AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

VOTING MACHINES: WILL THE NEW STANDARDS AND GUIDELINES HELP PREVENT FUTURE PROBLEMS?

JOINT HEARING

BEFORE THE

COMMITTEE ON HOUSE ADMINISTRATION HOUSE OF REPRESENTATIVES

AND THE

COMMITTEE ON SCIENCE HOUSE OF REPRESENTATIVES

ONE HUNDRED NINTH CONGRESS

SECOND SESSION

JULY 19, 2006

Serial No. 109–56

Printed for the use of the House Committee on Science and House Committee on House Administration

Available via the World Wide Web: http://www.house.gov/science

U.S. GOVERNMENT PRINTING OFFICE

28–627PS WASHINGTON : 2006

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 SCIENCE

HON. SHERWOOD L. BOEHLERT, New York, *Chairman*

RALPH M. HALL, Texas
LAMAR S. SMITH, Texas
CURT WELDON, Pennsylvania
DANA ROHRABACHER, California
KEN CALVERT, California
ROSCOE G. BARTLETT, Maryland
VERNON J. EHLERS, Michigan
GIL GUTKNECHT, Minnesota
FRANK D. LUCAS, Oklahoma
JUDY BIGGERT, Illinois
WAYNE T. GILCHREST, Maryland
W. TODD AKIN, Missouri
TIMOTHY V. JOHNSON, Illinois
J. RANDY FORBES, Virginia
JO BONNER, Alabama
TOM FEENEY, Florida
RANDY NEUGEBAUER, Texas
BOB INGLIS, South Carolina
DAVE G. REICHERT, Washington
MICHAEL E. SODREL, Indiana
JOHN J.H. "JOE" SCHWARZ, Michigan
MICHAEL T. MCCAUL, Texas
MARIO DIAZ-BALART, Florida

BART GORDON, Tennessee
JERRY F. COSTELLO, Illinois
EDDIE BERNICE JOHNSON, Texas
LYNN C. WOOLSEY, California
DARLENE HOOLEY, Oregon
MARK UDALL, Colorado
DAVID WU, Oregon
MICHAEL M. HONDA, California
BRAD MILLER, North Carolina
LINCOLN DAVIS, Tennessee
DANIEL LIPINSKI, Illinois
SHEILA JACKSON LEE, Texas
BRAD SHERMAN, California
BRIAN BAIRD, Washington
JIM MATHESON, Utah
JIM COSTA, California
AL GREEN, Texas
CHARLIE MELANCON, Louisiana
DENNIS MOORE, Kansas
DORIS MATSUI, California

COMMITTEE ON HOUSE ADMINISTRATION

HON. VERNON J. EHLERS, Michigan, *Chairman*

BOB NEY, Ohio
JOHN MICA, Florida
JOHN T. DOOLITTLE, California
THOMAS REYNOLDS, New York
CANDICE MILLER, Michigan

JUANITA MILLENDER-MCDONALD, California
ROBERT A. BRADY, Pennsylvania
ZOE LOFGREN, California

CONTENTS

July 19, 2006

	Page
Witness List	2
Hearing Charter	3

Opening Statements

Statement by Representative Vernon J. Ehlers, Chairman, Committee on House Administration, U.S. House of Representatives	10
Written Statement	12
Statement by Representative Juanita Millender-McDonald, Ranking Minority Member, Committee on House Administration, U.S. House of Representatives	13
Statement by Representative Sherwood L. Boehlert, Chairman, Committee on Science, U.S. House of Representatives	14
Written Statement	16
Statement by Representative Bart Gordon, Ranking Minority Member, Committee on Science, U.S. House of Representatives	17
Written Statement	17
Statement by Hon. Rush Holt, Representative from the State of New Jersey	18
Written Statement	18
Prepared Statement by Representative Tom Feeney, Member, Committee on Science, U.S. House of Representatives	43
Prepared Statement by Representative Jerry F. Costello, Member, Committee on Science, U.S. House of Representatives	43
Prepared Statement by Representative Lynn Woolsey, Member, Committee on Science, U.S. House of Representatives	44
Prepared statement by Representative Mark Udall, Member, Committee on Science, U.S. House of Representatives	106
Prepared Statement by Representative Darlene Hooley, Member, Committee on Science, U.S. House of Representatives	44
Prepared Statement by Representative Sheila Jackson Lee, Member, Committee on Science, U.S. House of Representatives	45

Witnesses:

Ms. Donetta L. Davidson, Commissioner, Election Assistance Commission	
Oral Statement	46
Written Statement	47
Biography	52
Dr. William Jeffrey, Director, National Institute of Standards and Technology	
Oral Statement	52
Written Statement	54
Biography	56
Ms. Mary Kiffmeyer, Secretary of State for Minnesota	
Oral Statement	57
Written Statement	59
Ms. Linda H. Lamone, Administrator of Elections, Maryland State Board of Elections	
Oral Statement	60
Written Statement	62

Page

Ms. Linda H. Lamone, Administrator of Elections, Maryland State Board of Elections—Continued
Biography 64

Dr. David Wagner, Professor of Computer Science, University of California-Berkeley
Oral Statement 64
Written Statement 66

Mr. John S. Groh, Chairman, Election Technology Council, Information Technology Association of America
Oral Statement 72
Written Statement 73
Biography 78
Financial Disclosure 78

Discussion
Human Factors and HAVA Guidelines, Technology 79
Security in Electronic Voting 80
Voluntary Nature of Standards 82
Paper Trails and Mandatory Audits 83
Role of EAC 84
Dr. Wagner's Study 86
EAC's Guidelines to States 87
Paper Trails 88
Voluntary or Mandated Independent Testing Labs 89
Verification of Voter Identity 97
State Role in Federal Elections 98
Legislation That Addresses Voting Issues 99
Voting Systems in Context of Katrina and Emergency Situations 99
Military Personnel and Voting 100
Standards for Failure Rate 101
Vulnerabilities of Paper Trails and Foreign Investment in Voting Equipment 101
Poll Workers and Human Error 105
Voter Confidence and Turnout 105

Appendix 1: Answers to Post-Hearing Questions

Ms. Donetta L. Davidson, Commissioner, Election Assistance Commission 110

Dr. William Jeffrey, Director, National Institute of Standards and Technology 122

Ms. Mary Kiffmeyer, Secretary of State for Minnesota 125

Ms. Linda H. Lamone, Administrator of Elections, Maryland State Board of Elections 129

Dr. David Wagner, Professor of Computer Science, University of California-Berkeley 136

Mr. John S. Groh, Chairman, Election Technology Council, Information Technology Association of America 149

Appendix 2: Additional Material for the Record

Statement of the U.S. Public Policy Committee of the Association for Computing Machinery 156

Statement of Lawrence Norden, Chair, Task Force on Voting System Security, Brennan Center for Justice, New York University School of Law 159

Comments on the 2005 VVSG, by Roy Lipscomb, Directory of Technology, Illinois Ballot Integrity Project 162

Statement of the National Committee for Voting Integrity (NCVI) 167

Statement of VerifiedVoting.org 172

Maryland Registered Voters' Opinions About Voting and Voting Technologies, Donald F. Norris, National Center for the Study of Elections, Maryland Institute for Policy Analysis and Research, University of Maryland, Baltimore County, February 2006 177

Page

A Study of Vote Verification Technologies for the Maryland State Board of Elections 213

Statement of the U.S. Election Assistance Commission (EAC) 216

Voting System Independent Testing and Certification Process: Comprehensive, Rigorous, and Objective, The Election Technology Council, November 2005 .. 221

Security Analysis of the Diebold AccuBasic Interpreter, David Wagner, David Jefferson, and Matt Bishop, Voting Systems Technology Assessment Advisory Board (VSTAAB) 224

VOTING MACHINES: WILL THE NEW STANDARDS AND GUIDELINES HELP PREVENT FUTURE PROBLEMS?

WEDNESDAY, JULY 19, 2006

HOUSE OF REPRESENTATIVES,
COMMITTEE ON HOUSE ADMINISTRATION,
JOINT WITH THE
COMMITTEE ON SCIENCE,
Washington, DC.

The Committees met, pursuant to call, at 2:02 p.m., in Room 2318 of the Rayburn House Office Building, Hon. Vernon J. Ehlers [Chairman of the Committee on House Administration] presiding.

COMMITTEE ON SCIENCE
U.S. HOUSE OF REPRESENTATIVES

Voting Machines: Will the New Standards and Guidelines Help Prevent Future Problems?

Wednesday, July 19, 2006

2:00 PM – 4:00 PM

2318 Rayburn House Office Building (WEBCAST)

Witness List

Ms. Donetta Davidson
Commissioner
Election Assistance Commission

Dr. William Jeffrey
Director
National Institute of Standards and Technology

Ms. Mary Kiffmeyer
Secretary of State for Minnesota

Ms. Linda Lamone
Administrator of Elections
Maryland State Board of Elections

Mr. John Groh
Chairman
Election Technology Council
Information Technology Association of America

Dr. David Wagner
Professor of Computer Science
University of California at Berkeley

Section 210 of the Congressional Accountability Act of 1995 applies the rights and protections covered under the Americans with Disabilities Act of 1990 to the United States Congress. Accordingly, the Committee on Science strives to accommodate/meet the needs of those requiring special assistance. If you need special accommodation, please contact the Committee on Science in advance of the scheduled event (3 days requested) at (202) 225-6371 or FAX (202) 225-0891.

Should you need Committee materials in alternative formats, please contact the Committee as noted above.

HEARING CHARTER

COMMITTEE ON HOUSE ADMINISTRATION
U.S. HOUSE OF REPRESENTATIVES
JOINTLY WITH THE
COMMITTEE ON SCIENCE
U.S. HOUSE OF REPRESENTATIVES

Voting Machines: Will the New Standards and Guidelines Help Prevent Future Problems?

WEDNESDAY, JULY 19, 2006
2:00 P.M.–4:00 P.M.
2318 RAYBURN HOUSE OFFICE BUILDING

Purpose

The purpose of the hearing is to review new federal voluntary standards for voting equipment, which were issued late last year, to see if they are likely to improve the accuracy and security of voting, and to see if states are likely to adopt the standards.

The new standards, known as the Voluntary Voting Systems Guidelines (VVSG), were required by the *Help America Vote Act* (HAVA), which was enacted in 2002. Under the Act, the Election Assistance Commission (EAC) promulgates the standards, based on recommendations from the Technical Guidelines Development Committee (TGDC), which is chaired by the National Institute of Standards and Technology (NIST). The language in the Act regarding the standards was written by the House Science Committee and the House Administration Committee.

Witnesses

Ms. Donetta Davidson—Commissioner, Election Assistance Commission.

Dr. William Jeffrey—Director, National Institute of Standards and Technology.

Ms. Mary Kiffmeyer—Secretary of State for Minnesota.

Ms. Linda Lamone—Administrator of Elections, Maryland State Board of Elections.

Mr. John Groh—Chairman, Election Technology Council, Information Technology Association of America.

Dr. David Wagner—Professor of Computer Science, University of California at Berkeley.

Overarching Questions

The hearing will address the following overarching questions:

1. Are the new voting equipment standards, if adopted, likely to improve the accuracy and security of voting? What additional elements, if any, are needed to improve the standards? When should the standards be updated?
2. Are states likely to adopt the new voting equipment standards? What needs to be done, if anything, to make the new standards more useful for states and voting equipment manufacturers?
3. What is the status of certifying the labs, known as Voting System Testing Laboratories (VSTLs), that will test voting equipment to see if it complies with standards?
4. How will the new standards, particularly those sections that addressing human factors in voting, improve the usability and accessibility of voting systems?

Overview

- "The U.S. election system is highly decentralized, with primary responsibility for managing, planning, and conducting elections residing at the local jurisdictions—generally at the county level in most states, but some states have delegated election responsibility to sub-county governmental units. Sub-county election jurisdictions in nine states account for about 75 percent of about 10,500 local election jurisdictions in the United States, but about 12 percent of the 2000 U.S. Census population. Local election jurisdictions vary widely in size and complexity, ranging from small New England townships to Los Angeles County, whose number of registered voters exceeds that of many states."[1]
- In October 2002, Congress enacted the *Help America Vote Act* (HAVA) (P.L. 107–252) to help address problems with voting machines that were brought to the public's attention during the 2000 federal election. HAVA encourages states and localities to eliminate punch card and lever voting machines by providing funds to the states to replace such equipment. Under HAVA, the states have received $2.9 billion since 2003 to improve their elections processes, including by purchasing new voting equipment.
- HAVA established an Election Assistance Commission (EAC) to carry out aspects of HAVA. HAVA also established a number of basic requirements that voting machines and systems should meet, and a process by which new voluntary technical standards would be developed to ensure the reliability and accuracy of new voting equipment.
- Under HAVA, draft technical standards for voting system hardware and software are developed by the Technical Guidelines Development Committee (TGDC), a 14-member panel chaired by the Director of the National Institute of Standards and Technology (NIST). The TGDC recommends standards to the EAC, which approves and promulgates voluntary standards after review and input from a HAVA-established Standards Board (composed of State and local elections officials) and a Board of Advisors (appointed by associations representing governors, legislators, election directors, county officials, and others).
- The EAC approved the first edition of these standards, the 2005 Voluntary Voting Systems Guidelines (VVSG), in December 2005, but made the new standards (the 2005 VVSG) officially effective as of December 2007.
- The 2005 VVSG standards are voluntary. States are free to adopt them, in whole or in part, or not at all, as they see fit. Two earlier sets of voluntary standards promulgated by the Federal Election Commission (FEC), one promulgated in 1990 and one promulgated in 2002, are also available. The voluntary nature of these standards means that earlier standards are not necessarily superseded by the promulgation of updated standards. Some states have adopted the 1990 FEC standards, some states have adopted the 2002 FEC standards, some states are in the process of adopting the 2005 VVSG standards prior to their official effective date, some states have created their own standards, and a handful of states have not yet adopted standards for voting equipment.
- In a recent GAO report, *The Nation's Evolving Election System as Reflected in the November 2004 General Election,* which included a survey of states, the GAO noted widespread inconsistency in the use of federal technology standards. For the November 2006 election, 11 states will require local jurisdictions to meet the 1990 FEC standards, 29 states will use the 2002 FEC standards, five will use the draft version of the 2005 VVSG, and the remainder did not require compliance with any federal standard, used a mix of federal standards, had not decided, or did not respond.
- In addition, the same GAO study noted that the performance of the voting systems—such as accuracy, reliability, and efficiency—was not consistently measured by states. Half of jurisdictions were collecting such data, meaning that there is no nationwide data on the performance of voting systems. Such information could help improve technology and elections in the future.

[1] GAO, Elections: *The Nation's Evolving Election System as Reflected in the November 2004 General Election,* GAO–06–450 (Washington, D.C.: June 6, 2006).

Issues

Timing of the 2005 VVSG Versus State Voting Systems Purchases—The transition to the new standards regime has been slow. The members of the EAC were not appointed until the end of 2003, and the EAC was initially provided with little funding to support its activities, including the development of standards. Furthermore, the TGDC could not meet until the EAC had been appointed, so the first TGDC meeting did not take place until July 2004. When the EAC began distributing funds to the states to help them purchase new voting equipment to replace punch-card and lever voting machines, the TGDC had not finished the process of developing the 2005 VVSG.

This has raised concerns that the new standards will not have a significant effect on the technology that is currently being purchased. Today, voting systems meet the 1990 or 2002 FEC standards, but none are certified to meet the 2005 VVSG standards. One of the reasons is that although the 2005 VVSG have been adopted, they are generally recognized to be incomplete. The TGDC still needs to develop a comprehensive suite of tests that instruct vendors and accredited testing laboratories how to assess the performance of voting systems versus the standards. Another reason is that the EAC, when they approved the 2005 VVSG, included a 24-month grace period for states to adopt the standards, reasoning that the testing laboratories had yet to be accredited, there were no test suites to accompany the 2005 VVSG, and that states and vendors had not had time to review and digest the new standards. This means that the standards effectively do not apply until 2007. By this time, all of the federal funds provided to the states under HAVA will have been disbursed.

Security—Numerous reports have been released by computer science experts that detail specific security flaws in electronic voting systems, particularly in voting systems software used in direct record electronic (DRE) or "touch-screen" voting machines. Due to these flaws, most of these experts recommend the use of an independent paper record to ensure that elections officials can audit election results, spot-check for accuracy, and re-count should electronic results be lost or compromised. They have also recommended various security procedures to ensure access to the voting machines is strictly controlled.

These reports have been criticized by the voting systems vendors and by some elections officials as offering unlikely and alarmist scenarios. They point out that, to date, there is no evidence that an electronic voting system has been hacked. They also point out that the creation of a paper record creates additional opportunities for mischief and management headaches for election workers. However, computer security experts warn a relatively unskilled hacker with even a few minutes' access to the machines—either through physical contact or through a wireless connection—could change election results. Hacking aside, they point out that software errors, or errors that are made during the programming of the ballot into the machine to get it ready for a specific election, can lead to errors in the vote count. Up to now, it is these types of problems, rather than hacking, that have led to counting errors by electronic voting machines.

The 2005 VVSG includes technical standards related to electronic voting machine security, but some security experts say that the standards require additional scope and detail. In particular, they say that true security testing goes beyond running through a checklist of tests and should include actually trying different ways of breaking into a system to alter vote counts. This type of testing should be required and carried out routinely on voting systems, they say, before there will be any assurance that systems are truly secure. The 2005 VVSG also contains guidelines for the use of a voter-verifiable paper trail, should states decide to require one. Currently 27 states have chosen to do this. Another eight do not have the requirement although individual jurisdictions within those states have chosen this technology.

Testing—The 2005 VVSG consists of two volumes totaling 370 pages. *Volume I National Certification Testing Guidelines* describes the minimum capabilities, hardware, software, security, and functionality requirements that a voting system should have. This includes such topics as human factors that affect the usability of these systems, requirements for ballot preparation and election programming, and environmental tolerances for heat, cold, and rough treatment such as dropping.

For a standard to be useful, there must be a test or tests to validate that it has been met. For this reason, *Volume II Voting System Performance Guidelines* contains procedural requirements for vendors and test labs and a high level description of the areas that shall be tested. However, it does not contain tests for every topic covered by the 2005 VVSG and therefore the 2005 VVSG will have to be updated with more detailed testing protocols. Currently the VVSG include protocols for the

most basic varieties of environmental testing. For example, the guidelines describe a test (Section 4.6.5.2) where the equipment is heated for a specific period of time to ensure that variations in environmental conditions do not interfere with its basic functions, since equipment could be used or stored (up to months or years) under extremely hot (or cold) temperatures. In another section of the guidelines, standard tests from the International Electrical Code that are already in use are recommended to test for resilience to power disturbance, electromagnetic radiation, lightning surges, and other phenomena.(Section 4.8.1–4.8.8).

