you.

Mr. PUTNAM. Thank you very much.

[The prepared statement of Mr. Rubin follows:]

Testimony: Government Reform Committee's Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census

"The Science of Voting Machine Technology: Accuracy, Reliability, and Security."

Dr. Aviel D. Rubin, Professor of Computer Science
July 20, 2004

My name is Avi Rubin. I am a Professor of Computer Science and Technical Director of the Information Security Institute at Johns Hopkins University. I am author or co-author of several widely used books on the subject of computer and network security, and I have chaired several of the top security research conferences. I received my Ph.D. in Computer Science from the University of Michigan in 1994 in the specialization of Computer Security. I have been researching security issues related to electronic voting since 1997. Last year, by invitation of the Department of Defense, I served on the security peer review group of the SERVE voting system for absentee voting for military personnel and overseas civilians. I also participated as a panelist in the 2000 National Science Foundation study of the feasibility of electronic voting. Last year, my research team analyzed the code used in the Diebold Accuvote TS and TSx and wrote a report citing many security flaws that we found. Our study was published in the top peer reviewed computer security conference, the IEEE Symposium on Security and Privacy. I am a member of the National Committee on Voting Ingerity, and in March, I served as an election judge in Baltimore County where Diebold Accuvote TSx machines were used.

I am here as an expert in a particular domain, namely computer security. I recognize that voting is a complicated issue with a diverse set of values, each of which is very important to the functioning of this process in a way that is reliable and trustworthy in the broadest sense. Security is a necessary component of a fair and accurate election process. However, there are other equally important components. Making sure that everyone can participate in a way that is private and independent is also key to our electoral process. Making sure that people from all walks of life can participate in the process in a language they can comprehend is also important. An accurate and secure system that limits the ability of individuals with disabilities and language minorities would fall short of meeting the goals of our democracy, as would a system that allowed everyone to participate but failed to protect the integrity and accuracy of their vote. Luckily, security and accessibility are not competing goals. While today's DREs increase accessibility, they do not provide adequate security. Appropriately designed voting systems, can provide accessibility and security. Our commitment to a fair, inclusive, secure election process requires us to demand both from our election machinery.
I come before you today to contribute my expertise garnered over years of experience. You will hear from experts representing the disability community and the civil rights community. They are experts in their domains. I am an expert in computer security. Given that we all agree that security is an important component of elections, I ask that you hear me and understand the serious nature of my critique of current DREs.

My primary concerns with today's DREs are:

- There is no way for voters to verify that their votes were recorded correctly.
- There is no way to publicly count the votes.
- In the case of a controversial election, meaningful recounts are impossible.
- The machines must be completely trusted. They must be trusted not to fail, not to have been programmed maliciously, and not to have been tampered with at any point prior to or during the election. We have techniques for building secure systems, and they are not being utilized.
- With respect to the Diebold Accuvote TS and TSx, we found gross design and programming errors, as outlined in our attached report. The current certification process resulted in these machines being approved for use and being used in elections.
- We do not know if the machines from other vendors are as bad as the Diebold ones because they have not made their systems available for analysis.

Since our study came out, three other major studies often referred to as the SAIC report, the Ohio reports, and the RABA report, all cited serious security vulnerabilities in DREs. RABA, which is closely allied with the National Security Agency, called for a "pervasive rewrite" of Diebold'scode. Yet, the vendors, and many election officials, such as those in Maryland and Georgia continue to insist that the machines are perfectly secure. I cannot fathom the basis for their claims. I do not know of a single computer security expert who would testify that these machines are secure. I personally know dozens of computer security experts who would testify that they are not.

I have been disappointed that the policy community did not reach out to the computer security community when making decisions about voting technology, and when my community came to the table, they said it was too late. At this point the failures of current DREs have been documented in four major studies by leading computer security experts, and we have ample field experience documenting failures at the polling place. Yet computer security experts, myself included, find ourselves routinely referred to as luddites and conspiracy theorists. Failing to confer with computer security experts in decisions about voting technology was a mistake. Given the gravity of the security failings the computer security community has documented in current DRE systems it is irresponsible to move forward without addressing them.

Addressing the problems I and others have documented with DREs requires more than just fixing the machines. We must reform the process for establishing voting technology to provide transparency. Vendors are not subject to public code review. In the one instance where independent security experts had an opportunity to examine a voting system, the results proved that the current process results in machines being deployed with unacceptable lack of quality control. We cannot achieve perfectly secure systems; such things do not exist. But on the spectrum of terrible to very good, we are sitting at terrible. Not only have the vendors not implemented security safeguards that are possible, they have not even correctly implemented the ones that are easy.

The defenders of the DREs do not account for the ease with which a malicious programmer could rig an election. It is much easier to hide malicious code in software than it is to detect it. Without an external check on the system, a fully electronic voting machine cannot be properly audited. Research needs to be done on how to design auditable and voter verifiable elections. The best way to achieve this today is with a paper ballot that voters can verify. There is no reason why touchscreen machines cannot be used to generate ballots, but they should not be used to tally votes. The tallying software should be as compact as possible, and it should be available to the public for inspection.

I'd like to stress one important point. Security and functionality are completely different things. Functionality is whether or not something works when it is used as planned. Functionality can be tested, and the tests can be used to make predictions about the future behavior of a system. Security, on the other hand, has to do with how a system behaves under unanticipated circumstances with an active, dynamic adversary trying to subvert it. By definition, you cannot test a system for security the way you test for functionality. It is inappropriate and incorrect to draw conclusions about the security of a system based on its past performance. The fact that this argument is consistently put forward in defense of the security of the DREs demonstrates just how much real security expertise is needed in this process. You would not design a heart implant without feedback from cardiologists. You would not design defense systems for the physical security of this country without consulting military experts, and you should not design systems for computerized elections in this country without consulting computer security experts. I can assure you from my analysis of the Diebold machines that no such expertise was utilized.

In conclusion, my colleagues and I have presented our analysis to many different groups of computer scientists, including the National Science Foundation, the National Academy of Science, and several security conferences. We have won awards for this work, and the community at large is in strong agreement with our conclusions. I recommend that you continue to seek broad input from the computer science and the computer security communities. These people have a long history of experience with designing mission critical systems. The opinions of the experts in this matter are quite different from the picture being painted by the vendors and some state officials, all of whom have much less expertise, or no expertise whatsoever, in computer security.

Mr. PUTNAM. Our next witness is Dr. Michael Shamos. Dr. Shamos is a distinguished career professor in the school of computer science at Carnegie Mellon University where he serves as co-director of the Institute for E-Commerce, and the director of the Center for Privacy Technology. He is also editor in chief of the Journal of Privacy Technology.

From 1980 to 2000, he was statutory examiner of computerized voting systems for the Secretary of the Commonwealth of Pennsylvania. From 1987 to 2000, he was the designee of the Attorney General of Texas for electronic voting certification. During that time, he participated in every electronic voting examination conducted in those two States, involving over 100 different voting systems, accounting for more than 11 percent of the popular vote of the United States in the 2000 election.

He is the author of "Electronic Voting: Evaluating Threat," and "Paper V-Electronic Voting Records: An Assessment." He is a member of the Serve Project Review Group, and the recent National Research Council Workshop on Electronic Voting.

Welcome to the subcommittee. You are recognized for 5 minutes.

STATEMENT OF MICHAEL SHAMOS, PROFESSOR, CARNEGIE MELLON, DIRECTOR, UNIVERSAL LIBRARY; CO-DIRECTOR, INSTITUTE FOR E-COMMERCE

Mr. SHAMOS. I thank you, Mr. Chairman, members of the committee, and visiting members. This hearing is about the science of voting machine technology. There presently is no such field of science, if by science we mean an organized experimental discipline with authoritative principles and published journals. The reason is that until the year 2000, it was difficult to interest scientists in a problem so apparently trivial as counting ballots.

As we saw in Florida in 2000, it is not a trivial problem, and we desperately need a field of voting science. However, there is no systematic science of voting machine technology, no engineering journal devoted to the subject, no academic department nor even a comprehensive textbook. There are no adequate standards for voting machines nor any effective testing protocols. It is only a set of minimum statutory requirements, public budgets, and the law of the marketplace that have shaped the development of voting machines.

When a flaw is detected in a voting machine, there is no compulsory procedure for reporting it, studying it, repairing it, or even learning from the experience. The voting machine industry is unregulated and has not chosen to regulate itself. I don't believe the public will long tolerate such a situation.

While recent newspaper articles and statements by certain computer scientists have shed doubt on the ability of direct recording electronic machines to count votes securely and reliably, it should be noted that in the 25 years these machines have been used in the United States, there has not been a single verified incident of tampering or exploitation of a security leak.

The concerns have been expressed and, unfortunately, taken up with unjustified gusto by the popular press, representing a hypothetical rather than a real threat to the electoral process. Various design flaws and potential avenues of attack have been verified,

and it is important to analyze and repair them rather than to flee to methods of voting that are even less safe.

For reasons of cost and convenience, evolution of voting systems has tracked that of personal computers. As we now know, the operating systems of such machines are highly vulnerable to attack and infiltration by malicious software such as viruses.

In addition, the temptation to connect voting machines together by networks and link them to central counting stations through telecommunications has introduced new vulnerabilities not previously seen. The only set of standards used to evaluate voting systems, the Federal Voting Systems Standards, FVSS, now the province of the Election Assistance commission, have not kept pace with either developments or threats. For example, these standards place responsibility for virus protection and elimination on the vendor, and provide for no test procedures by which the presence of viruses or the susceptibility of a system might be determined.