However, for more advanced matters such as software security, tests have not been fully detailed in the 2005 VVSG. For example Volume I has an extensive section on standards to protect the security of voting systems. Volume II's section on testing for security mostly relies on requiring the vendor to describe their own security testing, or on the test laboratory designing tests. Although there are tools used by the software industry to check software for errors, as well as malicious code, no specific techniques, procedures, de-bugging software or other tools are listed as mandatory for labs to test voting systems software to meet a security standard. However it is important to note that in the broader software industry software security testing is not particularly standardized because there is so much customization in software.

Usability—Electronic voting machines (i.e., computers, often with "touch screens") have the potential to simplify voting and reduce errors. Their similarly to Automated Teller Machines (ATMs), which many people use on a routine basis, has made their use in the polling place more intuitive for many voters. Electronic voting machines can also be outfitted with devices to help the disabled vote without assistance. Nevertheless, problems with the design and set-up of voting machines, ballots, and the polling places themselves still can make voting a confusing and discouraging experience. But even when the machines are user-friendly and intuitive for voters, they may still remain problematic for poll workers who need to set them up and break them down on Election Day, and solve problems when voting machines do not perform as expected.

In May 2004, before the formation of the TGDC, NIST published a report entitled "Improving the Usability and Accessibility of Voting Systems and Products." This report, often referred to as "the Human Factors Report," detailed how research and best practices developed in human-machine, human-computer, and usability engineering disciplines could be applied to improve the usability of voting systems, both for voters and poll workers, and for the disabled community. The report noted that usability and accessibility were only partially addressed in the FEC voting systems standards, and made recommendations on how usability and accessibility could be addressed in the standards updates mandated by HAVA.

Background

A Brief History of Voting Standards—Before the passage of the *Help America Vote Act* (HAVA), voluntary voting systems standards were developed and promulgated by the Federal Election Commission (FEC). There were two versions of these standards, the 1990 version, and the 2002 version. These standards were developed by volunteers from the elections community that did not necessarily include a range of expertise on technical issues, such as security. The accreditation of the testing laboratories that tested equipment against the FEC standards was performed by the National Association of State Elections Directors. The FEC standards had been originally developed in recognition of the need for minimum performance requirements for voting technologies that were becoming increasingly complex and sophisticated. However, compared with most technical standards, these standards were more descriptive than prescriptive. The design of tests to comply with them was generally left to individual testing laboratories, resulting in differences in interpretation and application of the standards. For these and other reasons, HAVA included the language requiring the development more rigorous standards.

The 2005 VVSG used the 2002 FEC standards as a starting point, although they significantly expanded and refined them. HAVA transferred the responsibility for accrediting the testing laboratories to the newly created EAC, which would accredit laboratories upon the recommendation of NIST. These testing laboratories are now referred to as Voting Systems Testing Laboratories (VSTLs). NIST is evaluating prospective VSTLs through its National Voluntary Laboratory Accreditation Program. NIST will make recommendations to the EAC based on those evaluations about which laboratories to accredit.

VVSG Development and Approval Process—HAVA directed the TGDC to make recommendations to the EAC, which would then have the recommendations reviewed by the EAC Board of Advisors, a 37-member body drawn from federal, state,

and local entities, and Congressional appointees, and by the EAC Standards Board, which is composed of 110 members drawn from State and local election officials. The first meeting of the TGDC was held July 9, 2004, and the TGDC has held regular meetings and teleconferences since that date. The TGDC submitted its recommended draft standards to the EAC May 9, 2005.

HAVA required a public comment period of unspecified length on the draft standards. The EAC held a 90-day public comment period during which time it received and reviewed over 6,000 comments on the proposed guidelines. The EAC made some changes to TGDC's recommended standards based on the public comment, and comments by the Board of Advisors and the Standards Board. The EAC voted to approve the final standards on December 13, 2005, while delaying their official effective date by 24 months to December 2007.

The TGDC continues to meet, as it believes there are major areas for improvement and expansion in the standards. In addition to the test suites to accompany the 2005 VVSG, the TGDC and NIST are working to update the VVSG for 2007, which will complete the standards and guidelines that were not fully addressed in the 2005 VVSG.

Recent Issues—Although the majority of new electronic voting equipment performed well in the 2004 election and in the 2006 primaries held thus far, some problems have occurred. During the 2004 election, the race for the post of agriculture commissioner in North Carolina had to be re-run because a problem in a voting machine caused it to stop counting votes. During the Indiana and West Virginia primaries this year, election officials in several counties had to manually count ballots because of programming errors in the equipment that tabulated the results from the voting machines. Recently tests in Utah revealed potential security vulnerabilities in one manufacturer's machines (see attached news article). Many new voting systems that have exhibited problems related to software errors had their systems evaluated and passed by testing laboratories, which did not catch these errors. This raises questions about how to improve software standards and testing for voting systems so that these types of errors are caught in the future.

Witness Questions

The witnesses were asked to address the following specific questions:

Ms. Donetta Davidson—Commissioner, Election Assistance Commission (EAC).

1. What is the EAC doing to encourage states to adopt the 2005 Voluntary Voting Systems Guidelines (VVSG)? How many states have adopted the VVSG for the 2006 election? How many states do you anticipate will adopt the VVSG for the 2008 election? Why are states adopting or failing to adopt the guidelines?
2. Does the EAC intend to update the VVSG? If so, when will they next be updated and what standards, testing procedures, and other technical issues will be considered as part of the update? What impact will these updates have on equipment already in use?
3. To what extent did you review the VVSG with respect to human factors and usability issues? To what extent do you think human factors and usability need to be addressed in updates of the guidelines?
4. What is the EAC's role in the approval of a certification process for Voting Systems Testing Laboratories (VSTLs) and what is the status of this process? When will the first VSTLs be approved?
5. What actions, in addition to establishing a process to certify VSTLs, does the EAC need to take to ensure that voting equipment meets the 2005 VVSG and future updates?

Dr. William Jeffrey—Director, National Institute of Standards and Technology (NIST).

1. What is the TGDC doing to update the 2005 Voluntary Voting Systems Guidelines (VVSG)? What are the primary gaps in the 2005 VVSG that need to be filled? To what extent would voting equipment still be subject to problems if it complied with the 2005 VVSG?
2. What is NIST doing to implement a certification process for Voting Systems Testing Laboratories (VSTLs) and what is the status of this process? How many testing laboratories have applied for approval and when will recommendations for qualifying laboratories be submitted to the Election Assistance Commission (EAC)?

3. What were the findings and recommendations of NIST's 2004 report "Improving the Usability and Accessibility of Voting Systems and Products," which addressed human factors in voting? To what extent were those findings and recommendations reflected in the 2005 VVSG? To what extent do the 2005 VVSG and the 2004 human factors reports emphasize the importance of ease of use of voting systems for both poll workers and voters?

Ms. Mary Kiffmeyer—Secretary of State for Minnesota.

1. To what extent are the 2005 Voluntary Voting Systems Guidelines (VVSG) being used by Minnesota and why? If Minnesota is not adopting the 2005 VVSG, what standards are you using for voting equipment purchasing decisions and operation, and why did you select these standards?
2. Are the 2005 VVSG comprehensive enough to guide states' voting equipment purchasing decisions and voting systems operation during elections? If so, why, and if not, why not?
3. What do the Election Assistance Commission (EAC) and Technical Guidelines Development Committee (TGDC) need to do to make it more likely that states will update equipment using the latest VVSG? Do the 2005 VVSG need to be changed or improved in any way to make them more useful to the states? If so, what changes or additional information would you recommend for the VVSG? If not, why not?
4. How important are human factors, such as those described in the National Institute of Standards and Technology (NIST) 2004 report "Improving the Usability and Accessibility of Voting Systems and Products," in your selection of voting equipment? Is this report, together with the 2005 VVSG, having an impact on voting systems and elections, and if so, how? If not, why not?

Ms. Linda Lamone—Administrator of Elections, Maryland State Board of Elections.

1. To what extent are the 2005 Voluntary Voting Systems Guidelines (VVSG) being used by Maryland and why? If Maryland is not adopting the 2005 VVSG, what standards are you using for voting equipment purchasing decisions and operation, and why did you select those standards?
2. Are the 2005 VVSG comprehensive enough to guide states' voting equipment purchasing decisions and voting systems operation during elections? If so, why, and if not, why not?
3. What do the Election Assistance Commission (EAC) and the Technical Guidelines Development Committee (TGDC) need to do to make it more likely that states will update equipment using the latest VVSG? Do the 2005 VVSG need to be changed or improved in any way to make them more useful to the states? If so, what changes or additional information would you recommend for the VVSG? If not, why not?
4. How important are human factors, such as those described in the National Institute of Standards and Technology (NIST) 2004 report "Improving the Usability and Accessibility of Voting Systems and Products," in your selection of voting equipment? Is this report, together with the 2005 VVSG, having an impact on voting systems and elections, and if so, how? If not, why not?

Mr. John Groh—Chairman, Election Technology Council, Information Technology Association of America (ITAA); and Vice President of Marketing and Director of International Sales, Elections Systems and Software, Inc., a voting machine manufacturer.

1. To what extent are the 2005 Voluntary Voting Systems Guidelines (VVSG) sufficient to inform the development and manufacture of new voting machines? Is there additional information and guidance voting machine manufacturers need?
2. Do you believe that changes are needed to the 2005 VVSG, and if so, what are they and why are they necessary? If not, why not?
3. What does your industry need in terms of tests and other procedures to ensure that your products meet these guidelines? Do you believe the current process for approval of Voting Systems Test Laboratories (VSTLs) for voting equipment will meet your needs?

4. How important are human factors, such as those described in the National Institute of Standards and Technology (NIST) 2004 report "Improving the Usability and Accessibility of Voting Systems and Products," in your design of voting equipment? Did this report, together with the 2005 VVSG, impact your industry, and if so, how? If not, why not?

Dr. David Wagner—Professor of Computer Science, University of California at Berkeley.

1. What should the Technical Guidelines Development Committee (TGDC) and the Election Assistance Commission (EAC) do to improve the 2005 Voluntary Voting Systems Guidelines (VVSG)? What are the primary gaps in the 2005 VVSG that need to be filled? To what extent would voting equipment still be subject to problems if it complied with the 2005 VVSG?
2. What are the most effective and practical measures that election officials can take today to make existing voting systems as secure and reliable as possible in November?
3. Do the VVSG adequately address human factors and usability issues? Do you think that they need to be improved in this area? If so, why, and if not, why not?

Chairman EHLERS. This hearing will come to order. Welcome to today's hearing on *Voting Machines: Will the New Standards and Guidelines Help Prevent Future Problems?*

First, a few things to get out of the way. We have a unanimous consent on rules for the joint hearing, since this is a joint hearing of both the Science Committee and the Committee on House Administration.

I ask unanimous consent that we conduct today's hearing under Science Committee rules, the five-minute rule, and using the following order of recognition. Opening statements by the Chair, then Ranking Member of House Administration, opening statements by Chair, then Ranking Member of the Science Committee. Following witness testimony, questions from the Chair, then Ranking Member of House Administration. Questions from the Chair, then Ranking Member of the Science Committee, questions from a majority, then minority Member of House Administration, questions from majority, then minority Members of the Science Committee, and so forth, until each Member present has been recognized for the initial round of questions under the five-minute rule. The presiding Chairman may use discretion to ensure orderly and balanced recognition, based upon time of arrival and seniority, as may be appropriate under the circumstances. Without objection, so ordered.

I also ask unanimous consent for the gentleman from New Jersey, Mr. Holt, to join us on the dais for today's hearing, that he be able to ask questions of the witnesses and introduce a statement for the record. Without objection, so ordered.

Now, having taken care of that bit of business, to organize the meeting of the joint Committees, I just want to do a brief explanation of procedure for the witnesses and the Members and audience. Now, we are likely to have a vote on the Floor very, very soon, and the bells will ring, and we will have to go vote. I am hoping it will be only one vote, in which case we probably can go to the Floor vote and be back within 15 minutes. If there is a series of votes, it will be longer, and I beg your forbearance during that time. But we will certainly do it as expeditiously as possible, and I also am very hopeful that we will not have another vote during the course of this hearing, so that we can proceed directly through it.

So, I am pleased to welcome all of you to this joint hearing of the Committees on Science and House Administration to review the development and implementation of the Voluntary Voting System Guidelines.

My main objective in holding this hearing is to discuss how voting technology standards can help us come closer to two very important goals. First, that every citizen knows that their vote is being accurately counted, and second, that every citizen knows that their vote is not being diluted by illegal or improper votes. At this hearing, I look forward to hearing testimony from expert witnesses who may help us understand how voting equipment standards and testing can help improve the accuracy and security of the country's voting systems, and prevent errors and fraud.

The new Voluntary Voting System Guidelines were developed pursuant to the requirements of the *Help America Vote Act of 2002,* or HAVA, and it was the Science Committee and the House Admin-

istration Committee that wrote the language requiring these federal technical guidelines. So, the technical part of the HAVA bill originated in this committee, and it was also very much a joint minority-majority effort—as I recall, Mr. Barcia was the Ranking Member at that time, and he and I worked hand-in-hand in drafting that.

Under HAVA, these draft technical standards for voting systems are developed by the Technical Guidelines Development Committee, TGDC, a 14-member panel chaired by the Director of the National Institute of Standards and Technology, better known as NIST. And the Director is present to offer testimony. The TGDC recommends standards to the Election Assistance Commission, EAC, which approves the voluntary standards after review and input from a HAVA-established Standards Board and Board of Advisors composed of federal, State, and local election officials.

This sounds like an incomprehensible alphabet soup, but the system, although cumbersome, was designed to provide input and action from experts in the field from all different areas, ranging from the smallest township in the country to the largest manufacturers.

The first set of standards under HAVA, known as the Voluntary Voting System Guidelines, were approved by the EAC in December 2005, although their official effective date was delayed until December 2007.

The creation of the 2005 Voluntary Voting System Guidelines was an important step in improving voting standards, but the utility of the guidelines in ensuring honest and fair elections will only be demonstrated by their adoption and implementation in the states. Also, NIST still needs to approve test protocols at companies that will certify that voting systems meet the guidelines.

I look forward to hearing from our witnesses how the guidelines will be used by states in the selection and use of voting equipment, and when we can expect NIST to complete certification of the testing companies. Our hearing today should give us a better understanding of our progress in applying these standards, as well as the efforts underway to facilitate their adoption.

Another important issue with regard to voting standards is the ability to update the guidelines as circumstances change and technologies evolve. In the event that the guidelines are updated, some existing equipment may fall out of compliance with the updated regulations. We need to understand what impact these updates will have on equipment—pardon me—already in use, and what guidance the EAC will offer the states in assessing this impact and helping them deal with it.

The matters we will discuss today are technical in nature, and while they may be complicated, the underlying question is a simple one. How will the new standards improve the integrity and accuracy of our voting systems? As the name suggests, the *Help America Vote Act* was enacted to help our citizens exercise their right to vote. Technology can help us advance that goal, but it must be deployed with the proper standards, standards that take into account the human factors that will determine whether or not real people, the voters, will be able to use the technology with ease and confidence. Our objective is to ensure that every person who is eligible to vote is able to do so with the assurance that their vote will

be accurately counted, and that their vote will not be nullified by fraud.

I would like to thank our witnesses for offering their insight into these issues, as we continue to improve our voting systems and processes on behalf of all Americans.

Now, just one last, one other quick comment. I notice a number of Members in the audience wearing T-shirts demonstrating their support for a paper trail. That is a very important issue. It is not likely to be addressed today, unless some of the witnesses bring it up, but I have discussed it with Dr. Holt, to whom we have granted the privileges of sitting with us and commenting and questioning.

And I am trying to arrange a hearing, a separate hearing on the paper trail, presumably some time in September, but we had too much to do already in this hearing, without having to deal with that separate issue, which is complex and important, and I felt it deserved a hearing of its own.

With that, I am very pleased to now recognize Ms. Millender-McDonald, the Ranking Member of the House Administration Committee, for an opening statement.

[The prepared statement of Chairman Ehlers follows:]

PREPARED STATEMENT OF CHAIRMAN VERNON J. EHLERS

Good afternoon. I want to welcome everyone to this joint hearing of the Committees on Science and House Administration to review the development and implementation of the Voluntary Voting Systems Guidelines (VVSG).

My main objective in holding this hearing is to discuss how voting technology standards can help us come closer to two very important goals: First—that every citizen knows that their vote is being accurately counted, and second—that every citizen knows that their vote is not being diluted by illegal or improper votes. At this hearing, I look forward to hearing from expert witnesses whose testimony may help us understand how voting equipment standards and testing can help improve the accuracy and security of the country's voting systems, and prevent errors and fraud.

The new Voluntary Voting System Guidelines were developed pursuant to the requirements of the *Help America Vote Act of 2002,* or HAVA, and it was the Science Committee and House Administration Committee that wrote the language requiring these federal technical guidelines.

Under HAVA, draft technical standards for voting systems are developed by the Technical Guidelines Development Committee (TGDC), a 14-member panel chaired by the Director of the National Institute of Standards and Technology (NIST). The TGDC recommends standards to the Election Assistance Commission (EAC), which approves the voluntary standards after review and input from a HAVA-established Standards Board and a Board of Advisors composed of federal, State and local election officials.

The first set of standards under HAVA (known as the Voluntary Voting Systems Guidelines (VVSG)) were approved by the EAC in December 2005, although their official effective date was delayed until December 2007.

The creation of the 2005 Voluntary Voting Systems Guidelines was an important step in improving voting standards, but the utility of the guidelines in ensuring honest and fair elections will only be demonstrated by their adoption and implementation in the states. Also, NIST still needs to approve test protocols at companies that will certify that voting systems meet the guidelines. I look forward to hearing from our witnesses how the guidelines will be used by states in the selection and use of voting equipment, and when we can expect NIST to complete certification of the testing companies. Our hearing today should give us a better understanding of our progress in applying these standards, as well as the efforts underway to facilitate their adoption.

Another important issue with regard to voting standards is the ability to update the guidelines as circumstances change and technologies evolve. In the event that the guidelines are updated, some existing equipment may fall out of compliance with the updated regulations. We need to understand what impact these updates

will have on equipment already in use, and what guidance the EAC will offer the states in assessing this impact and helping them deal with it.

The matters we will discuss today are technical in nature and, while they may be complicated, the underlying question is a simple one—how will the new standards improve the integrity and accuracy our voting systems? As the name suggests, the *Help America Vote Act* was enacted to help our citizens exercise their right to vote. Technology can help us advance that goal, but it must be deployed with the proper standards—standards that take into account the human factors that will determine whether or not real people—voters—will be able to use the technology with ease and confidence. Our objective is to ensure that every person who is eligible to vote is able to do so, with the assurance that their vote will be accurately counted, and that their vote will not be nullified by fraud.

I would like to thank our witnesses for offering their insight into these issues, as we continue to improve our voting systems and processes on behalf of all Americans.

Ms. MILLENDER-MCDONALD. Thank you so much, Mr. Chairman, and I, too, would like to join you in welcoming all of the expert witnesses, those who are participating with us in the audience, and others today. It is great to see you all here as we convene this joint hearing.

And given that it is a joint hearing, I would like to thank both Chairmen, my own Chair, Ehlers, and Chairman Boehlert, for calling this very important joint oversight hearing.

Given that the Election Assistance Commission, EAC, was created to be the election issue clearinghouse, they are working tirelessly to remedy the inherent problems with lever and punch card machines that plagued past elections. This issue was clearly brought to light during the 2000 Presidential election in Florida. As part of HAVA, the EAC was tasked with updating the Voluntary Voting System Guidelines, which were promulgated by the now-defunct FEC Office of Election Administration. The EAC worked in tandem with the National Institute of Standards and Technology and the Technical Guidelines Development Committee to address computerized voting equipment as well as standards.

The media has focused much of its attention in the last few years on the perceived problems with direct recording electronic, DRE, voting machines, as well as calls for a voter-verifiable paper audit trail, VVPAT. The EAC was tasked by HAVA to determine if there are actual versus perceived problems with paperless DRE voting machines, and recommend standards for states that have decided to implement VVPAT.

I believe that the EAC's chief functions in determining these standards will be the testing certification, decertification, and recertification of voting system hardware and software. To that end, the EAC heard public opinion on the Voting System Guidelines, received over 6,500 comments from the public, and incorporated elements of these comments into the Election Management Guideline Project.

Elections today are not the same as they were 200 years ago, not even 60 years ago. We are moving to a more technologically-driven world, and we need comprehensive standards to reflect these changes. States may decide to adopt the Voluntary Voting System Guidelines in their entirety or in part prior to the effective date of December 2007. However, we are hopeful that all states will implement these standards.

During a hearing held by our committee in July of 2004, Brit Williams, Kennesaw State University Professor of Computer

Science, suggested one way to improve the way elections are run is to test machines before, during, and after elections to verify their soundness. I am interested in hearing the panel's thoughts on this concept. As we are in the midst of the 2006 election cycle, I intend to ask about one of HAVA's mandates for states which requires that each polling station be equipped with at least one machine that is fully accessible to the individuals with disabilities. That mandate became effective January 1 of this year.

One way states may satisfy this obligation is with the use of DRE voting equipment. Now, are all states going to be compliant before this upcoming November election? That is yet to be determined. DRE machines were at one point thought to be the great panacea to the problems associated with the 2000 election, but much concern has continued to brew since the enactment of HAVA. These Voluntary Voting System Guidelines will be directly affecting the way elections are conducted.

So, I look forward to the hearing today, from the panel of experts, about voting machines, and the hearing, and to hear their answers to such questions as, "Will they be secure, while still allowing for people with a disability to vote without assistance and in private?" And Mr. Chairman, I am very pleased that you have suggested that we will have a hearing some time in the near future on the paper trail.

When I had my week off, we all had weeks off here a couple of weeks ago, I heard from an overwhelming amount of constituents on the paper trail issue, and I think it is important that we bring this to the forefront, so Americans across this nation can hear our thoughts on a paper trail.

So, I thank the two Chairmen for convening this hearing, and I look forward to the testimony of this esteemed panel, to answer those questions, some of which I have raised.

Thank you, Mr. Chairman.

Chairman EHLERS. Thank you for your comments. Next, I am pleased to recognize a very, very distinguished gentleman, the Chairman of the full Science Committee, who has devoted a good share of his life to the Congress and to this committee, and unfortunately, has chosen to retire, and will be honored today at a retirement reception.

But Congressman Boehlert from New York has done yeoman service, and I think, frankly, we should, we have a good group here, let us all give him a round of applause for his good work.

The Chairman is recognized for his opening statement.

Chairman BOEHLERT. Thank you very much, Mr. Chairman.

And I have to observe at the outset that we have the entire Congressional Physics Caucus with us here today on the dais. Both Chairman Ehlers and Dr. Holt are distinguished scientists in their own right. Both have Ph.D.s in physics, so it is a pleasure to work in association with you. They are scientists first, politicians second.

I want to join the Chairman in welcoming everyone to this extraordinarily important hearing. Elections are obviously the keystone of our entire democratic system. If elections are not seen as legitimate, the entire American system unravels. But making sure that election results are credible is a trickier and more technical matter than first appears to be the case. That is why our commit-

tees worked together under the leadership of Dr. Ehlers to craft language in the *Help America Vote Act,* requiring new technical standards for voting equipment, and a new testing regime for those standards. That is not the part of the law that got the most attention, but it may prove to be the most important part of the law for the future of American democracy.

I say that because, as the Nation moves to electronic voting systems, that is, to computers, which is a good trend on the whole, the kinds of things that can go wrong with voting machines may become harder to recognize, harder to fix, and harder to prevent. I am referring here mostly to unintentional problems, but security issues become more complex as well.

Over the long-run, newer voting machines are going to require clear, comprehensive technical standards, and testing, to ensure that election results are credible. In the short-run, I think we also need to require paper trails, even though they have their own problems, to ensure that election results can be checked.

I think, excuse me, I think all of us need to pay close attention to the testimony that will be offered today by Dr. Wagner, and to his recommendations for making sure that electronic voting machines make voting more accurate and more secure, not the opposite. I am not endorsing all the recommendations at this point, but I am going to want to hear from each of our witnesses what they think of each of Dr. Wagner's recommendations.

And I don't simply want to hear that the recommendations will be expensive. How much is American democracy worth? As a nation, we ought to be willing to invest in election equipment, invest as much in election equipment as we invest in campaign ads. Frankly, we in Congress haven't invested as much as we should in the development of the new standards, which have been delayed as a result. I am not happy to learn that new standards are not likely to be fully enforceable until 2010, at the earliest, and that is only in states that choose to adopt them. I have to say that I had wanted the *Help America Vote Act* to require any state using federal money to purchase voting equipment to abide by the standards, but we weren't able to get that language into the bill.

But what we have now is an entirely voluntary system, and we need to make sure that it works. I hope that today, our committees will get clear guidance on what needs to be done to ensure that comprehensive standards get developed, to ensure that those standards are capable of preventing problems with electronic voting machines, and to encourage states to adopt and effectively implement those standards.

And once again, let me say, if we are going to spend taxpayer dollars to develop federal standards, I think we should require that the states that want to access those federal dollars should meet those standards. I am not enamored with the concept that they voluntarily can choose to comply.

That is what is necessary to have credible election results in the future. The essayist E.B. White once defined democracy as "the recurrent suspicion that more than half of the people are right more than half of the time." That makes democracy a pretty fragile construct to begin with, but it is an unworkable idea if we can't accurately count what half of the people are thinking.

I look forward to today's testimony, and I thank you, Mr. Chairman, for the courtesy.

[The prepared statement of Chairman Boehlert follows:]

PREPARED STATEMENT OF CHAIRMAN SHERWOOD L. BOEHLERT

I want to join Chairman Ehlers in welcoming everyone here to this extraordinarily important hearing. Elections are obviously the keystone of our entire democratic system. If elections are not seen as legitimate, the entire American system unravels.

But making sure that election results are credible is a trickier and more technical matter than first appears to be the case. That's why our committees worked together, under the leadership of Dr. Ehlers, to craft language in the *Help America Vote Act* requiring new technical standards for voting equipment and a new testing regime for those standards. That's not the part of the law that got the most attention, but it may prove to be the most important part of the law for the future of American democracy.

I say that because, as the Nation moves to electronic voting systems, that is, to computers—which is a good trend, on the whole—the kinds of things that can go wrong with voting machines may become harder to recognize, harder to fix, and harder to prevent. I'm referring here mostly to unintentional problems, but security issues become more complex as well.

Over the long-run, newer voting machines are going to require clear, comprehensive technical standards and testing to ensure that election results are credible. In the short-run, I think we also need to require paper trails—even though they have their own problems—to ensure that election results can be checked.

I think all of us need to pay close attention to the testimony that will be offered today by Dr. Wagner and to his recommendations for making sure that electronic voting machines make voting more accurate and more secure, not the opposite. I'm not endorsing all of his recommendations at this point, but I am going to want to hear from each of our witnesses what they think of each of his recommendations.

And I don't simply want to hear that the recommendations will be expensive. How much is American democracy worth? As a nation, we ought to be as willing to invest in election equipment as we are in campaign ads.

Frankly, we in Congress haven't invested as much as we should in the development of the new standards, which have been delayed as a result. I'm not happy to learn that new standards are not likely to be fully enforceable until 2010 at the earliest—and that's only in states that choose to adopt them. I have to say that I had wanted the *Help America Vote Act* to require any state using federal money to purchase voting equipment to abide by the standards, but we weren't able to get that language into the bill.

But what we have now is an entirely voluntary system, and we need to make that work. I hope that today our committees will get clear guidance on what needs to be done to ensure that a comprehensive standards gets developed, to ensure that those standards are capable of preventing problems with electronic voting machines, and to encourage states to adopt and effectively implement those standards. That's what's necessary to have credible election results in the future.

The essayist E.B. White once defined democracy as "the recurrent suspicion that more than half of the people are right more than half of the time." That's makes democracy a pretty fragile construct to begin with. But it's an unworkable idea if we can't accurately count what half of the people are thinking.

I look forward to today's testimony. Thank you.

Chairman EHLERS. And I thank you for your comments. And before we go to the next person, I just want to comment on the reference to Dr. Holt and myself as physicists. We are the first two research physicists elected to the Congress. When he was elected, we decided to form a Physicists' Caucus. Since then, we have been looking for a suitable office for the caucus, but so far, we have not found a phone booth with a chalkboard. And physicists can't meet without a chalkboard.

Having said that, it is my pleasure to recognize the Ranking Member of the Science Committee. I am pleased to recognize Mr. Gordon for his opening statement.

Mr. GORDON. Thank you, Mr. Chairman. Let me add my welcome to everyone that is here today. It is good to see a full house. I also want to welcome our friends and colleagues from the House Administration, many of whom had little trouble finding this room, since Dr. Ehlers and Zoe Lofgren also do double duty here, so we welcome you, and certainly, Rush Holt, who has taken a major role in this issue.

But most importantly, I want to welcome our distinguished guests today, who are going to be speaking to us. I am in that position where, being the fourth speaker, most everything has been said. I haven't said it, and I am going to leave it that way, and just quickly say that as my friend, Chairman Boehlert, pointed out, the root and foundation of any democracy is a feeling among its people that once the election is over with, you were treated fair and square, and that you can go home, be upset maybe that your candidate didn't win, but you can then be a part of the loyal opposition, and the process can move forward until the next election.

When you don't have that, as we are seeing in Mexico right now, problems persist. Recently, concerns have developed in our country about that level of being fair and square, whether it is intentional or unintentional, and so, I hope that today's hearings will help us to move forward. I have to say that I am disappointed that we are behind schedule, and I do not see, obviously, much taking place in 2006, maybe not even 2008. We need to move forward. There needs to be transparency. There needs to be credibility in this process, and we need to move on with it.

So, thank you, and hopefully, this hearing today will allow us to do so.

[The prepared statement of Mr. Gordon follows:]

PREPARED STATEMENT OF REPRESENTATIVE BART GORDON

I want to welcome everyone to this afternoon's hearing and to welcome our House Administration colleagues to the Science Committee hearing room.

The development of new voting standards by NIST and the Election Administration Commission (EAC) was meant to improve the accuracy, reliability and integrity of our voting systems. However, the facts highlight that these updated guidelines may have little impact on the 2006 or even the 2008 elections.

According to a June 2006 GAO report, eleven states are still using the 1990 Federal Election Commission (FEC) standards which are known to be inadequate. Twenty-nine states are using the 2002 FEC standards which GAO has also found to be weak. Currently, only five states plan on using the new 2005 standards developed by the EAC and NIST during the 2006 elections. In addition, there are serious questions about the current testing procedures used to determine if voting equipment meets any standards. The current conformance testing is not transparent and results are not public. This issue needs to be addressed now.

While NIST has worked hard to develop new standards, the revised EAC/NIST standards will not go into effect until December 2007. For these new standards, transparent conformance tests still need to be developed. While these standards and test methods were being developed, states were already purchasing new voting equipment.

Will this new equipment meet the 2005 standards? At this time I don't think we know with any certainty.

We do know that there are questions about the security and integrity of direct recording electronic voting equipment. And some states have experienced significant problems with these voting systems.

Finally, if purchased equipment does not meet updated standards and conformance tests, we need to decide who will pay for equipment upgrades.

I don't have the answers to these questions, but we have a distinguished panel with a wide range of experience and views on this issue. I hope they can shed some light on the issues I've raised, and I look forward to their comments.

Chairman EHLERS. I thank the gentleman for his statement, and I do have good news. We thought we would be interrupted by votes before this, but fortunately, the manager's action on the House floor have taken up three suspensions, which will postpone votes, perhaps to the point where we can finish the hearing. That remains to be seen.

Mr. HOLT. Mr. Chairman.

Chairman EHLERS. Yes.

Mr. HOLT. I would like to thank you for the courtesy of taking part in this. I appreciate your calling the hearing. I would like to ask unanimous consent to put, at this point, in the record a written statement, which will make the basic point that the subject of today's hearing, standards for design and certification, are good, but not sufficient, and that one needs auditability, and a required audit process, as well.

And I will have to excuse myself at some point soon for an Intelligence Committee hearing, but I thank the gentleman, the Chairman, for his courtesy.

Chairman EHLERS. Well, I thank you, and it is a pleasure to find out that there is some intelligence in the Congress.

I will make the general statement, if there are Members who wish to submit additional opening statements, your statements will be added to the record. Without objection, so ordered.

[The statement of Representative Rush Holt follows:]

PREPARED STATEMENT OF REPRESENTATIVE RUSH HOLT

Chairmen Ehlers and Boehlert, Ranking Members Millender-McDonald and Gordon, Honored Members of the Committees, I am Rush Holt, Representative from the 12th District of New Jersey. I would like to reiterate my gratitude, as expressed on the occasion of the House Administration Committee's recent hearing on the issue of voter identification, that the Committees are jointly addressing another critical aspect of election reform—the Voluntary Voting Systems Guidelines for voting equipment. But I would like to say again, however, that I fear that our opportunity to meaningfully and decisively address the very real issue of the security risks and accuracy problems plaguing our electronic voting systems is passing us by. At a result, this November may yet again strike a blow to the public's confidence in our elections.

It was my honor to speak before the House Committee on Science, Subcommittee on Technology, on this matter two years ago, when it held a hearing in June 2004 entitled *"Testing and Certification of Voting Equipment: How Can the Process Be Improved?"* In my statement to the Committee, I reviewed some of the history of the development of voting system standards, first implemented in 1990, and updated in 2002, to cover punch card, optical scan, and direct recording electronic (DRE) voting systems.

But I also directed the Committee's attention to the 2001 Report of the CalTech MIT Voting Technology Project—*"Voting—What Is, What Could Be,"* which stated that "[t]he existing standards process is a step in the right direction, but it does not cover many of the problems that we have detected. . .important things are not reviewed currently, including ballot and user interface designs, auditability, and accessibility." The CalTech MIT study also recommended, under the heading "Create a New Standard for Redundant Recordings," that "[a]ll voting systems should implement multiple technological means of recording votes. For example, DRE/touchscreen systems should also produce optical scan ballots. This redundancy insures that independent audit trails exist post-election, and it helps insure that if fraud or errors are detected in one technology there exists an independent way to count the vote without running another election."

Since then, the same recommendation has been made by one authoritative body after another. In the wake of the 2004 election, the Commission on Federal Election Reform, Co-Chaired by former President Jimmy Carter and former Secretary of State James Baker, again studied the problem of electronic voting security. The Commission released its findings in September 2005, in a report entitled *"Building*

Confidence in U.S. Elections." The Commission concluded, among other things, that "of course, DREs are computers, and computers malfunction," and that "[t]he standards for voting systems, set by the EAC, should assure both accessibility and transparency in all voting systems." However, the EAC cannot mandate transparency in the standards because HAVA does not mandate it. Therefore, the Commission recommended that "Congress should pass a law requiring that all voting machines be equipped with a voter-verifiable paper audit trail and, consistent with HAVA, be fully accessible to voters with disabilities." It further noted that "[t]his is especially important for [DREs]" in order to "provide a backup in cases of loss of votes due to computer malfunction" and "to test—through random selection of machines—whether the paper result is the same as the electronic result." Finally, it noted that "paper trails and ballots currently provide the only means to meet the Commission's recommended standards for transparency."

Just last month, the Brennan Center for Justice, working in conjunction with NIST, Ron Rivest of M.I.T. (a co-author of the CalTech/MIT study), Howard Schmidt, former White House Cyber Security Advisor for George W. Bush and Chief Security Officer for Microsoft and eBay, and other computer security experts, released the most comprehensive and rigorous analysis to date of e-voting security risks and remedies. My colleagues Tom Davis and Tom Cole joined me at a press conference commending the Brennan Center on the Report.

Entitled *"The Machinery of Democracy: Protecting Elections in an Electronic World,"* the report explained in detail the various risks associated with using all of the three major types of voting systems now used in the United States. The report assumed, in its analysis, that (1) an Independent Testing Authority (ITA) has certified the model of voting machine used in the polling place; (2) Acceptance Testing was performed on machines as soon as or soon after they were received by the County; (3) pre-election Logic and Accuracy testing was performed by the relevant election official; (4) prior to opening the polls, every voting machine and vote tabulation system was checked to see that it was still configured for the correct election, including the correct precinct, ballot style, and other applicable details; and (5) the jurisdiction was not knowingly using any uncertified software that is subject to inspection by the ITA. Even so, however, the report found that "[a]ll three voting systems have significant security and reliability vulnerabilities, which pose a real danger to the integrity of national, State, and local elections." To mitigate those risks, the report recommended a voter-verified paper record accompanied by automatic routine random audits of those records, a ban use of voting machines with wireless components, and other security measures, all to be implemented as expeditiously as possible.

That same month, the National League of Women Voters issued similar recommendations in a resolution passed at its Annual Convention in June. The resolution states that the League of Women Voters "supports only voting systems that are designed so that: they employ a voter-verifiable paper ballot or other paper record, said paper being the official record of the voter's intent. . .the paper ballot/record is used for audits and recounts. . .the vote totals can be verified by an independent hand count of the paper ballot/record. . .and routine audits of the paper ballot/record in randomly selected precincts can be conducted in every election, and the results published by the jurisdiction."