An example of disorganization in the field of voting technology is the recent popular call embodied in several bills now before Congress to add paper trails to existing voting machines in the vain belief that this would suddenly make untrusted machines trustworthy.

No scientific study has been performed comparing the security of paper ballots to electronic records, yet fear of the machines is so prevalent that entire States are now insisting on the introduction of a technology that does not yet exist to solve a problem that has never been observed.

I could give testimony for 2 hours on exactly how one can take any method of voting that is performed with paper ballots or paper devices, and I can explain in detail numerous methods of tampering with a ballot. If I were to do that, one of the effects would be that many Americans would not go to the polling places this November because they would have no faith in any method of voting.

I believe this situation has occurred, because allegations have been made that voting machines jeopardize democracy. But there is no engineering study available to rebut the allegation, and we need one.

The scientific establishment of the United States needs to be mobilized to investigate the problem. Some efforts are already underway in this regard. Last week, the National Research Council convened a committee of approximately 20 experts on voting technology and election practices to formulate a set of questions for further study, but the investigation is as yet unfunded and may take several years to complete. The National Science Foundation should fund proposals to study various aspects of voting.

Other than health and nuclear safety, it is difficult to think of a more pressing subject for NSF support. HAVA, the Help America Vote Act of 2002, tasks the National Institute of Standards and Technology with major technical responsibility for guiding the development of voting systems standards. Yet this effort remains tragically unfunded. Section 273 of HAVA authorized an appropriation of $20 million for research on voting technology improvements during fiscal 2003. The total actual appropriation was zero dollars, and no authorization even exists for 2004.

I have heard it expressed that Congress wants to give HAVA a chance to work before enacting further voting legislation, but it is elementary that HAVA cannot work if it is never implemented. As scientists have begun to study voting seriously, a number of revolutionary breakthroughs have occurred that can allow a previously unheard of degree of transparency in the process of voting and tabulation. For example, you will hear later, right after me, about a system called VoteHere. Also, because of a development by computer scientist David Chaum, it is now possible to accord each voter the ability after voting has taken place to verify that her vote has not only been counted but counted correctly. It is also feasible for any member of the public independently to verify the correctness of the tabulation, and to be sure that no unauthorized votes have been added to the total, all of this without compromising the secrecy of the ballot. Technologies such as these need Federal support in order to flourish.

I thank you for the opportunity to testify today.

Mr. PUTNAM. Thank you very much.

[The prepared statement of Mr. Shamos follows:]

Testimony of Michael I. Shamos
Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census of the U.S. House of Representatives Government Reform Committee

Oversight hearing on "The Science of Voting Machine Technology: Accuracy, Reliability, and Security," July 20, 2004

Mr. Chairman: My name is Michael Shamos. I have been a faculty member in the School of Computer Science at Carnegie Mellon University in Pittsburgh since 1975. I am also an attorney admitted to practice in Pennsylvania and before the United States Patent and Trademark Office. From 1980-2000 I was statutory examiner of electronic voting systems for both Pennsylvania and Texas and participated in every voting system examination held in those states during those 20 years. In all, I have examined over 100 different electronic voting systems, used to count over 11% of the popular vote of the United States in the 2000 election.

This hearing is about the science of voting machine technology. There presently is no such field of science, if by science we mean an organized experimental discipline with authoritative principles and published journals. The reason is that until the year 2000 it was difficult to interest scientists in a problem so apparently trivial as counting ballots. As we saw in Florida in 2000, it is not a trivial problem and we desperately need a field of voting science.

However, there is no systematic science of voting machine technology, no engineering journal devoted to the subject, no academic department, nor even a comprehensive textbook. There are no adequate standards for voting machines, nor any effective testing protocols. It is only a set of minimum statutory requirements, public budgets and the law of the marketplace that have shaped the development of voting machines. When a flaw is detected in a voting machine, there is no compulsory procedure for reporting it, studying it, repairing it or even learning from the experience. The voting machine industry is unregulated and it has not chosen to regulate itself. I do not believe the public will long tolerate such a situation.

While recent newspaper articles and statements by certain computer scientists have shed doubt on the ability of direct-recording electronic machines (DREs) to count votes securely and reliably, it should be noted that in the 25 years these machines have been used in the United States, there has not been a single verified incident of tampering or exploitation of a security weakness. The concerns that have been expressed, and unfortunately taken up with unjustified gusto by the popular press, represent a hypothetical rather than a real threat to the electoral process. Various design flaws and potential avenues of attack have been identified, and it is important to analyze and repair them, rather than flee to methods of voting that are even less safe.

For reasons of cost and convenience, evolution of voting systems has tracked that of personal computers. As we now know, the operating systems of such machines are highly vulnerable to attack and infiltration by malicious software such as viruses. In addition, the temptation to connect voting machines together by networks and link them to central counting stations through telecommunications has introduced new vulnerabilities not previously seen. The only set of standards used to evaluate voting systems, the Federal Voting Systems Standards (FVSS), now the province of the Election

Assistance Commission, have not kept pace with either developments of threats. For example, these standards place responsibility for virus protection and elimination on the vendor, and provide for no test procedures by which the presence of viruses or the susceptibility of a system might be determined.

An example of disorganization in the field of voting technology is the recent popular call, embodied in several bills now before Congress, to add paper trails to existing voting machines in the vain belief that this would suddenly make untrusted machines trustworthy. No scientific study has been performed comparing the security of paper ballots to electronic records, yet fear of the machines is so prevalent that entire states are now insisting on the introduction of a technology that does not yet exist to solve a problem that has never been observed.

I believe this has occurred because allegations have been made that voting machines jeopardize democracy, but there is no engineering study available to rebut the allegations. We need one. The scientific establishment of the United States needs to be mobilized to investigate the problem. Some efforts are already underway in this regard. Last week, the National Research Council convened a committee of approximately 20 experts on voting technology and election practices to formulate a set of questions for further study, but the investigation is as yet unfunded and may take several years to complete. The National Science Foundation should fund proposals to study various aspects of voting. Other than health and nuclear safety, it is difficult to think of a more pressing subject for NSF support.

HAVA, the Help America Vote Act of 2002, tasks the National Institute of Standards and Technology with major technical responsibility for guiding the development of voting systems standards, yet this effort remains tragically unfunded. Section 273 of HAVA authorized an appropriation of $20 million for research on voting technology improvements during fiscal 2003. The total actual appropriation was $0 and no authorization even exists for 2004. I have heard it expressed that the Congress wants to give HAVA a chance to work before enacting further voting legislation, but it is elementary that HAVA cannot work if it is never implemented.

As scientists have begun to study voting seriously, a number of revolutionary breakthroughs have occurred that can allow a previously unheard-of degree of transparency in the process of voting and tabulation. Because of a development by computer scientist David Chaum, for example, it is now possible to accord each voter the ability, after voting has taken place, to verify that her vote has not only been counted but counted correctly. It is also feasible for any member of the public independent to verify the correctness of the tabulation and to be sure that no unauthorized votes have been added to the total, all of this without compromising the secrecy of the ballot. Technologies such as these need federal support to flourish.

I thank you for the opportunity to present testimony here today.

Mr. PUTNAM. Our third witness is Mr. Jim Adler. Mr. Adler is the founder and CEO of VoteHere, Inc. He is widely regarded as an authority on the subjects of cryptography, security, and e-voting. He has served on California's groundbreaking 1999 Internet Voting Task Force, testified before legislatures on the subject of e-voting, and is defining certification procedures for e-voting systems. Currently, he is co-chair of the Institute of Electrical and Electronics Engineers Voter Verification Standards Committee which is defining national standards as part of the Help America Vote Act of 2002.

Early in his career, he was a rocket scientist working on Atlas, Titan and Space Station Freedom avionics systems. He received a B.S. in electrical engineering with high honors from the University of Florida—go Gators—an M.S. in electrical engineering from the University of California, San Diego.

Welcome to the subcommittee. You are recognized for 5 minutes.

STATEMENT OF JIM ADLER, FOUNDER AND CEO, VOTEHERE, INC.

Mr. ADLER. Thank you, Mr. Chairman, members of the committee, and visitors.

So far we have heard a bipolar debate between, on the one hand, electronic voting machines are fine as is, and on the other, the only way forward is to go back to paper ballots.

Many people agree that there is a problem with electronic voting today. However, we don't all agree that the paper ballot is the best solution, because we already know paper-based solutions are badly flawed. I am here to tell you there is a third way, perhaps the technology that Dr. Simons is waiting for, a better solution to prove that every vote is counted properly without falling back to paper ballots, the same paper ballots that have been at the root of electrical fraud and disenfranchisement throughout our history.

There are technologies available today, and VoteHere's VHTi is one of them that can make electronic voting better than paper ballots and still retain all of the accessibilities and operational benefits. Just because some have diagnosed electronic voting disease doesn't mean the only cure is going back to paper ballots. There are other more effective cures.

Interesting that Dr. Rubin mentioned safety belts. The call for paper ballots is similar to the call nearly 100 years ago to ban the automobile and go back to horses. Back then the automobile was considered dangerous new technology, lacking critical safety equipment such as safety glass. Instead of moving backward in elections, we need to look forward and, in effect, add safety glass to our electronic voting machines.