I expect the Chairman recalls the testimony of Michael Shamos, Professor of Computer Science at Carnegie Mellon University, who also spoke before the Subcommittee on Technology during its hearing in June 2004. At the very outset of his remarks, he said: "I am here today to offer my opinion that the system we have for testing and certifying voting equipment in this country is not only broken, but is virtually nonexistent. It must be re-created from scratch or we will never restore public confidence in elections. I believe that the process of designing, implementing, manufacturing, certifying, selling, acquiring, storing, using, testing and even discarding voting machines must be transparent from cradle to grave, and must adhere to strict performance and security guidelines that should be uniform for federal elections throughout the United States."

Chairman Ehlers, you and I are scientists. Like scientists, we rely on evidence. Scientists can collect evidence and collect more evidence. As policy-makers, we know that for policies that determine how our government functions, we must not wait so long that delay harms the functioning of our government and thus harms the people. We are at that point today: we need no more inquiry on the issue of the transparency and independent auditability in our elections. The public, numbering in the millions—and I believe that is no exaggeration—is losing confidence in the integrity of our voting systems. This undermines the essential democracy of America. Citizens are beginning to doubt our ability to govern ourselves. What could be more important?

We have heard from a President, a Cabinet Secretary, a White House advisor on computer security, computer security experts at NIST, election integrity experts at the Brennan Center for Justice, the League of Women Voters and many other voting integrity activists, and a lengthy list of this nation's top computer security experts. After extensive study and consideration, they all agree that (1) no matter how rigorous the testing and certification process, it cannot, by itself, prevent fraud or errors; (2) voter-verified paper records accompanied by routine random audits are necessary as an independent audit mechanism; and (3) paper is the only technology available at this time by which we may establish such independent auditability.

I have attached a document prepared by the voting integrity group *VotersUnite.org.* This map sets forth a partial list—51 reported incidents—in which ballot programming errors recently resulted in votes being recorded other than as evidently intended by the voter. It is important to note that in every single instance, the machines which failed had already been tested and certified and were either deployed or about to be deployed for use in actual elections, under our existing testing and certification regimen. What follows are just a few examples from this document, entitled *"Vote-Switching Software Provided by Vendors":*

- In June, 2006, in Pottawattamie County, Iowa, software in optical scanners recorded votes inaccurately. The County Auditor became suspicious when a college student was found to be leading the incumbent County Recorder (who'd held the job since 1983) by a count of 99 to 79 absentee votes. She stopped the computer count and ordered a hand count of the paper absentee ballots, and the result was reversed—the incumbent had 153 votes and the student had just 25.
- In May 2006, in a School Board election near Grand Rapids Michigan, optical scanners erroneously gave votes to non-existent write-in candidates. Brand new machines malfunctioned in 15 of 16 townships and the town of Hastings in Barry County, recording in one instance 90 write-in votes in a contest that received in only 127 votes. In only one township, as confirmed by a hand count of the optical scan ballots, did the software count the votes accurately.
- In June 2006, in Leflore and Jackson Counties, Mississippi, various glitches were experienced in the use of new paperless voting machines, including ballots not being properly customized for each precinct. An AP story published on June 7 about the irregularities quoted a County-level political official as saying: "If a hacker comes in and hacks that program, what are we going to do then? . . .We're praying that everything will work out for us."

These are but a few of the numerous incidences of electronic voting irregularities that have plagued this year's primary season. And the most important point about these examples is that, in the first two incidents, something unusual tipped off election officials and, because optical scan ballots were used, they were able to prove who actually won by counting those voter-verified paper ballots. In the third example, the fact that the ballots were not programmed correctly for each precinct was discoverable, but, because paperless touch screens produce no voter-verified paper ballots, the accuracy of the ultimate vote count could not be confirmed. In this third example, the political official in question was left to simply "pray" for accuracy.

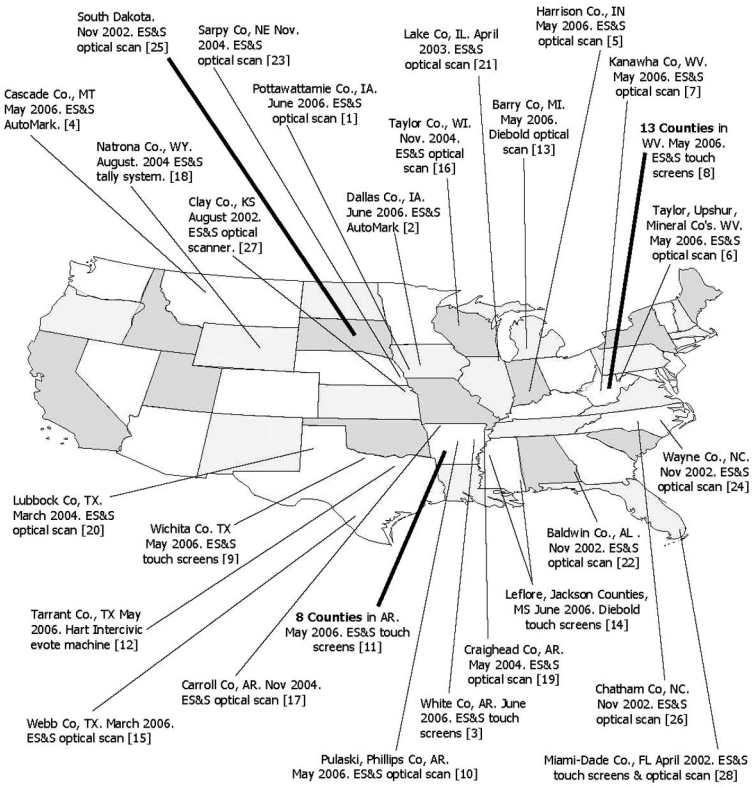
Hoping and praying for an accurate vote count is simply unacceptable in a democracy. We need no further study to conclude that vote counting must be transparent, and that the only way to achieve transparency today and for the foreseeable future is to require a voter-verified paper audit trail on all election machines. My legislation, the *Voter Confidence and Increased Accessibility Act of 2005* (H.R. 550) would establish a uniform national requirement for a voter-verified paper record for every vote cast, routine random audits of a small percentage of the electronic tally of those votes, a ban on the use of wireless devices, and other measures that will ensure not just the accessibility, but the independent auditability and transparency of our elections.

I thank the Committees again for giving their time and attention to matters of election reform, and I urge the Committee on House Administration to conduct a hearing or schedule a mark-up of my Voter Confidence Act as expeditiously as possible.

Vote-Switching Software Provided by Vendors

A Partial List — 51 Ballot Programming Flaws Reported in the News
These were detected; how many were not?

Ballot programming maps votes to candidates. Flaws cause votes to be counted wrong, often leaving totals unchanged. Voting machine vendors do the ballot programming for most jurisdictions in the U.S.



Detailed descriptions **www.VotersUnite.Org/info/mapVoteSwitch.pdf**

[1] **Faulty voting machines delay results; counting under way.** The Daily Nonpareil Online. June 7, 2006. Tim Rohwer, Staff Writer. http://www.zwire.com/site/news.cfm?newsid=16751509&BRD=2703&PAG=461&dept_id=555106&rfi=6

[2] **Too Much, Too Fast, More Than They Can Chew.** VoteTrustUSA. June 9, 2006. John Gideon. http://www.votetrustusa.org/index.php?option=com_content&task=view&id=1378&Itemid=51

[3] **Voters to decide candidates in runoff.** The Daily Citizen. June 12, 2006. Jeff Hunter. http://www.thedailycitizen.com/articles/2006/06/13/news/top_stories/top01.txt

[4] **Glitch, absentee votes slow results.** Great Falls Tribune. June 8, 2006. Sonja Lee, Tribune Staff Writer. http://www.greatfallstribune.com/apps/pbcs.dll/article?AID=/20060608/NEWS01/606080310/1002

[5] **Ballot-counting problem.** WHAS11.com. May 15, 2006. http://www.whas11.com/topstories/stories/WHAS11_TOP_ballotcounting.42e3d88f.html

[6] **Several Counties Have Vote Counting Problems.** WOWKTV 13. May 10, 2006. Dave Kirby. http://wowktv.com/story.cfm?func=viewstory&storyid=10787

[7] **Kanawha's dry run of voting machines remains incomplete.** Charleston Gazette. May 03, 2006. Archive http://www.votersunite.org/article.asp?id=6596

[8] **Election test delayed.** TMCnet. May 1, 2006. by Charleston Gazette writer Phil Kabler and AP. http://www.tmcnet.com/usubmit/2006/05/01/1628275.htm

[9] **Vendor bender. City clerk blames ES&S for Election Day difficulties.** Times Record News. May 14, 2006. Robert Morgan. Archived at http://www.votersunite.org/article.asp?id=6598

[10] **Recount Planned In Close Race For State House Nomination.** Todays THV. June 2, 2006. http://www.todaysthv.com/news/news.aspx?storyid=29413

[11] **Eight counties won't use electronic equipment in runoff.** The Log Cabin Democrat. June 9, 2006. by Andrew DeMillo, AP. http://ap.thecabin.net/pstories/state/ar/20060609/4000271.shtml

[12] **Ballot problems mark 1st day of early voting.** Star-Telegram. May 2, 2006. Neil Strassman. http://www.dfw.com/mld/dfw/news/local/14479735.htm

[13] **Malfunction delays Hasting results.** The Grand Rapids Press. May 04, 2006. By Ben Cunningham. http://www.mlive.com/news/grpress/index.ssf?/base/news-0/1146754492135040.xml&coll=6

[14] **Most voting goes smoothly. A few glitches in primary, not serious.** Sun Herald. June 7, 2006. By Shelia Byrd, AP. http://www.sunherald.com/mld/sunherald/news/state/14758095.htm

[15] **Election Uproar; County officials say there were plenty of red flags.** Laredo Morning Times, March 14, 2006 by Julie Daffern. http://www.zwire.com/site/index.cfm?newsid=16299334&BRD=2290&PAG=461&dept_id=473478&rfi=8

[16] **About 600 Medford ballots cast in November ignored.** Mar 12, 2005. Marshfield News-Herald. http://www.wisinfo.com/newsherald/mnhlocal/284049485656926.shtml

[17] **Computer glitch blamed for miscount in JP voting.** Carroll County Star Tribune. November 10, 1004. By Anna Mathews. Reproduced at http://www.votersunite.org/article.asp?id=3889

[18] **Clerk changes election vote totals.** Star-Tribune. August 21, 2004. By Matthew Van Dusen, staff writer. http://www.casperstartribune.net/articles/2004/08/21/news/casper/6c2e825b3f9e154187256ef70007adbb.txt

[19] **Commission OKs results of elections.** Jonesboro Sun, May 28, 2004. By LeAnn Askins. http://www.jonesborosun.com/archivedstory.asp?ID=9486

[20] **Software blamed in Precinct 8 Democratic chair race mixup.** Lubbock online.com; March 11, 2004; By Brian Williams, Avalanche-Journal. http://www.lubbockonline.com/stories/031104/loc_031104030.shtml

[21] **Returns are in: Software goofed — Lake County tally misled 15 hopefuls.** Chicago Tribune; April 4, 2003; By Susan Kuczka, Tribune staff reporter. Reproduced at http://www.vote.caltech.edu/mail-archives/votingtech/Apr-2003/0096.html

[22] **Voting snafu answers elusive.** The Mobile Register; 28 Jan 2003; by Brendan Kirby, staff writer. Referenced at http://www.votewatch.us/Members/Unregistered%20User/ electionexperience.2004-08-12.9166974619

[23] **A late night in Sarpy; glitches delay results.** Omaha World-Herald, 6 November 2002; Referenced in *Black Box Voting*, by Bev Harris. Chapter 2.

[24] **Winners' may be losers.** The News and Observer; November 12, 2002; By Wade Rawlins and Rob Christensen.

[25] **Analysis: Senate races in Minnesota and South Dakota.** NPR: Morning Edition, 6 November 2002; Ref. in Black Box Voting by Bev Harris, Chapter 2.

[26] **Mechanic to smooth vote.** New Observer. October 15, 2004. By Jessica Rocha, Staff Writer. http://newsobserver.com/news/story/1730333p-7996316c.html

[27] **Aug. 6 ballot problems alleged: Clay, Barton county candidates seek review of races.** Lawrence Journal-World. August 22, 2002. AP. http://www.ljworld.com/section/election02/story/103526

[28] **Technician's Error, Not Machines, To Blame In Dade Election Mix-Up.** The Miami Herald. April 4, 2002. By Oscar Corral.

Vote-Switching Software Provided by Vendors — A Partial List Reported in the News

Ballot programming maps votes to candidates. Flaws cause votes to be counted wrong, often leaving totals unchanged.
Voting machine vendors do the ballot programming for most jurisdictions in the U.S.

(Map Handout)

Map #	Date	Machine	Place/Description
1	June 2006	ES&S Optical Scan (M-100)	**Pottawattamie County, Iowa.** Ballot programming error by ES&S causes new optical scanners to tabulate votes incorrectly. [1] Things began to look fishy, [Pottawattamie County Auditor Marilyn Jo] Drake said, when the county's new computers counted the absentee ballots in the Republican Party's county race between longtime Recorder John Sciortino and newcomer Oscar Duran. Absentee ballots are the ones counted first. When all of those were counted, Duran, a University of Nebraska at Omaha student, had 99 votes, while Sciortino, the county recorder since 1983, had just 79. ... Drake said she decided to count the absentee ballots by hand to determine if the computers were counting correctly. They weren't - not by a long shot. The actual absentee ballot count in the recorder's race when done by hand found Sciortino had 153 votes and Duran just 25. It was then that she decided to stop the computer counting in all the races. "They could be tainted, we don't know," Drake said.
2	June 2006	ES&S AutoMark	**Dallas County, Iowa.** ES&S mis-programmed the ballots on the AutoMark. The review screen didn't match the marks on the paper ballot. [2] [Charles Krogmeier of the Secretary of State's staff] told VoteTrustUSA that a professor from Drake University asked to use the AutoMark machine when he voted. He went through the ballot, marking his choices, and when he was through he checked the ballot to find that one race had been swapped.

[1] **Faulty voting machines delay results; counting under way.** The Daily Nonpareil Online. June 7, 2006. by Tim Rohwer, Staff Writer.
http://www.zwire.com/site/news.cfm?newsid=16751509&BRD=2703&PAG=461&dept_id=555106&rfi=6

[2] **Too Much, Too Fast, More Than They Can Chew.** VoteTrustUSA. June 9, 2006. By John Gideon.
http://www.votetrustusa.org/index.php?option=com_content&task=view&id=1378&Itemid=51

Vote-Switching Software Provided by Vendors — A Partial List Reported in the News

Map #	Date	Machine	Place/Description
3	June 2006	ES&S iVotronic	**White County, Arkansas.** ES&S provides flawed ballot programming for the touch screens.[3] After initial problems with the county's new iVotronic electronic voting machines — including faulty electronic ballots, that forced the use of homemade paper ballots in early voting — White County Clerk Tanya Burleson said ballots in today's runoff will be cast electronically as originally planned.
4	May 2006	ES&S AutoMark	**Cascade County, Montana.** Programming problems occurred with the new AutoMark system.[4] Clerk and Recorder Peggy Carrico said most of the systems worked, although the AutoMark in Belt was shut down because of a programming problem.
5	May 2006	ES&S Optical scanner	**Harrison County, Indiana.** Flawed ballot programming errors by ES&S were detected in the testing on ES&S optical scanners.[5] Time didn't allow the revised programming to be tested. Programming errors in automatic tabulation equipment connected to voting machines were discovered by county officials before and during the primary. After the problems were discovered during a routine test before the election, county officials returned some of the equipment to the Omaha company for reprogramming, but there wasn't time before the primary to perform a second test, said AJ Feeney-Ruiz, a spokesman for Secretary of State Todd Rokita.
6	May 2006	ES&S Optical Scanners	**Taylor County, Upshur County, and Mineral County, West Virginia.** ES&S provided flawed programming for the optical scanners. [6] None of Taylor County's votes could be counted last night because the main computer would not read tabulators from individual voting machines. Upshur County's counter was in such bad shape that as of midnight the county was trying to get a similar machine from a neighboring county. Mineral County's optical scan ballot counter was producing **skewed results.**

[3] **Voters to decide candidates in runoff.** The Daily Citizen. June 12, 2006. By Jeff Hunter. http://www.thedailycitizen.com/articles/2006/06/13/news/top_stories/top01.txt

[4] **Glitch, absentee votes slow results.** Great Falls Tribune. June 8, 2006. By SONJA LEE, Tribune Staff Writer. http://www.greatfallstribune.com/apps/pbcs.dll/article?AID=/20060608/NEWS01/606080310/1002

[5] **Ballot-counting problem.** WHAS11.com. May 15, 2006. http://www.whas11.com/topstories/stories/WHAS11_TOP_ballotcounting.42e3d88f.html

[6] **Several Counties Have Vote Counting Problems. New voting systems were used for the first time.** WOWKTV 13. May 10, 2006. by Dave Kirby. http://wowktv.com/story.cfm?func=viewstory&storyid=10787

Vote-Switching Software Provided by Vendors — A Partial List Reported in the News

Map #	Date	Machine	Place/Description
7	May 2006	ES&S Optical Scanners	**Kanawha County, West Virginia.** Ballot programming flaws were provided by ES&S.[7] Kanawha County officials tried to test the county's new optical scan voting machines on Tuesday, but were unable to complete the dry run because the machines were not fully programmed.
8	May 2006	ES&S iVotronic	**West Virginia.** ES&S ballot programming errors were discovered before the elections on iVotronics touch screens in 13 out of 34 counties using the machines.[8] Ireland said the number of counties reporting problems with ES&S-prepared ballot software has increased to 13 of the 34 counties that have contracts with the company to provide electronic voting systems. A glitch in some of the systems allows users of the company's Ivotronic [sic] machines to cast ballots and have their votes recorded correctly, but does not count the votes properly.
9	May 2006	ES&S iVotronic	**Wichita Falls, Texas.** ES&S provided flawed programming for the touch screens.[9] And according to City Clerk Lydia Ozuna the blame rests firmly on the shoulders of Election Systems and Software, the county's election vendor. ... Besides a delay in ballot counting, Ozuna said she had received calls about difficulties with the electronic voting machines. Poll workers called in saying the machines were not working properly. Ozuna said she had hired a person from ES&S to solve issues with the machines. Programming was the main reason for the problems, she said.
10	May 2006	ES&S Optical scanner	**Pulaski County and Phillips County, Arkansas.** ES&S provided flawed ballot programming in both counties.[10] Daniels said that in Pulaski and Phillips counties, the problems involved old optical scanners that were not programmed adequately to count paper ballots in the election. Initial count showed a tie for House District 41, with both candidates getting 613 votes. The recount showed 655 to 664.

[7] **Kanawha's dry run of voting machines remains incomplete.** Charleston Gazette. May 03, 2006. Archived at http://www.votersunite.org/article.asp?id=6596

[8] **Election test delayed.** TMCnet. May 1, 2006. by Charleston Gazette staff writer Phil Kabler and The Associated Press. http://www.tmcnet.com/usubmit/2006/05/01/1628275.htm

[9] **Vendor bender. City clerk blames ES&S for Election Day difficulties.** Times Record News. May 14, 2006. By Robert Morgan. http://www.votersunite.org/article.asp?id=6598

Vote-Switching Software Provided by Vendors — A Partial List Reported in the News

Map #	Date	Machine	Place/Description
11	May 2006	ES&S iVotronic	**Arkansas.** Ballot programming errors were found on iVotronics touch screens in **eight** counties before the election.[11] Pulaski County Elections Director Susan Inman said that county decided not to use the machines after reviewing the programming code from voting machine vendor Election Systems & Software and discovering errors. "In its entirety, it was wrong," Inman said. "I forwarded to them in time for the deadline I was given the information for the runoff." 72 of 75 counties are have ES&S equipment. 64 still used iVotronics in the election.
12	May 2006	Hart Intercivic eSlate	**Tarrant County, Texas.** Ballot programming error on the eSlate omits contests from the ballot.[12] Two City Council races were dropped from the Tarrant County ballot in areas of the city served by non-Arlington schools because of a voting machine programming oversight, county election officials said Monday.
13	May 2006	Diebold AccuVote OS	**Barry County, Michigan.** Diebold delivers flawed ballot programming, which tallied votes incorrectly. [13] Hastings Clerk Thomas Emery saw the problem immediately after receiving the roll from the precinct where he had voted. "The person I voted for had zero votes, and I know how to fill in an oval," he said. Emery voted for the candidate on the top line of the ballot. The fourth line of the ballot -- reserved for write-in candidates -- accumulated 90 votes from only 127 ballots cast at the precinct. "I knew for certain there wouldn't be 90 write-ins," Emery said.

[10] **Recount Planned In Close Race For State House Nomination.** Todaysthv.com. June 2, 2006. http://www.todaysthv.com/news/news.aspx?storyid=29413

[11] **Election Problems Persist For Eight Counties.** Today's THV. June 8, 2006. http://www.todaysthv.com/news/news.aspx?storyid=29699

Eight counties won't use electronic equipment in runoff. The Log Cabin Democrat. June 9, 2006. by Andrew DeMillo, Associated Press Writer. http://ap.thecabin.net/pstories/state/ar/20060609/4000271.shtml

[12] **Ballot problems mark 1st day of early voting.** Star-Telegram. May 2, 2006. By Neil Strassman. http://www.dfw.com/mld/dfw/news/local/14479735.htm

[13] **Malfunction delays Hasting results.** The Grand Rapids Press. May 04, 2006. By Ben Cunningham. http://www.mlive.com/news/grpress/index.ssf?/base/news-0/1146754492135040.xml&coll=6

Vote-Switching Software Provided by Vendors — A Partial List Reported in the News

Map #	Date	Machine	Place/Description
14	June 2006	Diebold AccuVote TS	**Leflore, Jackson Counties, Mississippi.** Ballot programming by Diebold was incorrect on touch screens in these two counties.[14] In Leflore and Jackson counties, early voters had to cast paper ballots because the touch-screen machines were not customized for each precinct, said David Blount, spokesman for Secretary of State Eric Clark. The machines were fixed by Tuesday afternoon, he said. The problems prompted the Leflore County election commissioners to petition the Board of Supervisors for their own technician.[15] Diebold Election Systems, as part of its contract, will offer assistance to the county for five years. But the county's difficulties during the June 6 primary were due to improper programming by a Diebold technician. These problems prompted the commission's request.
15	March 2006	ES&S Optical AIS 315	**Webb County, Texas** ES&S blamed by county for errors in programming and inadequately training county staff.[16] Due to a programming error, the PEBs could not be used and tabulators had to read each individual flash card, significantly delaying the vote tally. The company prepared all software for the election. Additional problems cited include delays of three days before receiving coding for electronic ballots, following mistakes involving receipt of nearby McMullen County codes. The County is considering a suit against ES&S.[17] Webb County Commissioners Court may take its first step toward suing Election Systems and Software, Inc. today. The county paid nearly $900,000 for the electronic voting machines that officials alleged had programming errors and inadequately trained staff.

[14] **Most voting goes smoothly. A few glitches in primary, not serious.** Sun Herald. June 7, 2006. By Shelia Byrd, AP. http://www.sunherald.com/mld/sunherald/news/state/14758095.htm

[15] **Voting Machines.** The Greenwood Commonwealth. June 28, 2006. By Susan Montgomery. http://www.zwire.com/site/news.cfm?newsid=16858105&BRD=1838&PAG=461&dept_id=104621&rfi=6

[16] **Election Uproar; County officials say there were plenty of red flags** Laredo Morning Times, March 14, 2006 by Julie Daffern. http://www.zwire.com/site/index.cfm?newsid=16299334&BRD=2290&PAG=461&dept_id=473478&rfi=8

[17] **Suit eyed in vote machine controversy.** Laredo Morning Times, June 12, 2006. By Kirsten Crow. http://www.lmtonline.com/site/news.cfm?newsid=16776354&BRD=2290&PAG=461&dept_id=569392&rfi=6

Vote-Switching Software Provided by Vendors — A Partial List Reported in the News

Map #	Date	Machine	Place/Description
16	November 2004	ES&S Optical scan	**Taylor County, Wisconsin (Medford).** Four and a half months after the election, a consulting firm discovered that ES&S had programmed the optical scanners incorrectly, failing to account for partisan elections. All straight-party votes were lost, affecting approximately 27% of the ballots.[18] That failure meant that the votes of everyone who voted straight ticket - anyone who voted only for candidates of a single party - were not counted. In all, about 600 of 2,256 ballots cast were not counted, [Taylor County Clerk Bruce] Strama said. ... Medford and Taylor County officials have been told by Nebraska-based Election Systems & Software that the city will be reimbursed for the costs of setting up the vote-counting machine in the fall because the program was faulty. A spokeswoman said the company takes full responsibility for the error. ... "There's really nothing voters can do at this point," said Kevin Kennedy, the executive secretary of the State Elections Board.
17	November 2004	ES&S Optical scan	**Carroll County, Arkansas.** A mis-programmed chip from ES&S skewed the results from the JP District 2 race. [19] The glitch was discovered by Carroll County Election Commission members when they met to certify election results Monday at the Berryville courthouse. It is believed that the programming alignment was out of kilter, as provided by Election Systems and Software, the company that programs computer chips to read the local ballots. As a result, ballots for the JP District 2 race will either be hand counted, or re-run through the optical scanner machine once the correct computer chip is provided.

[18] **About 600 Medford ballots cast in November ignored.** Marshfield News-Herald. March 12, 2004. By Jake Rigdon. http://www.wisinfo.com/newsherald/mnhlocal/285285292773470.shtml

[19] **Computer glitch blamed for miscount in JP voting.** Carroll County Star Tribune. November 10, 1004. By Anna Mathews. Reproduced at http://www.votersunite.org/article.asp?id=3889

Vote-Switching Software Provided by Vendors — A Partial List Reported in the News

Map #	Date	Machine	Place/Description
18	August 2004	ES&S Unity Election Management System	**Natrona County, Wyoming.** The Unity Election Management System, used to tally votes from both optical scan machines and paperless electronic voting machines, failed to tally votes correctly. [20] Noticing that the totals for the city of Evansville seemed low, Natrona County Clerk Mary Ann Collins checked the printouts from the precinct voting machines in Evansville and found that the totals didn't match the totals computed by the Unity software, which combines all the totals countywide. The error changes the order in which some candidates finished, but does not affect which candidates will advance to the general election. Only one candidate lost votes but five of the 10 municipal races in the county had changed totals. ... Collins determined the software problem only affected nonpartisan races after checking the voting machine printouts and the absentee votes against the Unity software report in several partisan races. There does not appear to be any pattern in the skewed vote totals.
19	May 2004	ES&S Optical scanner (possibly Model 150)	**Craighead County, Arkansas.** The chip programmed by ES&S for the county's optical scanner gave one candidate all the votes for constable. A manual recount revealed the error. A recount was made in the District 13 constable race because returns from Precinct 20 showed one candidate received all 158 votes cast in the precinct, and the opposing candidate doubted that. The incident was traced back to a computer chip coding error, and the result of the recount was that both candidates had received votes in the precinct. [21]
20	March 2004	ES&S Optical Scan	**Lubbock County, Texas.**[22] The machines failed to count the votes for the Precinct 8 Democratic chairman race. Dorothy Kennedy, Lubbock County elections administrator said they would need to recount all the ballots for all races in the county. She said Omaha, Neb.-based ES&S, which prepared the vote tabulators, will foot the bill for the recount.

[20] **Clerk changes election vote totals.** August 21, 2004. By Matthew Van Dusen, Star-Tribune staff writer. http://www.casperstartribune.net/articles/2004/08/21/news/casper/6c2e825b3f9e154187256ef70007adbb.txt

[21] **Commission OKs results of elections.** Jonesboro Sun, May 28, 2004. By LeAnn Askins. http://www.jonesborosun.com/archivedstory.asp?ID=9486

[22] **Software blamed in Precinct 8 Democratic chair race mixup.** Lubbock online.com; March 11, 2004; By Brian Williams, Avalanche-Journal http://www.lubbockonline.com/stories/031104/loc_031104030.shtml

Vote-Switching Software Provided by Vendors — A Partial List Reported in the News

Map #	Date	Machine	Place/Description
21	April 2003	ES&S Model 100 optical scan	**Lake County, Illinois.** [23] Machines provided incorrect outcomes for 4 races in Lake County. The problem was caused by a programming error that failed to account for "no candidate" listings in some races on the ballot, Clerk Willard Helander said Thursday. As a result, election results were placed next to the names of the wrong candidates in four different races, including in Waukegan's 9th Ward. Incorrect results also were tabulated in races for the Libertyville Community High School District 128 Board, the North Chicago Community Unit District 187 Board and the Foss Park District Board in North Chicago. The clerk's office corrected the problem shortly after 10 p.m. on election night. But by then, many people who had kept track of the results on the clerk's online Web site believed the unofficial results were complete. ... Helander blamed the problem on Election Systems & Software, the Omaha company in charge of operating the county's optical-scan voting machines. She said a company official told her the programmers were unaware the county would have "no candidate" listings on its ballot.
22	November 2002	ES&S Optech 3P Eagle	**Baldwin County, Alabama.** Tabulation machine initially handed the gubernatorial election to the wrong candidate. Initial, unofficial results from Baldwin County showed that Democrat Don Siegelman garnered about 19,070 votes in the county, enough to give him a razor-thin victory over Republican challenger Bob Riley. The next morning, however, officials said those totals were inaccurate and certified returns giving Siegelman about 6,300 fewer votes -- enough to swing the election to Riley. ... Officials have traced the problem to a data pack from the Magnolia Springs voting location. They said the vote-counting machine there printed out accurate results when the polls closed at 7 p.m. But they said the cartridge, which resembles an eight-track cassette, gave bogus figures when it was plugged into the computer in Bay Minette. [24]

[23] **Returns are in: Software goofed — Lake County tally misled 15 hopefuls.** Chicago Tribune; April 4, 2003; By Susan Kuczka, Tribune staff reporter reproduced at http://www.vote.caltech.edu/mail-archives/votingtech/Apr-2003/0096.html

[24] **Voting snafu answers elusive.** The Mobile Register; 28 Jan 2003; by Brendan Kirby, staff writer. Referenced at http://www.votewatch.us/Members/Unregistered%20User/electionexperience.2004-08-12.9166974619. Confirmed by VotersUnite! with Sharon Jerkins in the Baldwin County Elections office, who provided the model number of the optical scan machines.

Vote-Switching Software Provided by Vendors — A Partial List Reported in the News

Map #	Date	Machine	Place/Description
23	November 2002	ES&S Optical scan	**Sarpy County, Nebraska.** The optical scan machines failed to tally "yes" votes on the Gretna school-bond issue, giving the false impression that the measure failed miserably. The measure actually passed by a 2-1 margin. Responsibility for the errors was attributed to ES&S, which provided the ballots and the machines. [25]
24	November 2002	Optech Eagle	**Wayne County, North Carolina.** A programming error caused the Optech Eagle optical scan machines to skip several thousand party-line votes, both Republican and Democrat. Correcting the error turned up 5,500 more votes and reversed the outcome for the House District 11 state representative race. [26]
25	November 2002	ES&S Optech 4C	**South Dakota.** When the optical scanner double counted votes, the error was blamed on a "flawed chip." ES&S sent a replacement chip, and voters demanded that the original chip be impounded and examined. Only ES&S was allowed to examine the chip. [27]
26	November 2002	ES&S Optech 3P	**Chatham County, North Carolina.** A ballot programming error caused Republican votes to go to the Libertarian candidate. [28] ... every time voters marked a straight Republican ticket, Frederick C. Blackburn, the N.C. House 54 Libertarian candidate, got a vote because of a voting machine programming error.
27	August 2002	ES&S Central count optical scan	**Clay County, Kansas.** The machine showed that the challenger (Jennings) had won, but a hand recount showed that the incumbent commissioner (Mayo) won by a landslide — 540 votes to 175. In one ward, which Mayo carried 242-78, the computer had mistakenly reversed the totals. [29] This statement indicates that the computer in the "one ward" had the candidates mis-mapped to the table that holds the voting results.

[25] **Omaha World-Herald,** 6 November 2002; "A late night in Sarpy; glitches delay results". Referenced in *Black Box Voting*, by Bev Harris. Chapter 2.

[26] **"Winners' may be losers."** The News and Observer; November 12, 2002; By Wade Rawlins and Rob Christensen.

[27] **NPR: Morning Edition,** 6 November 2002; "Analysis: Senate races in Minnesota and South Dakota" Referenced in *Black Box Voting* by Bev Harris, Chapter 2.

[28] **Mechanic to smooth vote.** New Observer. October 15, 2004. By Jessica Rocha, Staff Writer. http://newsobserver.com/news/story/1730333p-7996316c.html

[29] **Aug. 6 ballot problems alleged: Clay, Barton county candidates seek review of races.** Lawrence Journal-World. August 22, 2002. The Associated Press. http://www.ljworld.com/section/election02/story/103526

Vote-Switching Software Provided by Vendors — A Partial List Reported in the News

Map #	Date	Machine	Place/Description
28	April 2002	iVotronic and optical scanners	**Miami-Dade County, Florida.** In Medley, the software used to combine 45 absentee votes with the 309 electronic ballots changed the order of the candidates' names as it computed the results. The initial tally showed wins for two City Council candidates who actually lost the election. David Leahy, Miami-Dade **elections** supervisor said that all software had been tested before the election without a problem. Election workers who had been watching the results fed into the computer noticed the problem. **The tabulation computer didn't give any warning.** An ES&S technician had opened the ballot program on the memory cards to change a header. At the same time, he bumped the first candidate to the last position. When the technician saved the edit, a prompt most likely popped up on the monitor asking him if he was sure he wanted to change the order of the names. The technician ignored the prompt and confirmed the change. "It was something that should have been picked up and caught and was missed and was not flagged because the normal follow-up procedures to making a change in the database were not followed," [Mike] Limas [ESS Chief Operating Officer] said. ... Leahy said he is concerned because the computer did not raise any red flags, and humans had to spot the error. "If something is amiss you should get some type of error message, but there wasn't one," he said. ... In the future, Leahy said county election workers, not technicians from the equipment company, will program all the touch-screen and absentee ballot machines before an election to try to limit the possibility of error. He also suggested that humans might add up the absentee ballots with the touch-screen voting results to double check the computer's tally. [30]

[30] **Technician's Error, Not Machines, To Blame In Dade Election Mix-Up.** The Miami Herald. April 4, 2002. By Oscar Corral. [Purchase through Miami Herald online archives: http://www.miami.com/mld/miamiherald/archives/]

More Reports of Vote-Switching Software – Not Included on the Map Handout

Date	Machine	Place/Description
June 2006	ES&S Optical Scan (M-100)	**Pottawattamie County, Iowa.** Flawed ballot programming by ES&S reported results of all nine contested primary races incorrectly. [31] Pottawattamie County elections deputy Gary Herman said anomalies were noticed almost immediately. Electronic results were posted, but with a disclaimer that ballots would be hand-counted the next day. The results were dramatic. **Every winner in Pottawattamie County's nine contested races turned out, in retrospect, to be a loser.** Initial returns that showed incumbent Recorder John Sciortino losing by a margin of 1,245 votes to 1,167 was found to have actually won the election 2,061 votes to 347.
June 2006	ES&S Optical scan	**St. Francis County, Arkansas.** A recount of the State Senate District 16 runoff primary race reversed the initial, incorrect results caused by a ballot programming error.[32] Results in the Senate District 16 originally showed Representative Arnell Willis of Helena-West Helena defeating Earle School Superintendent Jack Crumbly by 28 votes. However, a recount in St. Francis County on Monday gave Crumbly 100 more votes, making him the winner. Election officials had said earlier that a tabulation error had resulted in 100 fewer votes being counted for Crumbly. St. Francis County Election Commission Chairman Frederick Freeman apologized to the candidates.
May 2006	ES&S Optical scan	**Phillips County, Arkansas.** Tabulators, with flawed ballot programming furnished by ES&S, mistook 432 Democratic votes for Republican and fail to count them in the Democratic primary. [33] Several days after the Election Commission certified that race and Crumbly and Willis began campaigning for the June 13 runoff, commission staff discovered that 432 votes cast at Allen Temple in Phillips County had mistakenly been counted as Republican ballots, effectively nullifying them. The malfunctioning ballot tabulating machine was programmed by Election Systems & Software, the Omaha, Neb.-based company that in November signed a $ 15 million contract to provide election equipment to Arkansas counties. Ballot programming problems in Phillips County also affected the House District 41 contest. [34]

[31] **Polk County recorder to contest election.** The Des Moines Register, June 24, 2006. Bert Dalmer, Register Staff Writer. http://desmoinesregister.com/apps/pbcs.dll/article?AID=/20060624/NEWS05/606240322/1001. Archive: http://www.votersunite.org/article.asp?id=6607

[32] **Recount In AR Race Reverses Result.** Eyewitness News. June 20, 2006. http://www.myeyewitnessnews.com/news/local/story.aspx?content_id=3734B371-B2D5-416C-9A72-D1AF88685953. Archive: http://www.votersunite.org/article.asp?id=6606

[33] **District 16 recount sought; 432 lost votes cited in suit.** Northwest Arkansas News Source, June 24, 2006. BY DANIEL NASAW. http://www.nwanews.com/adg/News/158589/. Archive: http://www.votersunite.org/article.asp?id=6605

More Reports of Vote-Switching Software – Not Included on the Map Handout

Date	Machine	Place/Description
November 2005	ES&S optical scanner	**Cumberland County, Pennsylvania.** Flawed ballot programming of straight-ticket votes hands the race to the wrong candidate for magisterial district judge. Straight-ticket Democrat votes were given to the Republican candidate. Straight-ticket Republican votes were not counted at all.[35] A 9.5-hour hand recount produced a new winner Thursday in the election for magisterial district judge for the Carlisle area. ...Democrat Jessica Rhoades came out on top by a slim two-vote margin — 1,703-1,701 — over Republican Kathy Keating in the recount. Initial vote totals recorded Tuesday night showed Keating won by a 1,650-1,468 margin. However, a programming error by the county's ES&S voting machines awarded all votes by Democrats casting a straight-ticket ballot to Keating. The problem involved a software coding error in which Keating's political affiliation was mislabeled as Democrat. Straight-ticket Republican votes were not awarded to either candidate. So the hand recount subtracted straight-ticket Democrat votes from Keating's total and added straight-ticket Republican votes. Meanwhile, Rhoades gained straight-ticket Democrat votes.