Today I will outline technology that brings measurable certainty and transparency from the voting booth to the final election results, solves the current dilemma, and is available now.

My message to you is very simple: We should let innovation and HAVA and NIST work, and not revert back to paper ballots which have historically failed us.

Last summer we announced a nonexclusive agreement with the Sequoia Voting Systems to put our technology in electronic voting machines, and just yesterday we announced another agreement

with Advanced Voting Solutions to put our technology in their machines. So this is not far off into the future. This is happening today. We will be testing that technology in the fall.

VoteHere has a solution called VHTi, a voter-verified election audit technology that works inside any machine, and even though hardware/software procedures may be opaque, the audit system is 100 percent transparent and will with certainty detect if a single ballot is corrupted either maliciously or accidently. The technology goes beyond paper ballots because it proves election results are valid end to end, not just at the polling booth.

It does two basic things: First, it gives voters a voter-verified receipt if they want to check both that their vote was properly recorded at the poll site and properly counted in the final results, while maintaining ballot secrecy throughout. And second, it enables a meaningful and transparent audit trail that lets anyone independently verify the election results with accuracy down to a single vote.

The effectiveness of this technology does not rely on securing software, source code, or the hardware, but instead relies on a transparent audit process that it enables. Elections have always been protected by detecting when elections are compromised, not necessarily just protecting elections from compromise.

Too often, security experts have misunderstood elections as being only secured by protective measures, big fences that you build around your house. Actually elections have, as I said, been always secured by detecting these problems, like guard dogs that alert you to intruders inside your house. It is always good to build big fences, always good to have a dog in the yard. In many ways this VHTi technology is that barking dog.

As a practical matter, tracking our votes is as simple as tracking a package sent through UPS or the U.S. Postal Service or tracking a lottery ticket to its point of purchase, and every day Americans track 12 million packages. If we can track the destiny of our packages, why can't we do so with our votes?

The often-used reason for not using a true receipt that could be used to be taken home is that it could violate a voter's privacy and be used for vote-buying or voter coercion. Well, now this cryptographic technology provides an encrypted voter-verifiable receipt to assure the voter that her vote was counted properly but cannot be used to pass that assurance on to anyone else. The same technology protects trillions of dollars of electronic banking, and it is time that we brought it into our voting process. I realize that the capability sounds unbelievable, but this is the type of long overdue innovation that we are now embarking upon, and in no small part is due to HAVA.

There is a demonstration on the VoteHere Web site, I know we don't have time to go into it, but a couple points need to be made. Just like at the gas pump, the voter has the option to obtain a detailed receipt of each race she wishes to verify. After the election, the receipt data is regenerated from the counted ballots, and she can look up the receipt on the county Web site to verify that the receipt she obtained in the polling place represents the same one that got counted. While the county tallies the votes, the public can also independently tally them as well, and nonpartisan groups such

as the League of Women Voters and others could verify the results independently.

With so much transparency and with so many people monitoring the results, you can statistically guarantee that anomalies will be caught, and in my appendix and written statement I go into that in some detail, and I also presented it at last December's NIST conference on security and transparency.

What is most attractive about this technology is that it acts as a spot check on the election system end to end. Much of the criticisms have focused on the fact that we have no way to trust and justify the trust we place in electronic elections. This voter-verified receipt gives you that spot check and provides us a degree of statistical confidence and guarantees the election results are valid.

I just want to talk about transparency. Cryptology is not a "Trust Me" technology, it is a "Trust No One" technology. In every election, absolutely everything connected with the vote is published for scrutiny. The protocols, the mathematics are published. We did that last September. The source code is published. We did that in April. And all the voting data is published in every election. Cryptography actually reduces the need to trust election officials, hardware, software, procedures, and vendors. And paper ballots just can't do that. Paper ballots let voters check that their vote was recorded, but voters have no idea that their vote was counted. It then drops into a ballot box, a black box, and we have to trust that votes were actually counted.

To just sum up, the promise of electronic voting is that it could be better than paper, not just as good as paper. The calls for security confidence and transparency are necessary. I wholeheartedly embrace them. Let's not go back to horse-and-buggy elections. Instead of banning technology, we should let innovation work and provide safety equipment to our electronic elections. Only then will we have a truly safe voting process. Thank you for your time.

Mr. PUTNAM. Thank you.

[The prepared statement of Mr. Adler follows:]

Testimony to the House Government Reform Committee

Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census

Washington, DC
July 20, 2004

Jim Adler
Founder, VoteHere, Inc.

TECHNOLOGY IS AVAILABLE TODAY FOR SECURE AND VERIFIABLE ELECTRONIC ELECTIONS

Thank you Mr. Chairman and members of the committee for inviting me here today.

Of course, the bad news about Election 2000 was that mainstream America, for the first time, realized that elections were not perfect. In fact, as the CalTech/MIT Voting Technology Project reported, 2 million ballots were lost due to the mechanics of voting – be it, punch card, lever machine, optical scan, or touch-screen. The good news is that we are now focused on innovating election technology to solve these complex issues.

So far we've heard a bipolar security debate between, on the one hand, "electronic voting machines are fine as-is" and, on the other, "the only way forward is to go back to paper ballots." Many people agree there is a problem with electronic voting today. However, we don't all agree that the CPR (contemporaneous paper record, or voter-verified paper ballot) is the best solution because we already know paper ballot-based systems are badly flawed. I am here to tell you that there is a third way – a better solution to prove that every vote is counted properly without falling back to paper ballots – the same paper ballots that have been at the root of electoral fraud and disenfranchisement throughout our history.

There are technologies available today (VoteHere's VHTi is one of them) that can make electronic voting better than paper ballots and still retain all the accessibility and operational benefits of electronic voting machines. Just because some people have diagnosed the electronic voting machine disease doesn't mean that the only cure is going back to paper ballots. There are other cures.

The call for paper ballots is similar to the call nearly 100 years ago to ban the automobile and go back to horses. Back then, the automobile was considered dangerous new technology lacking critical safety equipment such as safety glass. Instead of moving backward in elections, we need to look forward and in effect add "safety glass" to our electronic voting machines.

Today I'll outline technology that brings measurable certainty and transparency to every election – from the voting booth to the final election results, solves the current dilemma, and is available now (others are also available in the market today). My message to you

Copyright © 2004 VoteHere, Inc. All Rights Reserved.

is very simple: we should let innovation (and HAVA and NIST) work and not revert back to paper ballots, which have historically failed us.

ABOUT VOTEHERE

To provide context for my remarks, let me tell you a little bit about me, and the company I founded in 1996. VoteHere was born as a data-security company developing cryptographic software for encryption and digital signatures. We focused our expertise exclusively on electronic voting starting in 1998. In 1999, I served on the California Internet Voting Task Force. Currently, I co-chair the IEEE Special Task Group on Voter-Verifiability (P1583, STG3), where we have discussed e-voting security at great length. Before founding VoteHere, I worked on mission critical avionics systems for space launch vehicles. I've learned that this early training in mission-critical systems prepared me well for the more terrestrial mission-critical world of elections.

Over the last five years, VoteHere's Chief Scientist, C. Andrew Neff, has developed cryptographic protocols for conducting secure electronic elections that retain the secret ballot. Dr. Neff's work has been profiled at industry conferences and by the *Society for Industrial and Applied Mathematics*. Currently, MIT Professor Ron Rivest is teaching cryptography coursework using Dr. Neff's protocols for secure electronic voting. As many of you know, Professor Rivest is a cryptography pioneer, Turing Award winner, member of the CalTech/MIT Voting Technology Project, and has recently been appointed to the EAC Board of Advisors.

VoteHere is fundamentally a software company. We don't make electronic voting machines. We make software that goes inside electronic voting machines. Our technology proves, in every election, that electronic voting machines (and backend tabulation databases) aren't cheating or making mistakes, and provides for a meaningful audit.

At VoteHere, we understand mission critical applications, are world-class leaders in cryptography, and have advanced the state of the art in electronic voting. In many crucial ways, VoteHere represents the emerging face of innovative election technology.

Yesterday, we announced a non-exclusive alliance with Advanced Voting Solutions (AVS), a cutting-edge manufacturer of electronic voting machines. We plan to test our technology inside AVS's voting machines in the upcoming Fall elections. We are also in discussion with all of the other voting machine manufacturers and election officials who have expressed strong interest in deploying our technology.

IN EVERY ELECTION, VHTI PROVES THE TRUST PLACED IN ELECTRONIC VOTING

VoteHere has a solution called VHTi, a voter verified election audit technology that works inside any electronic voting machine. VHTi is an audit system that sits inside the electronic voting machine. Even though software, hardware, and procedures may be opaque, the audit system is 100% transparent and will, with certainty, detect if a single ballot is corrupted, either maliciously or accidentally.

VHTi goes beyond VVPB because it proves election results are valid end-to-end, not just at the polling booth. VHTi does two basic things. First, VHTi gives voters a voter verified

Copyright © 2004 VoteHere, Inc. All Rights Reserved.

receipt to check both that their vote was properly recorded at the poll site and properly counted in the final results while maintaining ballot secrecy throughout (see attached). Second, VHTi enables a meaningful and transparent audit trail that lets anyone independently verify the election results with accuracy down to a single vote.