[34] **Vendor bender. City clerk blames ES&S for Election Day difficulties.** Times Record News. May 14, 2006. By Robert Morgan. http://www.votersunite.org/article.asp?id=6598

[35] **DJ race still up in the air.** Sentinel, November 11, 2005. By John Hilton. http://www.cumberlink.com/articles/2005/11/11/news/news02.txt Archive: http://www.votersunite.org/article.asp?id=6323

More Reports of Vote-Switching Software – Not Included on the Map Handout

Date	Machine	Place/Description
November 2004	Optical Scan	**Lancaster County, Nebraska.** As the optical scanners read the election-day ballots, occasionally, they added votes. While County Election Commissioner David Shively explained that the software was reading ballots twice, ES&S referred to the misread as a mechanical problem. [36] Inexplicably, both Shively and the Nebraska deputy secretary of state for elections, Neal Erickson, agreed that "the malfunctions were not the type that taint vote counts." The problem, described by Shively: While machines correctly fed themselves just one ballot at a time, their software at times incorrectly detected two ballots. The machines in all cases stopped short of actually counting two ballots, Shively said, and instead responded by shutting down. ... Shively said it became clear after 2 p.m. Tuesday that problems existed. At that time, officials began testing the six machines — four for election-day ballots, two on loan from Election Systems & Software to count absentee ballots — and found that two were not correctly matching results. That came as a surprise, Shively said, because all were tested late last week and performed well. After consulting with ES&S, Shively decided to use the two absentee-ballot machines to speed up the election-day counting. But the problem was apparently contagious. From about 10:30 p.m. to 12:30 a.m., the machines were purring along glitch-free, Shively said. "I thought, 'Boy, we're back in business,'" Shively said. **Then the two-ballot problem described by Shively began, plaguing almost all the machines,** drastically slowing the count.

[36] **Problem machines spur call for recount.** Lincoln Journal Star. November 14, 2004. By Nate Jenkins. http://www.journalstar.com/articles/2004/11/14/election/doc4189b9c7f14bf764391458.txt

More Reports of Vote-Switching Software – Not Included on the Map Handout

Date	Machine	Place/Description
November 2004	Optical Scan	**Sarpy County.** Election officials ended up with around 10,000 phantom votes (more votes than voters). They still don't know what went wrong. [37] Johnny Boykin lost his bid to be on the Papillion City Council. The difference between victory and defeat in the race was 127 votes. Boykin says, "When I went in to work the next day and saw that 3,342 people had shown up to vote in our war, I thought something's not right." He's right. There are not even 3,000 people registered to vote in his ward. For some reason, some votes were counted twice. Deputy Sarpy County Election Commissioner Ed Gilbert says, "It affected 32 of the 80 precincts. And I suppose as many as 10,000 votes." ... No one is sure exactly what went wrong. Astonishingly, election officials are projecting a winning candidate based on the assumption that the votes were counted twice and that the outcome wouldn't be affected. Election officials say they don't believe the glitch will impact who won and who lost any of the races. They figure that when votes were doubled in a particular race, the totals were doubled for both candidates. Vote totals would be skewed but percentages would not change. In spite of that, the candidates want to know the real numbers. VotersUnite contacted the Sarpy County Elections office and was told that ES&S had analyzed the problem and determined it to be "mechanical and procedural." That was all the election staff knew.

[37] **Countinghouse Blues: Too many votes.** WOWT Omaha. November 5, 2004. http://www.wowt.com/news/headlines/1161971.html

More Reports of Vote-Switching Software – Not Included on the Map Handout

Date	Machine	Place/Description
August 2004	Sequoia Veri-Vote	**Sacramento, California.** In a demonstration of its Direct Recording Electronic voting machine with a paper trail, Sequoia demonstrated that its machine failed to report four votes in Spanish.[38] Last week, Sequoia vice president and former California assistant secretary of state Alfie Charles was showing off the new Veri- Vote printer that his firm is supplying to Nevada when an astute legislative aide in Johnson's office noticed two votes were missing. Charles tried again to vote in Spanish with the same result: He cast votes on two mock ballot initiatives, but they were absent from the electronic summary screen and the paper trail. "The paper trail itself seemed to work fine but what it revealed was when he demonstrated voting in Spanish, the machine itself did not record his vote," Chesin said. "Programming errors can occur and the paper trail was the way we caught it."
May 2004	Optical scanner (possibly Model 150)	**Fulton County, Arkansas.** The chip programmed by ES&S for the county's optical scanner didn't work. ES&S claimed that the printer didn't send them all 16 ballots needed for the programming. The printer said he did send the entire set of ballots, and his records showed that the weight of the package mailed to ES&S was the weight of 16 ballots. [39] Riverside Graphics printer Michael Eaton insisted his company sent ESS [sic] a full set of ballots. "We printed the ballots for Independence County where there are three times as many people and we didn't have any problems. We've had this problem with ESS before," said Eaton. ... He said Riverside Graphics checked its postage records, and the weight of the package sent to ESS was consistent with a package containing 16 ballots.
May 2004	Model 150	**Sevier County, Arkansas.** The chip programmed by ES&S counted all ballots as blank. The test ballots were printed correctly, and the pre-election testing was successful. But then the ballots for election day were printed in a completely different print run, and the codes on these election-day ballots didn't match the codes on the computer chip prepared by ES&S. [40] After consulting with officials from Election Systems & Software, it was determined that the codes on the computer chip and the codes on the ballot didn't match.

[38] **Lawmakers cut e-voting's paper trail: Manufacturers demonstrating new printers in Nevada were embarrassed when machine failed to recognize votes.** Tri-Valley Herald. August 13, 2004. By Ian Hoffman, Staff Writer. Reproduced at: http://www.votersunite.org/article.asp?id=2512

Wrong Time for an E-Vote Glitch. Wired News. August 12, 2004. By Kim Zetter. http://www.wired.com/news/evote/0,2645,64569,00.html?tw=wn_tophead_2

[39] **No explanation for ballot machine malfunction.** South Missourian; May 27, 2004; by George Jared, Staff Writer

[40] **Ballots counted by hand in primary elections.** The DeQueen Bee; May 24, 2004. http://www.dequeen.com/news/comments.php?id=1188_0_1_0_C

More Reports of Vote-Switching Software – Not Included on the Map Handout

Date	Machine	Place/Description
March 2004	Unity Election Management Software	**Bexar County, Texas.** Misprogramming causes the Unity software to balk at accumulating votes from the optical scan machines used to count absentee ballots. [41] Tabulation of the Bexar County votes was delayed for about 1 1/2 hours, beginning about 8 p.m. ..."They have big problems," said Nick Peña, a poll watcher for District 28 U.S. Rep. Ciro Rodriguez, D-San Antonio. "They look very worried. "They have a bunch of technicians in the tabulation room, and they are pulling out wires and reattaching them, and the computer screens are all frozen. You can tell that something is happening," Peña said. ... Borofsky said the delay occurred after it was discovered the tabulation computers hadn't been properly programmed with updated data in order to count the mail-in paper ballots. The computer system then was taken off line and updated with the information needed to process the 3,000 paper ballots, which were tabulated using high-speed scanners.
March 2004	Diebold AccuVote optical scan	**San Diego, California.** Optical scan machines counted 208,446 ballots. The machines miscounted 2,821 votes in the Democratic presidential race and the Republican U.S. Senate seat. [42] Most of the absentee miscounts occurred in the Democratic presidential race, in which 2,747 votes cast for John Kerry were incorrectly credited to Rep. Dick Gephardt. In the Senate race, in which Bill Jones won, 68 votes cast for Barry L. Hatch were credited to candidate Tim Stoen, and six votes cast for James Stewart were credited to Stoen. [43]
November 2002	ES&S optical scan	**Scurry County, Texas.** A landslide victory for two commissioner candidates caused poll workers to question the results. The chip in the ES&S 650 contained an incorrect ballot program. ES&S sent a new chip, and the county officials also counted the votes by hand. The opposing candidates actually won by large margins.[44]

[41] **Bexar computer glitch delays counting of votes.** San Antonio Express News. March 10, 2004. Tom Bower. http://www.mysanantonio.com/news/metro/stories/MYSA10.12A.VotingProblems0310.4ea013d9.html

[42] **New electronic scanners miscounted some county votes.** NC Times April 7, 2004; By: Gig Conaughton - Staff Writer; http://www.nctimes.com/articles/2004/04/08/news/top_stories/22_27_394_7_04.txt

[43] **Some votes miscounted in primary, officials say.** Union-Tribune. April 8, 2004. By Luis Monteagudo Jr. and Helen Gao, staff writers. http://www.signonsandiego.com/news/politics/20040408-9999-1m8vote.html

[44] 06/03/04. Conversation with Scurry County Elections Director, who told VotersUnite it was an ES&S 650. She said it was the chip with the ballot programming on it, that they had to get a new one from ES&S. Original reference was from *Black Box Voting*, Chapter 2. Houston Chronicle, 8 November 2002; "Ballot glitches reverse two election results"

More Reports of Vote-Switching Software – Not Included on the Map Handout

Date	Machine	Place/Description
November 2002	Sequoia optical scan	**Taos, New Mexico.** A software programming error caused the Sequoia Optech optical scanner to assign votes to the wrong candidates. Just 25 votes separated the candidates in one race; another race had a 79-vote margin. After noticing that the computer was counting votes under the wrong names, Taos County Clerk Jeannette Rael contacted the programmer of the optical machine and was told it was a programming error.[45]
November 2002	Optical scan	**Adams County, Nebraska.** During the general election, Adams County was the last in Nebraska to have election results, due to both machine and software malfunctions. ES&S talked about some compensation for the election problems including paying for election worker overtime and not charging for **programming adjustments.** [46]
September 2002	Optical scan	**Union County, Florida.** [47] In Union County, Florida, a programming error caused machines to read 2,642 Democratic and Republican votes as entirely Republican in the September 2002 election. The vendor, ES&S, accepted responsibility for the programming error and paid for a hand recount.
September 2002	Optical scan	**Robeson County, North Carolina.** Ballot tabulating machines failed to work properly in 31 of 41 precincts. Local election officials said the problem was the result of a software glitch, and ballots had to be recounted. There had been a problem in the programming of the memory cards. [48]

[45] 06/03/04. Conversation with a woman at the Elections Division of New Mexico. She told me Taos used the Sequoia Optech and confirmed that it was a programming error by the local programmer. New Mexico does not have their ballot programming done by the vendor. Original reference from *Black Box Voting*, Chapter 2. Albuquerque Journal, 7 November 2002; "**Taos To Recount Absentee Ballots**"

[46] YorkNewsTimes.com, December 20, 2002; "**Omaha election systems firm to pay for county election problems**." Referenced in *Black Box Voting*, by Bev Harris. Chapter 2.

[47] **Black Box Voting** by Bev Harris, Chapter 2.

[48] January 2004 Conversation with Dinah in the Robeson County Clerk's office. Original reference was "Voter turnout surprises officials." Sun News. September 12, 2002. http://www.myrtlebeachonline.com/mld/sunnews/news/local/4056664.htm

More Reports of Vote-Switching Software – Not Included on the Map Handout

Date	Machine	Place/Description
April 2002	Optical Scan and iVotronic	**Dallas County, Texas.** A ballot programming error tallies 18 results incorrectly. Here is one case when flawed ballot data on a paperless electronic voting machine caused a serious election miscount. It was detected only because voters also used optical scan paper ballots in the election.[49] Mrs. Hawkins-Curtis, a candidate for Rowlett mayor was added to the ballot four days before the start of early voting. The change in the ballot definition wasn't programmed into all 390 ES&S iVotronic machines until after early voting began. The ballot data was changed only in Rowlett polling places. When the results were combined with the results from ES&S optical scan machines, the error caused the tally software to improperly tally results in the mayor's race as well as 17 other races, including propositions and school board races. Nearly 5,000 of the 18,000 ballots were improperly counted. An initial count didn't reveal a problem, and the results of all races were posted as final but "unofficial" on the Election Department's Web site at 10:17 p.m. Saturday. A few minutes later, a second count - called the reconciliation process - began to show that the number of voters who signed in at numerous precincts didn't match the vote totals, Ms. Pippins-Poole [county's assistant elections administrator] said. The extent of the miscount wasn't discovered until Monday when Election Systems & Software began a thorough investigation, Ms. Pippins-Poole said. ...The touch-screen ballots have been used in early voting in 91 elections since 1998 without any problems, Ms. Pippins-Poole said.

[49] **Glitch affects 18 races: Problems in counting early votes could alter some election outcomes.** Dallas Morning News. May 8, 2002. Ed Housewright, staff writer.

More Reports of Vote-Switching Software – Not Included on the Map Handout

Date	Machine	Place/Description
March 2002	AVC Edge	**Palm Beach County, Florida.** Former Boca Raton Emil Danciu was ahead by 17 points in a poll conducted by the opposition. Exit polling indicated an overwhelming win for Danciu, but he received only 19% of the votes, even losing in his home precinct. Voters report that their votes appeared to be registered for his opponent. "What really alarmed us was the next day when we started getting phone calls from voters who had gone into the voting places -- people we didn't even know -- and pushed Emil Danciu's name only to end up with a check mark by Susan Haynie's name. They repeatedly tried to vote for him, but another name, particularly Haynie's, came up. They couldn't get their vote registered. They were telling wild stories about poll workers unplugging and kicking the machines. They didn't know whether their votes ever counted. Some were told to vote again." [50] In addition, the results were delayed because, according to the election supervisor's office, 15 cartridges had been lost, and the system won't give a final tally until it has read all the cartridges. The office said that a poll worker had taken them home, and then they found them. With no paper ballots to check the accuracy of the machine, Danciu sued for the right to look at Sequoia source code. The county attorney argued that it would be a felony to disclose the source because it is a trade secret. The judge denied Danciu's request for the software code. [51]
November 2000	Diebold AccuVote OS	**Bernalillo County, New Mexico.** Flawed ballot programming for the presidential election caused 67,000 absentee and early-voting ballots to be counted incorrectly. The panicked officials first thought computerized tabulation machines or balloting software were at fault. The county uses the AccuVote optical scan system from Global Election Systems Inc. of McKinney, Texas. The tabulation system and software worked correctly, but a county technical employee failed to set up an element of the system properly, said Frank Kaplan, Global's Western regional manager. New Mexico's ballots are designed for voting by party, but voters can choose candidates from other parties. A programmer did not link the candidates' names to their respective parties.[52]

[50] **Out of Touch: You press the screen. The machine tells you that your vote has been counted. But how can you be sure?** New Times; April 24, 2003; By Wyatt Olson. http://www.newtimesbpb.com/issues/2003-04-24/feature.html/1/index.html

[51] **Electronic voting's hidden perils.** Mercury News. February 1, 2004. By Elise Ackerman. http://www.mercurynews.com/mld/mercurynews/news/special_packages/election2004/7849090.htm

[52] **Human error is cause of N.M. election glitch.** Government Computer News; November 20, 2000; Vol. 19 No. 33 http://www.gcn.com/vol19_no33/news/3307-1.html

More Reports of Vote-Switching Software – Not Included on the Map Handout

Date	Machine	Place/Description
November 1998	Votronic and Model 100	**Dallas, Texas** A software programming error caused Dallas County, Texas's new, $3.8 million high-tech ballot system to miss 41,015 votes during the November 1998 election. The system refused to count votes from 98 precincts, telling itself they had already been counted. Operators and election officials didn't realize they had a problem until after they'd released "final" totals that omitted nearly one in eight votes. The system vendor, ES&S, assured voters that votes were never lost, just uncounted. The company took responsibility and was trying to find two apparently unrelated software bugs, one that mistakenly indicated precinct votes were in when they weren't, and another that forgot to include 8,400 mail-in ballots in the final tally. Democrats were livid and suspicious, but Tom Eschberger of ES&S said, "What we had was a speed bump along the way."[53] After Nov. 3, Sherbet was quoted in the Dallas Morning News as saying, "In 17 years of doing this, there's been nothing more troublesome to me, more humiliating."[54]

[53] **Black Box Voting** by Bev Harris, Chapter 2.

[54] **Who Counts The Votes?** By Gary Ashwill and Chris Kromm. http://www.southernstudies.org/reports/votingmachines-new.htm

[The prepared statement of Mr. Feeney follows:]

PREPARED STATEMENT OF REPRESENTATIVE TOM FEENEY

Today's hearing continues our effort to ensure that every properly completed ballot is counted and fraud and error do not dilute legitimate votes. The adoption and implementation of technical standards for voting equipment ensure that the best technology and operational practices are applied to each election.

In order to achieve these goals, I have introduced H.R. 3910, the *Verifying the Outcome of Tomorrow's Elections (VOTE) Act.* As to voting equipment standards and guidelines, the VOTE Act requires that:

1. direct recording electronic systems also produce voter-verified paper records;
2. technical standards address the security of data electronically transmitted or received by voting systems; and
3. ballot tabulation equipment is regularly tested to ensure compliance to prescribed error rates.

However, technical standards are only one part of preserving the integrity of every vote. You can cast your vote on technically flawless equipment. But if ineligible voters also cast ballots or corrupt election officials oversee the process, your vote is cheapened.

Accordingly, the VOTE Act implements these security procedures:

1. each election official is subject to a criminal background check;
2. political party representatives can observe ballot tabulations; and
3. voters must present photo identification before casting a ballot.

Let's not delude ourselves into believing that technology by itself creates honest and fair elections. We should focus on preserving the integrity of the overall election system in which technology plays an important but not exclusive role.

[The prepared statement of Mr. Costello follows:]

PREPARED STATEMENT OF REPRESENTATIVE JERRY F. COSTELLO

Good afternoon. I want to thank the witnesses for appearing before our committee to review new federal voluntary standards for voting equipment which were issued late last year. Today's hearing serves as an opportunity to examine the accuracy and security of voting and to see if states are likely to adopt the Voluntary Voting Systems Guidelines (VVSG) standards.