VHTi and similar technologies on the market today go beyond paper ballots by allowing voters to verify, not just that their vote was recorded (as paper ballots claim to do) but, that their vote actually got counted (which paper ballots absolutely cannot do) – even when faced with hackers, malicious software, procedural missteps, and software bugs that may compromise their ballot along the way – all without reintroducing the known weaknesses of paper ballots or violating ballot secrecy.

The effectiveness of our technology does not rely on securing software source-code or hardware, but instead on the transparent audit process it enables. It does not protect elections from compromise but detects when elections are compromised – whether by hackers, corrupt insiders, or software bugs. Too often security experts have misunderstood elections as only being secured by *protective* measures, like big fences you might build around your house. Elections have always been secured by *detecting* election problems when they occur, like guard dogs who alert you to intruders or problems inside your house.

Yes, it is always good to build big fences, but it is just as critical to have a guard dog that barks when intrusions inevitably occur. By providing voters the ability to verify that their vote was counted and providing third parties the ability to verify election results, VHTi is that guard dog.

As a practical matter, tracking our votes is really as simple as tracking a package sent by the U.S. Postal Service or tracking a lottery ticket to its point of purchase. Everyday, using simple tracking codes, Americans verify the delivery of 12 million packages. If we can know the destiny of our packages, why can't we know the destiny of our votes? Well now we can.

The oft-used reason for not using a true receipt that could be taken home is that it could violate a voter's privacy and be used for vote buying or voter coercion. VHTi provides an encrypted receipt to assure the voter that her vote was counted properly but cannot be used to pass that assurance on to anyone else. I realize that this capability may sound unbelievable, but this is the type of long overdue innovation that we're now embarking upon – in no small part due to HAVA.

The Help America Vote Act (Title III, Subtitle A, Section 301.a.2.B.i) already requires voting systems to print paper ballots for a recount, typically after the polls close. This has been criticized on the grounds that it makes little sense to print the ballots *after* the election if the voting machine is not trusted to record them correctly in the first place. VHTi provides a means to prove the trust placed in voting machines, through its voter-verified receipt, so that printing of voted ballots after the election can be trusted.

How VHTi works

Briefly, here's how it works (this demonstration is also available at http://www.votehere.com/downloads.html):

Copyright © 2004 VoteHere, Inc. All Rights Reserved.

VOTEHERE

Just like at the gas pump, the voter has the *option* to obtain a detailed receipt of each race she wishes to verify. A random tracking code is built by the machine and by the voter for the voter's chosen candidate. This tracking code and its connection to the vote choice is shown to the voter in the privacy of the voting booth, but the receipt shows all of the candidates in order to mask the voter's choice. In this way, the receipt cannot be used to *prove* how she voted outside of the polling place. After the election, the receipt data is regenerated from the counted ballots and she can look up her receipt on the county website (or county office or election hotline) to verify that the receipt that she obtained in the polling place is the same that got counted.

While the county tallies the votes, the public can tally them independently as well. Nonpartisan watchdog groups (such as the League of Women Voters) could also verify the results independently to ensure that no votes were lost or changed. Since all of the ballots are published into an entire election transcript, voters can do their part to verify their own vote and then anyone can verify the backend ballot box to verify that the count is right. In this way, voters have confidence that their own vote is in the final results because those results have been independently verified as a whole.

With so much transparency and with so many people monitoring the results, you can statistically guarantee that anomalies will be caught.

What's most attractive about this type of voter-verified receipt is that it acts as a "spot-check" on the election system. Much of the criticisms have focused on the fact that we have no way to justify the trust we place in electronic elections. The encrypted voter-verified receipt allows voters to spot-check the election system with a degree of statistical confidence that guarantees the election results are valid.

In Appendix A, I provide a standard that defines a measurable "margin of error" on the election results that applies even when faced with accidental and malicious errors in hardware, software, and procedure. This standard has been submitted to California's Secretary of State, Kevin Shelley; to the IEEE Voting Equipment standard; and to the EAC. Any election system, whether paper or electronic, should be held to this standard.

TRANSPARENCY IS CRUCIAL FOR ELECTION CONFIDENCE

Finally, I'd like to talk about transparency.

Elections have always been safeguarded by transparent third party audit. Voters generally do not understand how a lever machine works, or how a punch card system works, or how a ballot is optically scanned. However, they trust that authorities, party observers, and watchdog groups will scrutinize both the mechanism and the process of our elections. The transparency that enables the scrutiny is what's important to voter confidence.

To that end, and since VoteHere's founding, we have recognized the importance of this openness. And, being good students of cryptography, we understand that there is no security in obscurity. After all, if I hide my money by burying it in my backyard, I may think it's safe, but most would agree that it is not really secure. VoteHere began a full-disclosure process in 1999 by filing (and as a result, publishing) the underlying VHTi

Copyright © 2004 VoteHere, Inc. All Rights Reserved.

technology patents. In September 2003, we publicly released detailed technical documentation. And earlier this month, we released the full source-code that implements the VHTi technology for public and scientific scrutiny, along with a sample implementation.

The use of cryptography is NOT just another "trust me" technology. In fact, exactly the opposite – it is a "trust no one" technology. In every election, absolutely everything connected with how every vote is handled end-to-end is published absolutely for scrutiny. Let me be clear: the software code is published, the cryptographic protocols are published, and all the election data is published. It's all laid out in the open. This lets ANYONE independently verify the results of the whole election. And every voter can verify that their vote was counted properly in the final results. Cryptography REDUCES the need to trust election officials, hardware, software, procedures, and vendors.

Paper ballots cannot do that. Paper ballots let voters check that their vote was recorded at the poll-site (if they check them at, which I'll discuss in a moment), but then it drops into a "black box" for the rest of the process. With paper ballots, we are forced to trust that our votes are handled properly beyond the poll-site.

Because, with paper ballots, the paper is the official source document, it is expected that only a very small percentage will check the paper under glass with the on-screen ballot. In a contested election, the paper ballot box will be impugned because the vast majority of voters are not looking at these supposed "source documents." However, if the voting machine produces a receipt, everyone need not ask for one. A small sample will detect problems. If they're ballots, every voter must scrutinize them, and carefully. We presented a statistical analysis on this issue at last December's NIST conference (see http://votehere.com/2003_12_01_jimadler_archive.html#107801943567893232).

CONCLUSION

The real fundamental axioms in this debate are:

(1) Voter-verification that allows a voter to ensure their individual vote is counted properly;

(2) Public verification of election results as a whole; and

(3) Transparency into the election process so that (1) and (2) occur in each election.

These fundamental axioms prove that the election technology and procedures didn't cheat or make mistakes, and election results can be meaningfully audited. With technology such as VHTi, we can prove these axioms in every election.

This is the promise of electronic voting – not just that electronic voting can be as good as paper, but that electronic voting can be better than paper. Frankly, the calls for better security, confidence, and transparency are necessary and we wholeheartedly embrace them.

But let's not be distracted by the call for paper ballots and be tempted to bring back the "horse and buggy". Instead of banning technology in elections, we should let innovation

Copyright © 2004 VoteHere, Inc. All Rights Reserved.

work and add "safety equipment" to our electronic voting machines. Only then will we have truly safe elections.

Elections have never been perfect but we should encourage the "pursuit of perfection." Today, I've discussed standards and technology to guide and measure how well we are doing. HAVA has empowered the EAC and NIST to do set those standards and perform those measurements. To resolve our current election dilemma, I urge you to keep the door open to innovation that will allow us to pursue perfection for the benefit all voters.

Thank you for your attention and I'd be happy to answer any questions.

Copyright © 2004 VoteHere, Inc. All Rights Reserved.

VOTEHERE

APPENDIX A: RECOMMENDED STANDARD FOR MEASURABLE ELECTION CONFIDENCE

As co-chair of the IEEE Special Task Group on Voter-Verification (P1583, STG3), we have discussed voter-verification at great length. Although a contemporaneous paper replica (CPR, the so-called VVPAT or VVPB) may be configured to produce a measurable level of confidence in election results, your currently drafted standards have no such specification.

I would ask that you consider standard language that defines a measurable "margin of error" on the election results that applies even when faced with accidental and malicious errors in hardware, software, and procedure. Any election system, whether paper or electronic, should be held to this standard.

This approach was discussed at December's *NIST Symposium on Trust and Confidence in Election Systems*.[1] Furthermore, David Jefferson, a member of the California Touch Screen Task Force and current member of the California Voting Systems and Procedures Panel (VSPP), recommended this analysis as "a quantitative analysis of the effectiveness of voter verification and random precinct recounts in discovering errors or fraud."[2]

Here is proposed language for such a verification system as proposed to IEEE P1583, STG3:

1. The verification system must produce a measurable level of confidence in the election results, without violating any privacy requirement. From voter intent to election result, the Margin Of Error shall be 1% (or less) with 99% (or higher) level of confidence for all federal and statewide races.
2. The Margin Of Error shall be demonstrably proven for each election, even in the presence of accidental errors and malicious fraud, including those in hardware, software, and human procedure.
3. Any verification capability shall preserve voter privacy, so that it is not possible to ascertain that any vote within a precinct is more likely than any other to have been cast by a particular voter. Specifically, this means that one has to obscure, for each ballot:
    - What time the ballot was cast;
    - On what machine the ballot was cast;
    - In what language the ballot was cast;
    - Whether the ballot was cast through a disability interface;
    - Whether the ballot was provisional;
    - Whether the ballot was an absentee or vote-by-mail ballot;
    - Or any other property that helps identify what voter might have cast the ballot.