In October, 2002, Congress enacted the *Help America Vote Act* (HAVA) to help address problems with voting machines that were brought to the public's attention during the 2000 federal election. HAVA established a number of basic requirements that voting machines and systems should meet and a process by which new voluntary technical standards would be developed to ensure the reliability and accuracy of new voting equipment.

Since HAVA's enactment, the states have received $2.9 billion to improve their election systems. In my home State of Illinois, it has received $143 million and has adopted the 2002 Federal Election Commission standards. Further, Illinois continues to work on the computerized state voter registration system to bring it into full compliance with the HAVA.

While I recognize the benefits of using electronic voting equipment to improve the accuracy of the ballot tallies, I believe we should proceed with caution. Reliability, efficiency, security, and usability concerns must be reviewed thoroughly to ensure electronic voting machines can be used by all registered voters and that election results are not compromised.

Further, consistent, nationwide data on the performance of voting systems would be useful to help improve technology and elections in the future. In the recent report completed by the Government Accountability Office (GAO) titled, *The Nation's Evolving Election System as Reflected in the November 2004 General Election,* it notes that the performance of the voting systems in the surveyed states was not consistently measured. I am interested to hear from our witnesses their comments on GAO's findings.

I look forward to hearing from the panel of witnesses.

[The prepared statement of Ms. Woolsey follows:]

PREPARED STATEMENT OF REPRESENTATIVE LYNN WOOLSEY

Mr. Speaker, I commend Chairman Boehlert and the Science Committee for holding this hearing today. The fairness and integrity of our federal elections is of paramount concern.

One need only look at the last two presidential elections to cite serious, well-documented concerns about disenfranchisement and voting rights violations without any Congressional investigation.

The U.S. is supposed to be a beacon of freedom. . .the greatest democracy in the world. . .yet we cannot seem to guarantee that the votes of our citizens are counted.

During the 2004 election we saw *it all*—from votes outnumbering voters in some precincts, to blatant voter intimidation in others. The time is long overdue for us to investigate these serious violations to our democracy and ensure that our voting machines are held to the highest standards possible.

And, there's also a tragic irony here: we're sacrificing thousands of American lives and billions of dollars to try to establish democracy in Iraq, yet we can't seem to get our own Democratic house in order.

This is not about which candidate won and which candidate lost on November 2, 2004. It's not about politicians at all; it's about citizens and their most fundamental rights.

We *must* ensure that any and all future elections are unmarred by fraud or even human error. A solution to this problem is not pie-in-the-sky—it *can be solved.* It's time this Congress stepped up to the plate and did something about it.

[The prepared statement of Ms. Hooley follows:]

PREPARED STATEMENT OF REPRESENTATIVE DARLENE HOOLEY

Thank you Chairman Boehlert and Chairman Ehlers for holding this hearing today on this vitally important issue.

The ability to vote, and the knowledge that your vote will be counted, is a right that every American knows is guaranteed to them by the Constitution.

As technology has improved, our ability to make sure that every vote is counted has been improved.

The election of 2000 demonstrated flaws within the system and gave us in Congress the opportunity to revise the standards for voting in this country and allow us to make better use of computers and other forms of technology to assist us in the goal of counting every vote. Now we have a chance to review the standards that were put into place as part of the *Help America Vote Act,* see what has worked and what needs to be improved.

One issue that I know my constituents in Oregon, and our fellow citizens across the country, care about is that of ballot security. Numerous reports have been released by computer science experts that detail specific security flaws in electronic voting systems. These reports have been criticized by the voting system vendors and by some elections officials as offering unlikely and alarmist scenarios. These people have correctly pointed out that, to date, there is no evidence that an electronic voting system has been hacked. I am glad that we are going to have the opportunity today to hear from experts about the possible security threats to these voting machines and I look forward to hearing their testimony.

One simple fix that I support is the use of an independent paper record to ensure that elections officials can audit election results, spot-check for accuracy, and recount should electronic results be lost or compromised.

My state is unique in the country in that we only have vote-by-mail and, as such, are guaranteed to have a paper trail that election officials can refer to if the need arises. It is not difficult to recognize the wisdom of having a paper trail to make sure that votes are being recorded and counted. Any action that can be taken by election officials to reassure citizens that their votes are being counted is one that I believe needs to be taken.

The final issue that I want to highlight is the difficulty that our senior citizens may have with these new voting machines. In an average election, around 70 percent of our nation's seniors vote and some of them have limited experience with computers or other electronic devices.

In addition, many of the precinct workers who man the polls on Election Day and may be called upon to offer technical assistance if one of these voting machines crashes may lack proper training. How do we know that these people are able to handle not just mis-voting and voter assistance, but also machine malfunction?

I look forward to hearing from the witnesses today and I am thankful to the Chairman and Ranking Members of the Science and House Administration Committees for holding this hearing and giving us all the opportunity to review voting

guidelines. The American people need to feel secure in their belief that when they cast a vote, it will be recorded and counted.

I am confident that we will do everything that we can assure our fellow Americans that their belief is well-founded and that their votes are secure.

[The prepared statement of Ms. Jackson Lee follows:]

PREPARED STATEMENT OF REPRESENTATIVE SHEILA JACKSON LEE

Mr. Chairman, thank you for holding this crucial hearing today, in which once again, we find how important science is not only to our economy and technological expertise around the world, but to our ability to protect and defend the most basic American civil rights. Now that voting standards have been promulgated, it is time to focus on their accuracy, reliability, and effectiveness.

Under the authority of the *Help America Vote Act of 2002,* the Election Assistance Commission was created to oversee and spearhead standards for voting equipment, and produce voluntary voting system guidelines for states to follow. Clearly, this was in response to the voting process disaster in 2000 election.

So far, the Election Assistance Commission has experienced significant delays and funding problems, resulting in only limited changes to the original Federal Election Commission standards. These new changes have been met with criticism because of 1) the undue burden it places on manufacturers of voting machines, 2) the fact that the standards are not comprehensive, 3) the fact that paper trails were not addressed, and 4) that conformance tests were not developed.

Just last month, the GAO published a report documenting the difficulties that states have with voter information databases, such as the surge of last minute voter registrations, inaccurate information on registration materials, and the varied means of counting the votes between states.

In addition, a report from the Brennan Center at the New York University School of Law highlighted problems in the verification process of registered voters. For example, one existing database in Florida contained as many as 40 misspellings of the word "Fort Lauderdale." If the voter-verification system in place relies on data matching, this would clearly obstruct an individual's ability to vote.

It is inexcusable that there should ever be barriers that prevent U.S. citizens from performing their civic duties. Just last week, we reauthorized the *Voting Rights Act,* thereby reaffirming our social and political commitment to civil rights. Today, we address the technological and procedural problems that remain in delivering these civil rights to every American.

It is shameful that in 2006, the 21st century, we are lacking in procedures to ensure open and fair elections. There must be a paper trail on every electronic voting machine. We experienced the failures of a paperless voting system in the 2000 and 2004 election. A voting machine without electronic paper trail is a voting machine doomed for fraud. Any standard must ensure that the minority vote is counted, and that discrepancies are thoroughly reviewed. America should be ashamed of itself, and the fact that it denies the opportunity to have elections reviewed transparently, legitimately, and credibly.

The problems that exist in voting machine and voting process standards are complex, and yet resolvable. I look forward to the testimony today to illustrate the evidence and the direction in which we should pursue legislative recourse, if necessary.

Thank you, Mr. Chairman, and I yield the balance of my time.

Chairman EHLERS. At this time, I would like to introduce our witnesses. We have an excellent panel. We thank you very much for coming here.

First, we have Ms. Donetta Davidson, Commissioner of the Election Assistance Commission, and the member of the commission, six-member commission. She is the member who is the techie, as you might call it. At least, you pay the most attention to it. Dr. William Jeffrey, a fellow physicist, Director of the National Institute of Standards and Technology, and chair of the Technical Guidelines Development Committee.

Next, I recognize the Member of this committee, the gentleman from Minnesota, Mr. Gutknecht, to introduce our third witness. Mr. Gutknecht is recognized.

Mr. GUTKNECHT. Thank you, Mr. Chairman.

I am pleased to announce, or to introduce Secretary Mary Kiffmeyer from Minnesota. Mary and her husband Ralph have been dear friends of mine for 25 years. She is Minnesota's twentieth Secretary of State. She was first elected in 1998, and was reelected in 2002. She is also the former President of the National Association of Secretaries of State, and she has been very active in the Election Assistance Commission Standards Board. Mary takes her job extremely seriously, and I don't know of anybody in elected office who works harder than Mary Kiffmeyer.

Minnesota has a reputation for clean elections, and she has done her level best to make certain that we maintain that reputation. So, Mary, we are delighted to have you here today, and I am honored to call you my friend, and even more honored to call you our Secretary of State.

Chairman EHLERS. Thank you, and we are pleased to have you here, and Minnesota is a good state. It is my birthplace.

Next, Ms. Linda Lamone, Administrator of Elections, the Maryland State Board of Elections. Mr. John Groh, Chairman, Election Technology Council, Information Technology Association of America. And Dr. David Wagner, Professor of Computer Science, University of California at Berkeley, the finest public university in this country. I just happened to have graduated from there.

Chairman BOEHLERT. Mr. Chairman, are we going to have all these commercials all day?

Chairman EHLERS. Thank you for yielding the chair to me. I am enjoying doing this.

As our witnesses should know, spoken testimony is limited to five minutes each, after which, the Members will each have five minutes to ask questions. And we are pleased to start by hearing the testimony of Ms. Davidson.

STATEMENT OF MS. DONETTA L. DAVIDSON, COMMISSIONER, ELECTION ASSISTANCE COMMISSION

Ms. DAVIDSON. Good afternoon. Chairmen, Ranking Members, and Committee Members of both committees. My name is Donetta Davidson, and I am with the Election Assistance Commission.

As a result of the *Help America Vote Act,* about one-third of our voters will be voting on new equipment in 2006. HAVA established minimum requirements that all voting systems must meet. The law also mandated that EAC adopt Voluntary Voting System Guidelines. The TGDC delivered guidelines within the nine months, and at that time, prior to our adoption, we held three public meetings, received and reviewed over 6,500 comments, and had a very transparent process.

The states have always been the decision-makers when it comes to making the decision on what equipment they are goint to use. HAVA did not change that, as some have stated. The VVSG was an initial update to the 2002 Voting System Standards that was in place. We focused mainly on security, usability, accessibility, and created a usability section, address the needs of all voters, and empowers election officials to adjust voting systems to improve interaction.

The EAC and NIST are already working on future iterations—software, forms of independent verification, security, comprehen-

sive test suites, the mean time between failure rate, and detailed threat analysis for voting systems are being addressed. HAVA mandates that the EAC also certify voting systems against new guidelines. The EAC has just adopted the first phase of the program for testing and certifying of voting systems.

The program will be more rigorous, transparent, and thorough than ever before. We will have to remember that voting systems are only half of the equation though. Voting is a human exercise. We must focus on protecting the integrity of the whole process, just not the machine. The bottom line is the voting equipment, whether it is paper or electronic, is only as good as the operator.

Attempts to compromise a voting system requires two things—access and knowledge of the voting system. That is why election officials must adopt management guidelines to make sure that we protect the process all the way. Speaking of training, the EAC has already developed a Quick Start Guide that we have here today for everybody. That will give the individuals and the states ideas, and make sure that they follow procedures to make sure that they address everything in a new voting system.

The larger part, we will be issuing election management guidelines that will cover the following topics: security protocol, all phases, setup, storage, transportation, election day, post-election, archiving, logic and accuracy testing, tabulation, training of employees and poll workers. As a former Secretary of State, I could tell you that regardless of what kind of voting equipment is in place, some things never change. Controlling access, having enough people to work in the polls, and making sure those people are well-trained, testing the equipment, and putting contingency plans into place are the highest priority.

Voting systems and people are not mutually exclusive. We must keep that in mind as we move forward, to make sure that the next generation of voting equipment is secure, accurate, and reliable.

Thank you, and I would be happy to answer any questions at this time.

[The prepared statement of Ms. Davidson follows:]

PREPARED STATEMENT OF DONETTA L. DAVIDSON

Good morning Chairmen Ehlers and Boehlert and Members of the Committees. I am pleased to be here this afternoon on behalf of the U.S. Election Assistance Commission (EAC) to discuss the changes in voting that have been effectuated by the *Help America Vote Act of 2002* (HAVA) and the role that EAC plays in supporting the states and local governments in implementing HAVA-compliant voting systems.

INTRODUCTION

EAC is a bipartisan commission consisting of four members: Paul DeGregorio, Chairman; Ray Martinez III, Vice Chairman; Donetta Davidson; and Gracia Hillman. EAC's mission is to guide, assist, and direct the effective administration of federal elections through funding, innovation, guidance, information and regulation. In doing so, EAC has focused on fulfilling its obligations under HAVA and the *National Voter Registration Act* (NVRA). EAC has employed four strategic objectives to meet these statutory requirements: Distribution and Management of HAVA Funds, Aiding in the Improvement of Voting Systems, National Clearinghouse of Election Information, and Guidance and Information to the States. Each program will be discussed more fully below. The topic at hand involves our strategic efforts to aid in the improvement of voting systems.

AIDING IN THE IMPROVEMENT OF VOTING SYSTEMS

One of the most enduring effects of HAVA will be the change in voting systems used throughout the country. All major HAVA funding programs can be used by states to replace outdated voting equipment. HAVA established minimum requirements for voting systems used in federal elections. Each voting system must:

- Permit the voter to verify the selections made prior to casting the ballot;
- Permit the voter to change a selection prior to casting the ballot;
- Notify the voter when an over-vote occurs (making more than the permissible number of selections in a single contest);
- Notify the voter of the ramifications of an over-vote;
- Produce a permanent paper record that can be used in a recount or audit of an election;
- Provide accessibility to voters with disabilities;
- Provide foreign language accessibility in jurisdictions covered by Section 203 of the Voting Rights Act; and
- Meet the error rate standard established in the 2002 Voting System Standards.

According to HAVA, the requirement for access for voters with disabilities can be satisfied by having one accessible voting machine in each polling place. In addition to these requirements, Congress provided an incentive for states that were using punch card or lever voting systems by providing additional funding on a per precinct basis to replace those outdated systems with a voting system that complies with the requirements set out above.

HAVA also provides for the development and maintenance of testable standards against which voting systems can be evaluated. It further requires federal certification according to these standards. EAC is responsible for and committed to improving voting systems through these vital programs.

Voluntary Voting System Guidelines

One of EAC's most important mandates is the testing, certification, decertification and recertification of voting system hardware and software. Fundamental to implementing this key function is the development of updated voting system guidelines, which prescribe the technical requirements for voting system performance and identify testing protocols to determine how well systems meet these requirements. EAC along with its federal advisory committee, the Technical Guidelines Development Committee (TGDC), and the National Institute of Standards and Technology (NIST), work together to research and develop voluntary testing standards.

On December 13, 2005, EAC adopted the first iteration of the *Voluntary Voting System Guidelines (VVSG).* The final adoption of the VVSG capped off nine months of diligent work by NIST and the TGDC. In May of 2005, the TGDC delivered its draft of the VVSG. EAC then engaged in a comprehensive comment gathering process, which included comments from the general public as well as from members of its Board of Advisors and Standards Board. Interested persons were able to submit comments on-line through an interactive web-based program, via mail or fax, and at three public hearings (New York, NY; Pasedena, CA; Denver, CO). EAC received more than 6,000 individual comments. EAC teamed up with NIST to assess and consider every one of the comments, many of which were incorporated into the final version.

The VVSG is an initial update to the 2002 Voting System Standards focusing primarily on improving the standards for accessibility, usability and security. The 2005 VVSG significantly enhances the measures that must be taken to make voting systems accessible to persons with disabilities and more usable for all voters. For example, the 2002 VSS contained 29 accessibility requirements, focusing primarily on accommodating persons with visual disabilities. The 2005 VVSG contains 120 requirements that establish testing measures to assure that voting systems accommodate all persons with disabilities, including physical and manual dexterity disabilities. In addition to ensuring accessibility requirements were increased and strengthened, the 2005 VVSG includes for the first time a usability section, which addresses the needs of all voters, empowering them to adjust voting systems to improve interaction. Those testing measures include allowing adjustment of brightness, contrast, and volume by the voter to suit his/her needs.

The 2005 VVSG also incorporated standards for reviewing voting systems equipped with voter-verifiable paper audit trails (VVPAT)[1] in recognition of the many states that now require this technology. In accordance with HAVA and to assure that persons with disabilities had the same access to review their ballots as non-disabled voters, the 2005 VVSG required VVPATs to be accessible when the paper record would be used as the official ballot or as definitive evidence in a recount. In addition, the VVSG addressed new technologies that emerged on the market since the 2002 VSS, such as wireless technology. Standards were established to require the wireless mechanism to be disabled during voting and to provide a clear, visual indicator showing when the wireless capability is activated. VVSG also establishes testing methods for assessing whether a voting system meets the guidelines. A complete listing of the changes and enhancements included in the 2005 VVSG can be found on the EAC web site, *http://www.eac.gov/Summary%20of%20Changes%20to%20VVSG.pdf*.

The 2005 VVSG, like the 1990 and 2002 VSS, is a voluntary set of voting system testing standards. States choose to make these standards mandatory for equipment purchased in those states by requiring national certification according to those standards in their statutes and/or rules and regulations. Currently, approximately 40 states require certification to either the 2005 VVSG or the 1990 or 2002 VSS. When EAC adopted the 2005 VVSG, it did so with an effective date of December 13, 2007. This two-year period was designed to allow states the time needed to make changes to their laws, rules and regulations to require certification to the new standards, as is standard practice when introducing new industry guidelines. New York has already legislatively mandated certification to the 2005 VVSG, and EAC expects over the next several years that the vast majority of the states will make changes to their legislation requiring certification to the 2005 VVSG. Prior to December 13, 2007, voting systems, components, upgrades and modifications can be tested against either the 2002 VSS or the 2005 VVSG, depending on the requirements of the states and manufacturers' requests. After December 13, 2007, EAC will no longer test systems to the 2002 VSS; systems and upgrades will only be tested to the 2005 VVSG.

Significant work remains to be done to fully develop a comprehensive set of standards and testing methods for assessing voting systems and to ensure that they keep pace with technological advances. In FY 2007, EAC along with TGDC and NIST, will revise sections of the VVSG dealing with software, functional requirements, independent verification, and security and will develop a comprehensive set of test suites or methods that can be used by testing laboratories to review any piece of voting equipment on the market. Much like the roll out of the 2005 VVSG, these future iterations will be adopted with an effective date provision and a procedure for when new voting systems, components, upgrades and modifications will be required to be tested against the new iteration of the VVSG.