WE NEED MEASURABLE CERTAINTY TO BRING CONFIDENCE TO ELECTIONS

A logical question would be, "how many voters must verify to safeguard the election?" Well, before I get to that question, let me digress for moment.

Before Election 2000, many believed that elections were perfect. This idyllic belief was shattered in many respects and we, as an industry and society, have struggled with that reality. Without defining and quantifying confidence, we are in an uncomfortable place where we are tempted to manage perceptions rather than scientifically provable realities.

Let me give you a stark example of the danger in letting perception and fear tactics override scientific proof. In the mid 17th Century, the Black Plague struck Edinburgh, Scotland and thousands were dying from the disease. The city council was politically pressured to act. So, at one of the town meetings, with no science to support the decision, the council concluded that cats were responsible for the spread of the plague, and so ordered them all slaughtered. This was bad policy considering that cats made excellent rat catchers, and rats carried the fleas that carried the plague bacteria. As you've already guessed, by killing the cats, the city council caused the rat population to skyrocket along with the plague. The punch line, of course, is that you'd better have a firm grasp on the science that drives an intended outcome.

I don't mean to compare elections to the Black Death, but without applying clear science, we are being tempted into similarly bad policy.

For example, consider California Election Code 15360, which requires at least 1% of the precincts to be randomly chosen for hand recount. This statute is often given as a justification for CPR, but statistically it turns out that 60%, or 150,000 votes (in a typical Congressional district election of 250,000 votes) could be changed without detection by the 1% hand recount. This is just an application of the basic statistics that governs the "margin of error" in political polls.

---

[1] http://realex.nist.gov/CONFERENCES/Voting/DayOne/session2.5/adler.pdf

[2] http://lists.hss.caltech.edu/pipermail/votingtech/2003-December/000507.html

Copyright © 2004 VoteHere, Inc. All Rights Reserved.

VOTEHERE

However, by allowing voters to verify that their votes were counted, a high level of confidence can be achieved with relatively few voters participating – like 2,000 out of 500,000. This is the punch line, so let me say it again: *if 2,000 voters faithfully verify their vote, the margin of error drops from 60% to less than 0.50%* – and the more voters that verify, the lower the margin of error.

This voter verification coupled with third party audit, proves that the entire election is *quantifiably* worthy of the trust we place in it – from voter intent to tabulated result. Malicious software, bugs, or errant procedures cannot touch the ballots without detection – that is, without the dog barking.

Copyright © 2004 VoteHere, Inc. All Rights Reserved.

VOTEHERE

APPENDIX B: COMMENTS ON THE CONTEMPORANEOUS PAPER RECORD (CPR)

We should have learned by now that elections are deceptively difficult to fully grasp. We don't know that the CPR (the contemporaneous paper replica, also known as the voter-verified paper ballot) "paper pill" will cure the ills of electronic voting machines. Would we mandate a new untested drug that prevents cancer and require everyone to take it? Of course not. Well this "paper pill" is not yet specified; it has not been tested in the lab; and has not been tested in trials. Yet why are we considering requiring it?

Consider this scenario: My 64 year-old mother has been using touchscreen voting machines in Florida for the last few years. With the call for CPR, I explained how they would work with her current voting machine:

> She checks, before the ballot is cast, that what is printed on the paper matches what is on the touchscreen, which is what she intended to vote. The current prototypes would not let her touch the paper ballot but would only allow her to view it through a glass pane for comparison with the on-screen electronic version. Once she is satisfied that the paper ballot is identical to the on-screen electronic version, she touches the button to cast her ballot.

She then asked an interesting question: "Would my vote still count if I didn't compare the on-screen ballot to the [CPR] paper ballot?" I reassured her that, of course, her vote would still count. She then commented that it was unlikely that she would look over at the paper ballot since her attention was focused on the screen.

Fast forward to a contested election where the "paper ballot box" differs from the "electronic ballot box." There are many ways for this to happen including procedural and machine fault. The losing candidate of the "paper ballot box" brings voters, like my mother, into court that testify that they never looked at the paper ballot. This casts more suspicion on the election.

The moral is that CPR may provide a good way to detect problems with electronic voting machines, but it doesn't necessarily provide a reliable mechanism for recount.

Given millions of ballots, it is inevitable that the CPR count will disagree with the machine count in a close election. In that case, we won't know which ballot box to use. It's like having two wristwatches – when the watches disagree, what time is it? A root cause of problems during Election 2000 was ambiguity in what constitutes a vote – that is, whether punch card chads were pimpled, dimpled, pregnant, or hanging. Additional ballot boxes may seem like a good thing but a likely unintended consequence would be an ambiguous election result.

I understand the election-year intensity surrounding this issue, but before we use the blunt instrument of legislation to impact elections for a generation, shouldn't we make sure the CPR " paper pill" isn't a placebo and is actually safe and effective?

We shouldn't restrict ourselves to paper as the only way to achieve confidence and proof in our elections. There are better ways than taking the "paper pill."

Copyright © 2004 VoteHere, Inc. All Rights Reserved.

Mr. PUTNAM. Our next witness is Mr. Sanford Morganstein. Mr. Morganstein is the president and founder of Populex Corp. He has more than 35 years of technology-based experience in both entrepreneurial and Fortune 500 companies. For the past 20 years, he has led several new high-technology corporations, including developing Dytel into a successful corporation. He has served as chief of Technology and Competitiveness for the Illinois Department of Commerce and Community Affairs. In this capacity, he was responsible for strategic planning in new initiatives in biotechnology, telecommunications, business modernization, and commercialization of advanced university research. He also served as a member of several Governors' task forces. He holds 29 United States and foreign patents for telecommunications and high-tech products. Welcome to the subcommittee. You are recognized for 5 minutes.

STATEMENT OF SANFORD J. MORGANSTEIN, PRESIDENT AND FOUNDER, POPULEX CORP.

Mr. MORGANSTEIN. Thank you, Mr. Chairman, Congressman Clay, invited Members of Congress.

What a great spirit of bipartisanship and democracy when the ranking member quotes Ronald Reagan in saying "Trust but verify." It was President Reagan who said that so many years ago.

I am here with one goal only, and that is to dispel misinformation that somehow voter verifiability and verifiable ballots are impractical, costly, and disenfranchise the blind. As Professor Rubin said, there is no reason at all that providing voters with a voter-verifiable, tangible ballot, one of which I am holding in my hand—and we will talk a little bit about that further—can't be used on touch-screen systems so that blind voters can work, undervotes are detected and warned, overvotes are not permitted, people who speak different languages can have their ballot easily translated into the language of their choice. There is absolutely no incompatibility with those noteworthy goals and the notion of having a voter-verifiable ballot.

Mr. Chairman, some who have said that there is an incompatibility have pointed to reams of cash register tape saying, if you want an audit trail, this is what you have to have. It is crinkled, it is folded, it tears. Who knows how you count such a thing? I think that is a piece of misinformation that insists that something that is voter-verifiable has to be of this nature.

And Mr. Adler to my right said let us not go back to paper. But it is not either/or. We can combine the best of the new, which is touch-screen voting, for its obvious advantages with the best of the old; something that can be verified, something that voters understand, something that they see, that is tangible, that goes in a ballot box, that is counted at the end of the day, as the Congresswoman asked, and that can be recounted. If you count this ballot, you will get the same result as when you recounted.

Let us look at whether or not it disenfranchises the blind voter. We have had two of our machines in use for several months at the National Federation of the Blind in Baltimore, and they are going to be issuing a report based on human interface—this is easy to use, hard to use. And they have looked at five or six machines. And I don't know what they will say about that, but I do know—and

I have questioned them and asked, can I quote you on that—that the blind voters who have taken the opportunity to verify their ballots—and they can by holding it underneath a supermarket scanner that we are all kind of used to and putting on headphones, it will read what is on that ballot. Those blind voters appreciated and understood that their ballots were being verified and that they were not being discriminated against because there was a technology that did not apply to them.

When the subcommittee issued its notice, it focused on technology and science. And there is a human component that I urge consideration. Mr. Chairman, I would be preaching to the choir if I said that, fundamentally, our system is one that is ruled by the consent of the governed. And what is missing in a lot of the debate is the confidence of the voter; not of the scientist, but the confidence of the voter. And if the voter erosion—and if the voter's confidence in an electoral system is eroded because they don't understand what happens to the ones and the zeros on the disk, or they know that they had a hard drive that crashed, and they read about viruses, then we have a real risk that the people who really make this country, the voters, will lose confidence. And, again, there is absolutely no reason that confidence is incompatible with the electronic systems that can ensure that we capture the vote and capture the voters' intent.

[The prepared statement of Mr. Morganstein follows:]

UNITED STATES CONGRESS
Committee on Government Reform
Subcommittee on Technology, Information Policy, Intergovernmental Relations and the Census

Testimony of Sanford J. Morganstein
President and Founder, Populex Corporation
July 20, 2004

Mr. Chairman, Congressman Clay, Members of the Committee:

My name is Sanford Morganstein. I am the president and founder of Populex Corporation: a company specifically founded to provide new solutions for secure, accurate and confidence-building elections for the nation.

If I have one goal, it is to dispel myths and inaccurate information that may lead American citizens to think they cannot have elections they can trust. At the same time, I would like to emphasize that to accomplish this goal, implementation of new voting systems and enhancements to existing systems must be effective and timely, but not rushed. They also must have bipartisan support.

After the upcoming election, greater attention should be given to the adoption of new, and better voting systems. This will help ensure smooth implementation of new solutions, which is a huge task for any election jurisdiction, requiring careful thought, care, widespread public education and acceptance by the electorate

Voting systems can be produced that use modern touch screens to prohibit overvotes, warn voters of potential undervotes, allow blind voters to vote in private and support multiple languages. Importantly, we have developed a system that has all of these features and more, while still providing voters with an official voter verifiable paper ballot.

In short, voting systems that combine the best of the new (computer assisted touch screen voting) and the best of the old (confidence-building paper ballots) are practical, trustworthy and affordable.

Unfortunately, the myths that persist, and which I hope to dispel, promote the idea that voter verifiable ballots are uncountable, impractical and disenfranchise Americans with disabilities. Please allow me to briefly take each of these one at a time.

Probably all of us have seen the specter of rolls and rolls of cash register paper tape, curled, creased and illegible as if that were the only way to provide a paper audit trail. What I have here are a few paper ballots produced by a modern touch screen computer system on which voters make their selections. These *are* the ballots. There are no vote totals kept in the machine that produced the ballots. Consequently, the perception that the computer count may be different from the audit trail is simply not true. These ballots produce the same result when counted and recounted. They are tangible, they are handled by the voter who has several methods available for verifying them, and they are

deposited in a locked ballot box. This process preserves what is "tried and true" and highly familiar to each and every voter. These ballots are not receipts, which, if taken out of the polling place, could lead to coercion and vote selling. They are the official ballots cast by the voters and left in the ballot box.

These systems are no more expensive than the touch screen systems found to be unacceptable by many voters and so many academicians and computer experts. These machines, designed to overcome the voting problems of the past, are not networked in the polling place: if one machine fails, or indeed if the printer jams, only one machine is momentarily taken out of service. In the unusual event of a paper jam, one voter is perhaps inconvenienced for a minute or two, but even in that case, that voter's vote is not lost.

This system does not disenfranchise blind voters. In fact, the opposite is true. The National Federation of the Blind has been experimenting with two of these systems for several months. While I understand that they will not be recommending any system over any other, and that they will be issuing a report, they have told me that blind voters have opined that they appreciate that *they too* can have a tangible ballot that when scanned reads its contents to them in private over headphones, without assistance.

Other advantages of this voter verifiable paper ballot are numerous: This ballot facilitates handling of provisional ballots, it is not destroyed or lost in the event of a computer crash, it facilitates reconciling the number of cast ballots with the number of voters who vote in the polling place, and the voting process, with selections made on a touch screen with a stylus, involves motions and procedures that are very familiar to voters. More abstractly, I had one professor of political science tell me that because the voter takes ownership of the ballot from the time that voter begins to vote until he or she deposits it in the ballot box, the connection between the voter and his or her democratic duty is strengthened in a salutary manner.

Just last week, I had the honor of working with a committee convened at the National Academy of Sciences here in Washington. In my opinion, the evidence presented to that committee was clear that the kind of voting systems used can significantly reduce voter error as measured by overvotes and undervotes. Precinct count systems are an improvement over non-precinct count systems, and properly designed touch screens can be better yet. This particular system is very close to being certified under the new, more stringent 2002 federal voting system standards. It is not a prototype, and it is affordable. The paper audit trail is practical, and it does not disenfranchise Americans with disabilities. Yes, we can have modern touch screen systems that produce a confidence instilling, voter verifiable, paper ballot that can be counted and recounted, if necessary, with unparalleled accuracy.

Thank you for the opportunity to testify. I would be happy to address any questions you may have.

Mr. PUTNAM. Thank you very much.

Let me begin with a question for you, sir. How many ballot questions will fit on the card that you held up?

Mr. MORGANSTEIN. Well, I have a lot of jokes about the city of Chicago, and I come from that city. And when I tell those jokes to people who are election officials there, I get into trouble. The typical Chicago ballot will have 75 judicial retention questions whereby judges are up, and you probably aware of that, sir. We have programmed an election for the city of Chicago—we programmed the 2000 election in which there were some, I think, 96 ballot questions, counting 75 judicial retention, President, Vice President, and so on. And that is, as a matter of fact, the limit that we can put on here. We can put 96. You can have thousands of people on the ballot, thousands of questions, but 96 selections, which is more than adequate for any election we have seen.

Mr. PUTNAM. So that being the ballot, the voter can read their 96 selections on that piece of paper?

Mr. MORGANSTEIN. Yes, sir. There are two ways the voter can do that. It is printed in a human readable format. You can see some numbers—and I am happy to pass these up to the committee if you would like to touch these.

Mr. PUTNAM. That would be helpful.

Mr. MORGANSTEIN. There is a human readable portion on the bottom, and then you see a bar code in there, which as the last time you went to the supermarket to buy a can of soup, you know that it read the price properly. The voter can hold that underneath a laser beam, and in the privacy of a voting booth it will show the selections, English selection, President of the United States and so on that they have picked up to 96.

Mr. PUTNAM. Dr. Shamos, considering the pool of people able to hack into electronic voting systems is presumably smaller than those who are able to do it the old-fashioned way by manipulating the paper system, would you agree or disagree that electronic systems increase security of the ballot?

Mr. SHAMOS. Properly designed and properly deployed and tested systems, DRE systems, do indeed increase the security of the ballot.

Mr. PUTNAM. Dr. Rubin, after volunteering as a poll worker, you were quoted as saying that the experience showed you that one potential attack would be far more difficult to pull off than you and your colleagues had assumed. Is that an accurate quote, and do you still feel that a serious attack is likely?

Mr. RUBIN. Yeah. It's not a misquote, but it's the first half of a sentence where the second half was, "I have found some attacks that I considered would have been harder to pull off in my precinct. I thought of new ones that I hadn't considered. And basically I think the experience focused me better on appreciating what the real risks were," and at the end of that paragraph, I stated that I still believe that these were a fundamental risk to our elections.

So I did not believe the system was any less secure after working there. I just sharpened my appreciation for the various attacks.

Mr. PUTNAM. Is it more or less difficult to perpetrate fraud using electronic devices over traditional paper ballots?

Mr. RUBIN. I believe it is probably more difficult to perpetrate fraud, but that the fraud would have much more far-reaching consequences if it were successful.

Mr. PUTNAM. And for the short term, this whole idea of a paper trail, is it technologically feasible to deploy an auditable, verifiable paper trail in every machine in America between now and November?

Mr. RUBIN. I don't know.

Mr. PUTNAM. Anyone else?

Mr. SHAMOS. It is not possible.

Mr. PUTNAM. Mr. Adler.

Mr. ADLER. It is not possible.

Mr. MORGANSTEIN. I would be wealthy if it were true, but it is not possible.

Mr. PUTNAM. So we are all in agreement, with the exception of Dr. Rubin, that this is really a discussion about improving or changing or altering the approach for the 2006 election, because 2004 is out.

Mr. MORGANSTEIN. There are primaries in 2005, and there are municipal elections in 2005.

Mr. PUTNAM. OK.

Mr. RUBIN. I will agree with that statement, too.

Mr. PUTNAM. OK. So this is all then, about post-Presidential election and the challenges that we are going to have to deal with. We have heard testimony that no system is perfect, they all have their problems, they all have their security issues. We all deal with a certain amount of error every day in on-line IRS filings, ATM machines, self-serve gas pumps that scan our credit cards, and we all deal with a margin of error in electronic devices involving our finances. And obviously voting is a fundamental piece of our democracy, and we ought to do everything we can to secure it as well.

But my concern is that this election is going to be seen as being a fiasco despite the fact that there may or may not be any greater error rate than historically has been the case because of the sensitivity, the international scrutiny, and the fact that now, frankly, both parties are ramping up teams of attorneys to figure out ways to exploit what everyone admits is an imperfect system.

So knowing that everyone, the first panel and I believe all of you are in agreement—and if you are not, please say so. Knowing that everyone agrees that there is a margin of error in every single system deployed, how do we develop some standard that defines an acceptable error rate, knowing that this thing is going to be litigated and played out both in the media and presumably in the courts again? How do we have some standard if everybody agrees that there is going to be something that someone can point to and say that is an imperfect system? Because we haven't designed a perfect one. What is the definition?

Mr. Morganstein, and we will work across the table.

Mr. MORGANSTEIN. Thank you, Mr. Chairman. I will be brief. I was very honored last week to participate in a panel at the National Academy of Sciences right here in Washington with some of the smartest people I have ever seen or had the pleasure to sit down next to. And evidence was presented, sir, that showed that the voting system unquestionably counts. It makes a difference. It

lowers error rates. Unquestionably. If you start from hand-marked ballots, which sound simple—make an X; well, some people make a circle and other things happen—to punchcards, which were good for a long time, and then we saw, well, maybe not so good; to optical scan that provide feedback to voters in the precinct. Better yet. And you can see that when we did these, the questions on the ballot didn't get easier, but the technology got better and the error rates did increase.

I think DREs are a step further yet, and a I think a voter-verifiable touch screen—which is not really a DRE, by the way—is yet another step.

The answer, sir, to your question is, like anything else that we have done in this country, we have recognized the importance of continual improvement. It is not like the Constitution says, a more perfect union; you know, it is something perfect, you can't make it more perfect. We are getting better and better, and that is the best we can do as humans, is make it better and better and work on continuing improvement.

Mr. PUTNAM. Mr. Adler.

Mr. ADLER. As Dr. Shamos said, there is no election science, and we—the election community—are making it up as we go. And that is just a true statement. On the committee that I co-chair at IEEE on voter verifiability, we have put out margin-of-error levels, standards that every system should meet, whether it be paper DREs or receipt-based systems where you can spot check these things.

Statistics govern our whole lives. How do you know that a vaccine works? Because you didn't get sick? If you didn't take it, you might not have sick either. We do statistical analyses in this society that we base policy upon. What we are not doing with voting is we are not measuring the margin of error. The first thing we have to do is measure it and figure out how to measure it across systems, whether it be DREs, whether it be paper ballots. And I think once we understand that—and we have done some analysis which says if 2,000 people faithfully spot check and verify their vote, actually counted properly in a congressional district of, say, 400,000 voters, you can get a margin of error that you can take to court that is about a quarter of a percent. If you want better than that, you need more spot checking.

And that is exactly what we did with lever machines; we used to spot check them. There was no paper to recount. We had a meaningful audit trail. And there are performance requirements that we need to institute and measure for every system on Election Day that will provide the second component, which we have all talked about, which is voter confidence. I get a receipt at the gas pump if I want it. If I get a receipt at the voting machine—in our focus groups, and we put about 70 people, you know, through our last incarnation, whether they were going to check or not, they said I would rather have it than not have it.

Between those two, measuring and giving the voters some confidence their vote counted and some proof their vote counted, I believe, is a way forward.

Mr. PUTNAM. That technology test that would give you that .25 margin of error, isn't it true that would not take into consideration a confusing ballot design that, frankly, in Florida was one of the

key reasons for voter confusion? But technically the machine worked. They were overvotes as a result of voter confusion on a complicated design. So, I mean, that is the whole other human piece; right?

Mr. ADLER. Well, I would agree that the most difficult place is between the voter's gray matter and how they represent it. And we have done a lot—the best things DREs do is stop overvotes. Overvotes have gone to zero. And so we will continue to deal with that gap, from gray matter to medium.

The question that I think we are all dealing with, and actually NIST put out a report on usability, is once the voter intent is captured, how do you make sure it is counted accurately or properly, faithfully? And then the chain of custody all the way to rolling up the result. You have to do it from gray matter all the way to results, and that is the end-to-end solution or end-to-end system that we need to measure.

Mr. PUTNAM. I will let the other two finish, and then go over to Mr. Clay.

Mr. SHAMOS. I have to make the question more complex before actually giving an answer. We have no definition of what error is in voting. Political scientists think it is an error when a voter goes into a voting booth and comes out without having voted for every race and question on the ballot. They actually use the word "error" in reference to that. Error can occur because of a difficulty in a voter expressing her choices. That is, they have in mind a certain slate they want to vote for, and it ends up, through error or mistake in the voting booth, they don't actually end up voting for those people.

Then, of course, there is the issue of error in the software, error in the hardware, that may cause the vote to be recorded differently from the correctly expressed intention of the voter. But even if that could ever be reduced to zero, which it can't, that still doesn't mean that we have error-free voting, because the votes must be totaled, the totals must be communicated through a central place. We must make sure that every voting machine that was used, that its totals are correctly reported and added together. And so there are many parts in the process which have the potential for introducing error.

The issue with paper, paper receipts and paper trails, is exactly which of those errors they address. And they do address one error very well; and that is, the error in the voter communicating her choices to the machine. When the verified piece of paper or whatever mechanism is used—and there are numerous ways of verifying ballots without using paper. Whatever the mechanism is used, it does provide an instantaneous feedback that, yes, the machine heard me correctly. Unfortunately, because of the inability to secure the physical custody of ballots—these, after all, are potentially touched by 1.4 million poll workers around the United States on their way to the central counting station. Despite the fact that the voter was heard properly, it doesn't mean that piece of paper is ever going to be around for a recount, that it will not have been augmented, destroyed, modified, or changed in some other way. That is the fundamental problem with relying on paper.

Mr. PUTNAM. Dr. Rubin.

Mr. RUBIN. My area of expertise is computer security. That is what I do for a living. And so I face this question all the time because no system that is on is secure. And in my consulting work I am often asked, we want you to help us design this or evaluate it to make sure it keeps hackers out, and that we are not vulnerable to data loss. And I say it can't be done.

So given that, the goal is to make things better and to make them as secure as possible. You know, I talk about spectrum from really insecure to very, very good. And you try to fall in the best possible spot on there.

I think what we need to do is use all the technologies available, whether the modern and computerized ones or the old paper ones, utilize the best properties of each, and make the system as good as possible and then hope that the election is not too close.

Mr. PUTNAM. Mr. Clay.

Mr. CLAY. Thank you, Mr. Chairman.

Dr. Rubin, the debate about improving the security and reliability of the electronic voting machine has up to this point focused on the use of a voter-verified paper audit trail. While the idea has many supporters, others say that moving toward this sort of paper trail is impractical and may prove unwieldy. In your opinion, are there any better solutions?

Mr. RUBIN. I believe that 20 years from now we will all be voting on systems like Mr. Adler's and David Chaum's, and universal verifiability. I think that cryptographic solutions hold a lot of promise.

I approached this from the point of view that many, many places are using DREs. And I got to see one of those DREs inside, and I believe that systems like that, that are fully electronic, that don't have the cryptographic protections cannot be relied upon without a voter-verifiable paper trail.

Mr. CLAY. Dr. Shamos, you said, "The system that we have for testing and certifying voting equipment in this country is not only broken, but it is virtually nonexistent."

Given that situation, should we have a moratorium on the purchase of new DRE equipment until we have adequate standards and an adequate certification process?

Mr. SHAMOS. I am thinking.

I have never met the question in that form. There are good DREs and there are bad DREs. And the problem is, the public doesn't know which is which, and often Secretaries of State don't know which is which because of failures in the certification process.

As Dr. Rubin pointed out, the systems that we have that are known to have serious security flaws all passed the independent testing authority certification process or qualification process and were actually adopted by a number of States. The issue with moratorium—I mean, I pointed out before that we haven't had a verified incident of tampering with a DRE machine in the United States. That doesn't mean it doesn't occur and it doesn't mean that it won't happen tomorrow. Except that when we are trying to safeguard against risks, we tend to focus our attention and money on those risks that have occurred at least once.

And so the answer is, if we know that certain machines have security flaws, for example, the ability to plug a keyboard—conceal a keyboard on one's person and plug it into a voting machine in

a polling place on Election Day and type things in to modify the contents of the machine, a grotesque security flaw. Nonetheless, there are safeguards that can be introduced to prevent anybody from actually doing that. If it's necessary to put people through a metal detector or watch them as they are going in and out of the booth, then we do that. And so I don't think the moratorium is the right answer, either, because it condemns us to live with the worst systems of the past.

Mr. CLAY. Thank you for your response.

Mr. Adler, can a computer be programmed to show one thing on a screen and record something else on an electronic device?

Mr. ADLER. I think the statement you made earlier about trust and verify applies. Yes, a machine can display one thing and record another. Just like even with the voter-verified paper ballot, it could record one thing electronically, print it on the paper, and hope the voter doesn't see it. And if I could give you one parable about how this might work.

My 64-year-old mother lives still in Florida, Tampa Bay area. She has been using these machines for the last 4 years. Loves them. Said: Mom, they are going to put a paper ballot next to it; you are going to have to compare them; and, if they are right, you press the button. She said, first question: If I don't compare them, will my vote count? And I said, of course it's going to count. She said, then why would I really do it? I am touching the screen.

Now, here comes the recount where the paper ballot and the electronic ballot box do not match. They are going to bring people like my mother into court and say, ma'am, did you look at that paper ballot? She is going to say, no, sir, I didn't think I needed to.

So is it voter verified? Is it a source document prepared by the voter, and can the system do exactly what you said: put one thing on the paper, put one thing electronically, and hope the voter doesn't see it?

Mr. CLAY. Let me ask you, did your company consider producing a voting product on the Internet?

Mr. ADLER. Yes, we did, and we do.

Mr. CLAY. And your company experienced an Internet attack? Do you feel the Internet is a safe place to vote?

Mr. ADLER. I think anyplace you use electronics, you must verify. And, again, it's not really about the hackers. With voting, we don't know where the bad guys are, depending on where you are politically sitting.

Mr. CLAY. OK. My time is up. Let me ask you, why should voters trust a company? This is not malicious in any way to your company, but why should voters trust a company that could not protect their own assets from attack over the Internet when they say they can produce a paperless voting system that is secure?

Mr. ADLER. They shouldn't trust anyone when it comes to voting. That is one of the reasons why we published our source code, we published all our mathematics and algorithms, protocols, we patented all our technology; which means it is published. And every election, all the data that comes out of this machine is verifiable by anyone. You shouldn't trust me, you shouldn't trust the local election official, you shouldn't trust the parties.

As Congressman Holt said, the voter can verify their vote, and we need to give them the means to do that, not just that it was recorded but that it was properly counted, and let anyone verify the results. No one should be trusted in voting. No one. Not the company, not anyone else. And we at VoteHere are dedicated to that. So that if something did happen—the worst catastrophe of a democracy is an undetected fraud. A detectable fraud is embarrassing and expensive, but recoverable. And we need to have the means to detect fraud when it occurs, and we are dedicated to that.

Mr. CLAY. Thank you for your response.

And Mr. Morganstein, why did your company choose to have paper ballots printed by your voting system?

Mr. MORGANSTEIN. We were asked to do that by an election official in our State—if it plays in Peoria, in fact it came from Peoria—by an election official who had been working in the field for some 20 years, who said, you know, I like this touch-screen idea, but there is no audit trail. And I was fortunate enough to have some other successful inventions, and they asked me to put my mind into that and that is what resulted.

Mr. CLAY. Thank you for your response.

Mr. Chairman, I yield back. Thank you.

Mr. PUTNAM. Ms. Kaptur, you are recognized.

Ms. KAPTUR. Again, I just want to thank the chairman, Mr. Putnam, and the ranking member, Mr. Clay, for holding this very important hearing. And so many Members are interested in this, and obviously our citizenry is interested in this issue of security of the vote.

I wanted to ask several questions, and I hope I can get through them quickly. One of the counties I represent, Lucas County, has a situation where they were going to bring on Diebold technology. And the Secretary of State has just said that is uncertified and has taken it off the list. And some of our counties in Ohio of 88 counties had signed contracts with Diebold. They cannot use that equipment now, as of November. The local county, Lucas in particular, is now being faced with a 300, I don't know, 80,000 bill, I guess, to try to bring on some type of optical scanning equipment by November to try to have the ballots in a situation where we can have a recount. Because, under Ohio statute, you have to be within one-half of 1 percent; if you are, a recount is required. And we are told that in the technologies they have been looking at, that was impossible. So they have to do the optical scan.

What advice would you give to the Board of Election? They are in a tizzy now, saying, well, that the Federal money that is available from Washington that I voted for can't be spent to pay for the optical scan for November. And the county is broke. We have 10,000 fewer jobs than we had 3 years ago. The State is broke. But all this money is sitting there from HAVA. Do you have any advice? What would you advise to our local county? Maybe some of you could give them a better price than Diebold is offering on these Optiscan machines.

Mr. SHAMOS. I would advise hiring a lawyer. It is important in procuring voting system equipment to get a representation and continuing warranty from the vendor that their system meets certain standards and will continue to meet those standards. And if

the system becomes decertified, then the financial burden should be placed on the vendor, ultimately its bonding company, to make good to the county so that it can purchase whatever substitute is necessary.

Ms. KAPTUR. Thank you for that suggestion. Believe me, I will pass it on to them. Do you think it is appropriate for private companies to coach and teach board of elections officials and precinct workers? Or should that training of election officials, which Federal money has been designated for, should that be done by publicly hired workers who work for the board of elections, not for any company?

Mr. SHAMOS. Well, maybe the vendors would want to give another answer. But I don't like it. However, it is almost a universally held opinion among election officials that there is no alternative to it, because there is no other source of expertise about the particular systems that are being used, other than the vendor who has seen them used in numerous jurisdictions, has seen all kinds of incidents and knows to deal with them.

Ms. KAPTUR. Well, this is a very troubling aspect to me, that private companies—Mr. Adler, I was very interested in what you said, that your technology patent was open to the public realm. When I made this statement in Ohio, that if we adopt a certain machine, that should fall into the public domain, there were many who opposed that point of view. You've stated exactly what I think should happen in terms of the technologies that are used: Are they public or are they private? Who provides the training? How do we know what is really going? Who are the experts that end up controlling the election process itself? I guess I am especially protective of the citizens' interests, because in our county, in Lucas County, we have always counted at the precinct level.

When I saw, Mr. Chairman, what happened in Florida, I couldn't believe it, where it take votes to another site, you count the votes. That is no anathema to what we do. It was agonizing to watch, actually. And our elections are very decentralized in my home county. And I am not saying there probably aren't errors, but it really is very democratic, gets right down to the precinct level, results have to be posted, they have to be placed on the outside doors. There are all kinds of things that—you have to have two people from each party, plus a judge, looking over each other's shoulders; and the count, it is very, very Jeffersonian. I mean, it is right down to the grassroots level.

So when I hear about what companies are doing in all of this, I am very troubled. And I wanted to ask you, I read some reports about Georgia in the last election, which said that there is this conjecture, 25,000 patches on machines that were employed in Georgia. What is a patch, and was that done or wasn't it done?

Mr. RUBIN. I will answer that first one. When a program is written, it contains lines of code. This is something that a programmer types in to make the computer do whatever they want. That gets compiled into software which is what runs on the machine. From time to time, errors are found in the software or something needs to be updated or fixed. And this generally occurs across all disciplines when software is developed, and you want to upgrade the software and make it new or change some of it. So you write a

patch, which is something that changes certain parts of the software. It adds lines of source code or removes lines. And when you apply a patch, what you are doing is you are creating a new version of the software that is based on the old version but has certain changes. So a patch can completely change the behavior of a software package. It can make it better, it can make it worse.

And I also have read a lot about the patches in Georgia. I don't have any personal firsthand knowledge that anything like that happened. But I would say that it is a very, very serious matter that if a patch gets applied to a voting machine on Election Day or shortly before, that is no longer a certified machine; it's a different machine, and it needs to be recertified.

And so you need to be very careful. And this gets to the point that you mentioned about access between the election officials and the vendors. On Election Day, the vendors should not be tinkering with the machines and applying patches to them.

Ms. KAPTUR. Well, I will tell you, in the home precinct that I am from—and I'm a precinct committeewoman, long before I was a Congresswoman—they sent out an official from the company to deal with a scanner that was malfunctioning in that precinct, because we didn't have election workers that were trained to do that work. And I am thinking, what is going on here?

Mr. Chairman, I want to thank you for holding this hearing. I don't want to go overtime. I have two small questions I still want to ask, if you would be kind enough to——

Mr. PUTNAM. You have time coming.

Ms. KAPTUR. Do I have time coming?

I just wanted to ask you if any of you are familiar with the technology that Mr. Akin Gibbs had. He was one of the few minority contractors that had a technology out there that could have been reviewed by the States—they and localities—as they make selections. Do you know, is that technology still on the market and what its name is? He was in the State of Tennessee.

Mr. MORGANSTEIN. The True Vote?

Ms. KAPTUR. I think that was the name.

Mr. MORGANSTEIN. That is all I know about it. Sorry.

Mr. RUBIN. I had read accounts, I believe this person was killed in a car accident. Is that right?

Ms. KAPTUR. Yes. He was due to come to Ohio to testify before our State legislature the next week, and he died the prior Friday, or that weekend.

Mr. RUBIN. I am not familiar with his technology.

Ms. KAPTUR. You are not familiar with his technology. All right.

A final question. If you are a local election official in any State in this Union right now, and you are interested in getting accurate information about machines' verifiability and so forth, what you are faced with is a barrage of private companies coming to you, telling you that their technology is the best in the world. It may or may not be. Where do you go now for good information? Where do you go to help you in your board of elections? None of you know anything about electronics, nothing about computers. There you sit with this major public responsibility. Where do you go for information? Where would you tell them to go?

Mr. RUBIN. One of the things to keep in mind is that there are some questions that can tip off right away the kind of vendor you are dealing with. So, for example, Chairman DeForest Soaries of the Election Assistance Commission made a statement that election officials should have the right to ask the companies for their source code under nondisclosure to get external security reviews. The first question to ask a potential vendor is if they would be willing to do that, and, if not, why not?

And you could try to produce a list of questions—I have some actually on my Web site—that you might want to ask a vendor, just like you would when you are buying a car. If you start to see that they are acting shady, they don't want to answer certain questions, they won't provide you written documentation of certain things, then you would proceed with caution. I don't know if there is an independent group out there that is providing advice on vendors.

Mr. SHAMOS. There are no consumer reports for voting systems.

Ms. KAPTUR. And if I could just say for the record, Mr. Chairman, I thought when we voted for HAVA, that's what we were voting for. We were voting for the National Institutes of Standards and Technology to be the Fort Knox or the Oak Ridge or the whatever national renewable energy lab for voting, the place where you would go to get information.

Mr. SHAMOS. This should be the province of the Election Assistance Commission. Previously, it was the voluntary province of the Federal Election Commission, to accumulate information about voting systems. But they couldn't get into the position of making specific comments about particular vendors. It just didn't seem appropriate in that context.

Mr. PUTNAM. That would be contrary to Jeffersonian ideals, I believe.

Mr. SHAMOS. So the answer is now many studies are being undertaken by many organizations, and one must keep up with the output of these things to try to determine which are authoritative and which are not.

Ms. KAPTUR. I thank you for your forbearance, Mr. Chairman, Mr. Ranking Member. And we thank the witnesses very much for helping educate our whole country and many election officials who will watch this and are trying to make the best decisions they can at the local level under these circumstances.

Mr. PUTNAM. Thank you, Ms. Kaptur, Mr. Clay. Thank you very much for your input and helping us to get some good expert testimony. I want to thank all of our witnesses.

In the event that there may be additional questions we did not have time for today, the record will be open for 2 weeks for submitted questions and answers. Thank you all very much. This subcommittee stands adjourned.

Whereupon, at 12:34 p.m., the subcommittee was adjourned.]

○