Accreditation of Voting System Testing Laboratories

HAVA Section 231 requires EAC and NIST to develop a national program for accrediting voting system testing laboratories. NIST's National Voluntary Laboratory Accreditation Program (NVLAP) will initially screen and evaluate testing laboratories and will perform periodic reevaluation to verify that the labs continue to meet the accreditation criteria. When NVLAP has determined that a lab is competent to test systems, the NIST director will recommend to EAC that a lab be accredited. EAC will then make the determination to accredit the lab. EAC will issue an accreditation certificate to the approved labs, maintain a register of accredited labs and post this information on its web site to fully inform the public about this important process.

In June 2005, NVLAP advertised for the first class of testing laboratories to be reviewed under the NVLAP program and accredited by EAC. Three applications were received in the initial phase, with two additional applications following in late 2005. Pre-assessments of these laboratories began in April 2006 and formal review is proceeding. NVLAP will conduct full evaluations of at least two initial applicants this fall and, depending on the outcome of the evaluations, will make initial recommendations to the EAC before the end of the year. All qualified candidates from among the pool of five applicants will be sent to the EAC by spring 2007.

In late 2005, EAC invited laboratories that were accredited through the National Association of State Election Directors (NASED) program as Independent Testing

[1] VVPAT is an independent verification method that allows the voter to review his/her selections prior to casting his/her ballot through the use of a paper print out. VVPAT is merely one form of independent verification. EAC is currently working with NIST to develop standards for additional methods such as witness systems, cryptographic systems, and split process systems.

Authorities (ITAs) to apply for interim accreditation to avoid a disruption or delay in the testing process. All three ITAs have applied for interim accreditation. Interim accreditation reviews by EAC contractors are under way and are expected to be completed by September 2006. ITAs will be accredited on an interim basis until the first class of laboratories is accredited through the NVLAP process. After that time, all testing labs must be accredited through the NVLAP evaluation process.

The National Voting System Certification Program

In 2006, EAC is assuming the duty as prescribed by HAVA to certify voting systems according to national testing standards. Previously, NASED qualified voting systems to both the 1990 and 2002 Voting System Standards. Historically, voting system qualification has been a labor intensive process to ensure the integrity and reliability of voting system hardware, software and related components. In six months, NASED received 38 separate voting system test reports for review and qualification. All requests were received, processed and monitored while the testing laboratory assessed compliance. Once a test report was produced, technical reviewers analyzed the reports prior to certification.

EAC's certification process will constitute the Federal Government's first efforts to standardize the voting system industry. EAC's program will encompass an expanded review of voting systems, and it will utilize testing laboratories accredited by EAC and experts hired by EAC to assure that the tested systems adequately met the standards.

The EAC will implement the Testing and Certification Program required by Section 231(a)(1) of HAVA in two distinct phases (pre-election phase and full program). Both phases will be rolled out in 2006. The first phase of the program will begin on July 24, 2006 and terminate upon the EAC's implementation of the program's second phase. The second phase (full program) will begin on December 7, 2006.

The pre-election phase of the program focuses on providing manufacturers a means to obtain federal certification for modifications required by state and local election officials administering the 2006 General Election. This pre-election phase will ensure a smooth and seamless transition from the NASED program (which has qualified voting systems at the national level for more than a decade) to the more rigorous and detailed EAC program. This will be done by delaying implementation of some the procedural requirements found in the full program until after the critical pre-election period. This will allow the EAC to diligently review voting system modifications while, at the same time, ensuring a smooth transition and avoiding the unacceptable delays often associated with rolling out a new program.

The full program will begin in December by requiring every voting system manufacturer that desires to have a product certified to register and disclose information about the company and its owners, board members and decision-makers. Manufacturers will be subject to a conflict of interest analysis including reviewing whether any owners or board members are barred from doing business in the United States. EAC will test complete voting systems including new components and how they integrate with the entire voting system. This process will be achieved by having technical experts review the reports provided by accredited testing laboratories to assure that the tests performed and the results are consistent with a system that conforms to the VVSG. These experts will recommend conforming systems for certification. Another new feature of the EAC certification program will be the quality assurance program. Through site visits to manufacturing facilities and field inspections, EAC will confirm that the systems that are being manufactured, sold to and used by election jurisdictions throughout the country are the same as those certified by EAC. Last, EAC will introduce a decertification process that will allow involved persons to file complaints of non-conformance, provide for the investigation of those complaints, and if warranted decertify systems because of a failure to conform to the VVSG.

Election Management Guidelines

To complement the VVSG, the EAC is creating a set of election management guidelines. These guidelines are being developed by a group of experienced state and local election officials who provide subject matter expertise. The project will focus on developing procedures related to the use of voting equipment and procedures for all other aspects of the election administration process. The election management guidelines will be available to all election officials if they wish to incorporate these procedures at the State and local levels. These guidelines cover the following topics:

- Storage of equipment
- Equipment set up
- Acceptance testing

- Procurement
- Use
- Logic and accuracy (validation) testing
- Tabulation
- Security protocols (all phases—storage, set up, transport and Election Day)
- Training of employees/poll workers
- Education for voters

The first of these management guidelines was issued by EAC in June 2006 in the form of a *Quick Start Guide* for election officials. This guide focused on the issues and challenges faced by election officials as they accept and implement new voting systems. The guide gave tips to the election officials on how to avoid common pitfalls associated with bringing new voting systems on line.

2006: A YEAR OF CHANGE, CHALLENGE AND PROGRESS

The federal elections in 2006 have and will mark a significant change in the administration of elections. In compliance with HAVA, states have purchased and implemented new voting systems. There is a strong shift to electronic voting, although optical scan voting is still popular. In addition, states have imposed new requirements on their voting systems, and they have implemented their own testing programs for voting systems they purchase. And, in at least 25 states, voter-verified paper audit trails (VVPAT) have been required for all electronic voting. Due to the introduction of new voting systems throughout the Nation, the voter's experience at the polls will be quite different in 2006 than it was in 2000. It is estimated that one in three voters will use different voting equipment to cast their ballots in 2006 than in 2004.

Voters with disabilities will likely experience the most dramatic changes. For the first time, every polling place must be equipped with voting machines that allow them to vote privately and independently. For many voters with disabilities, this may be the first time that they will cast ballots without the assistance of another person.

Voting systems do not represent the only changes in election administration that will be apparent in 2006. States have also developed statewide voter registration lists, which will provide the ability to verify voters' identity by comparing information with other State and federal databases. This will result in cleaner voter registration lists and fewer opportunities for fraud. Another anticipated benefit of the statewide lists will be a significantly reduced need for provisional ballots, as was the case in states that had statewide voter registration lists in 2004.

This year is one of transition, which is difficult to overcome in any business; elections are no different. The introduction of new equipment will present some challenges and hurdles to overcome. For State and local governments, there are also a host of new obligations. They must receive and test a fleet of new voting equipment. Training for staff and poll workers must be organized and conducted. And, extensive education programs must be implemented to inform the public about the new voting equipment.

Although EAC cannot be on the ground in every jurisdiction to lend a hand in these tasks, we have issued a *Quick Start Guide* to assist election officials as they implement new voting systems. We also encourage states to take proactive measures to test their voting systems and voter registration lists prior to the federal elections. Such activities have proven to be an excellent tool to identify problems and solutions prior to the stresses and unpredictability of a live election.

CONCLUSION

Over the past four years, significant changes have been made to our election administration system. New voting systems have been purchased and implemented. Each state has adopted a single list of registered voters to better identify those persons who are eligible to vote. Provisional voting has been applied across all 50 states, the District of Columbia and four territories. However, one thing has not changed. Elections are a human function. There are people involved at every level of the election process, from creating the ballots, to training the poll workers, to casting the votes.

With these changes will come unexpected situations, even mistakes. We cannot anticipate in a process that involves so many people that it will work flawlessly the first time. What we can embrace, however, is that the process has been irrevocably changed for the better. There is a heightened awareness of the electoral process in the general public. There have been significant improvements to the election administration process. And, more people have the ability to vote now than ever before.

Messrs. Chairmen, thank you for the opportunity to address the Committees today. I will be happy to answer any questions that you may have.

BIOGRAPHY FOR DONETTA L. DAVIDSON

Ms. Donetta L. Davidson was nominated by President George W. Bush and confirmed by unanimous consent of the United States Senate on July 28, 2005 to serve on the U.S. Election Assistance Commission (EAC). Her term of service extends through December 12, 2007. Ms. Davidson, formerly Colorado's Secretary of State, comes to EAC with experience in almost every area of election administration—everything from County Clerk to Secretary of State.

Ms. Davidson began her career in election administration when she was elected in 1978 as the Bent County Clerk and Recorder in Las Animas, Colorado, a position she held until 1986. Later that year, she was appointed Director of Elections for the Colorado Department of State, where she supervised county clerks in all election matters and assisted with recall issues for municipal, special district and school district elections.

In 1994, she was elected Arapahoe County Clerk and Recorder and re-elected to a second term in 1998. The next year, Colorado Governor Bill Owens appointed Davidson as the Colorado Secretary of State, and she was elected to in 2000 and re-elected in 2002 for a four-year term.

She has served on the Federal Election Commission Advisory Panel and the Board of Directors of the Help America Vote Foundation. In 2005, Ms. Davidson was elected President of the National Association of Secretaries of State, and she is the former President of the National Association of State Elections Directors (NASED). Prior to her EAC appointment, Ms. Davidson served on EAC's Technical Guidelines Development Committee (TGDC).

In 2005, *Government Technology* magazine named Ms. Davidson one of its "Top 25: Dreamers, Doers, and Drivers" in recognition of her innovative approach to improve government services. She was also the 1993 recipient of the Henry Toll Fellowship of Council of State Governments.

Davidson has devoted much of her professional life to election administration, but her first love is her family. Ms. Davidson was born into a military family in Liberal, Kansas and became a Coloradoan shortly thereafter when her family moved first to Two Buttes, then to Las Animas where they settled. Whenever possible Ms. Davidson spends time with her family, son Todd, daughter and son-in-law Trudie and Todd Berich, and granddaughters Brittany and Nicole.

Chairman EHLERS. And thank you very much for staying well below the five minute limit. Dr. Jeffrey.

STATEMENT OF DR. WILLIAM JEFFREY, DIRECTOR, NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

Dr. JEFFREY. Chairmen, Ranking Members, and Members of the Committee, thank you for the opportunity to testify today on "Voting Machines: Will the New Standards and Guidelines Help Prevent Future Problems?"

I am William Jeffrey, Director of the National Institute of Standards and Technology, and I am pleased to be offered this opportunity to participate in today's discussion.

NIST works closely with the Election Assistance Commission, by providing technical support directly to them and to the Technical Guidelines Development Committee, or TGDC. NIST is pleased to be working on this matter of national importance with our EAC and TGDC partners.

Today, I will focus on NIST's role in meeting the requirements of the *Help America Vote Act of 2002,* including development of voluntary guidelines for voting systems and laboratory accreditation.

HAVA assigned three major responsibilities to NIST. First, develop a report to assess areas of human factors research, and to ensure the usability and accuracy of voting systems. Second, chair and provide technical support to the TGDC. And third, recommend

testing laboratories to the EAC for accreditation. We believe that we have met or are on track to meeting these three responsibilities.

First, in January 2004, NIST completed the report, which assessed areas of human factors research. The recommendations from this report are being addressed in the Voting System Guidelines to ensure the usability and accuracy of voting systems.

Second, NIST is chairing and providing technical support to the TGDC, which is developing new voluntary voting system guidelines for consideration by the EAC. HAVA mandated that the first set of recommendations be delivered to the EAC nine months after the formal creation of the TGDC. To meet this incredibly aggressive schedule, NIST and the TGDC conducted workshops, meetings, and numerous teleconferences to gather input, pass resolutions, and review and approve NIST-authored materials. This was done in a fully transparent process, with meetings conducted in public, and draft materials available on the Web. The resulting document was delivered on schedule to the EAC in May of 2005.

These new guidelines are built upon the strengths of the previous Voting System Standards, enhancing areas needing improvement, and adding new material. The new material focuses primarily on usability, accessibility, and security. The new section on security includes the first federal standard for voter-verified paper audit trails. The new voluntary guidelines takes no position regarding the implementation of such paper audit trails, and neither requires nor endorses them. If states choose to implement the voter-verified paper audit trails, the new voluntary guidelines provide requirements that will help to ensure that their systems are usable, accessible, reliable, and secure. The new security section also contains requirements for addressing voter systems software distribution, validation of software used on Election Day, and wireless communications.

Immediately after completing its work on the '05 guidelines, NIST and the TGDC began work on the next version, currently planned for delivery to the EAC in July of 2007. The '07 voluntary guidelines will build upon the '05 version, but takes a fresh look at many of the requirements. The '07 guidelines will review every section of the current standard, and will consider inclusion of additional requirements, as identified by the TGDC.

NIST is aware that in addition to the '07 voluntary guidelines, an open test suite needs to be developed, so that the requirements in the new standard can be tested uniformly and consistently by all of the testing labs. The test suite development is planned to begin in Fiscal Year 2007.

The third task that NIST is given under HAVA is recommending testing laboratories to the EAC for accreditation. Simply stated, laboratory accreditation is formal recognition that a laboratory is competent to carry out specific tests. NIST is using its National Voluntary Laboratory Accreditation Program to accomplish this task. Thus far, we have received applications from five labs, and are working to submit the qualified labs to the EAC for accreditation in early 2007.

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

[The prepared statement of Dr. Jeffrey follows:]

PREPARED STATEMENT OF WILLIAM JEFFREY

Introduction

Chairmen Ehlers and Boehlert, Ranking Members Millender-McDonald and Gordon, and Members of the Committees, thank you for the opportunity to testify today on "The Status of Voluntary Voting System Guidelines." I am William Jeffrey, Director of the National Institute of Standards and Technology (NIST), part of the Technology Administration of the Department of Commerce. I am pleased to be offered the opportunity to add to this discussion regarding standards development for voting systems.

I will focus my testimony on NIST's role in meeting the requirements of the *Help America Vote Act of 2002,* specifically in providing technical expertise towards the development of voluntary guidelines for voting systems and providing assistance to the Election Assistance Commission (EAC) with respect to voting system testing laboratories. I will discuss NIST's role in producing the Voluntary Voting System Guidelines (VVSG) of 2005 and then discuss our current and future work, which is to produce a next iteration of the VVSG that is more precise and testable and to produce associated test suites for this redesigned VVSG. Lastly, I will discuss the status of our work in assessing potential voting system testing laboratories and recommending them to the EAC for accreditation.

HAVA

I will begin by giving a brief review of the *Help America Vote Act* (HAVA) of 2002 with respect to NIST's role. HAVA provided for the creation of the Technical Guidelines Development Committee (TGDC) and mandated that the TGDC provide its first set of recommendations to the Election Assistance Commission (EAC) not later than nine months after all of its members have been appointed.

HAVA assigned three major items to NIST. First, NIST was tasked with the development of a report to assess the areas of human factors research, which could be applied to voting products and systems design to ensure the usability and accuracy of voting products and systems. Second, NIST was tasked with chairing and providing technical support to the TGDC, in areas including (a) the security of computers, computer networks, and computer data storage used in voting systems, (b) methods to detect and prevent fraud, (c) the protection of voter privacy, and (d) the role of human factors in the design and application of voting systems, including assistive technologies for individuals with disabilities and varying levels of literacy. Third, NIST is to conduct an evaluation of independent, non-federal laboratories and to submit to the EAC a list of those laboratories that NIST proposes to be accredited to carry out the testing.

The first major item assigned by HAVA was the production of a human factors report. This report, titled *"Improving the Usability and Accessibility of Voting Systems and Products,"* was completed by NIST in January 2004. It assesses human factors issues related to the process of a voter casting a ballot as he or she intends. The report recommends developing a set of performance-based usability standards for voting systems. Performance-based standards address results rather than equipment design. Such standards would leave voting machine vendors free to develop a variety of innovative products and not be limited by current or older technologies. The EAC delivered this report to Congress on April 30, 2004.

Second, HAVA assigned NIST to provide technical support to the TGDC in the development of voluntary voting system guidelines. The TGDC provides technical direction to NIST in the form of TGDC resolutions, and it reviews and approves proposed guidelines and research material written by NIST researchers. The TGDC ultimately is responsible for approving the guidelines and submitting them to the EAC.

These voluntary guidelines contain requirements for vendors when developing voting systems and for laboratories when testing whether the systems conform to, or meet, the requirements of the guidelines. Voluntary standards or guidelines are common in industry. Voluntary standards encourage the adoption of requirements and procedures without the enforcement of regulation or law. The marketplace—in this case, the states and the public—provides the impetus for software developers to implement and conform to the standard.

2005 VVSG

I will now discuss NIST's role in producing the 2005 VVSG for the EAC. HAVA mandated that the first set of recommendations be written and delivered to the EAC nine months after the final creation of the TGDC. To meet this very aggressive schedule, the TGDC organized into three subcommittees addressing the following areas of voting standards: core requirements and testing, human factors and pri-

vacy, and security and transparency. Over nine months, NIST and the TGDC conducted workshops, meetings, and numerous teleconferences to gather input, pass resolutions, and review and approve NIST-authored material. This was done in a fully transparent process, with meetings conducted in public and draft materials available over the web. The resulting document, now known as the VVSG 2005, was delivered on schedule to the EAC in May 2005.

The VVSG 2005 built upon the strengths of the previous Voting Systems Standards and enhanced areas needing improvement and added new material. The new material adds more formalism and precision to the requirements using constructs and language commonly used in rigorous, well-specified standards. This includes rules for determining conformance to the standard and a glossary for clarifying terms, which is very important when one considers that each voting jurisdiction may define terms differently.

The new material focuses primarily on usability, accessibility, and security. The usability section includes requirements on voting system controls, displays, font sizes, lighting, and response times. It also requires voting systems to alert voters who make errors such as over-voting so as to reduce the overall number of spoiled ballots. The accessibility section is greatly expanded from the previous material and includes requirements for voters with limited vision and other disabilities. It also addresses the privacy of voters who require assistive technology or alternative languages on ballots.

The new section on security includes the first federal standard for Voter Verified Paper Audit Trails (VVPAT). As you know, many states require that their voting systems include a voter-verified paper trail. The VVSG takes no position regarding the implementation of VVPAT and neither requires nor endorses them. If states choose to implement VVPAT, the VVSG's requirements help to ensure that their VVPAT systems are usable, accessible, reliable and secure, and that the paper record is useful to election officials for audits of voting equipment.

The new security section also contains requirements for addressing how voting system software is to be distributed. This will help to ensure that states and localities receive the tested and certified voting system. Moreover, the section also includes requirements for validating the voting system setup. This will enable inspection of the voting system software after it has been loaded onto the voting system—again to ensure that the software running on the voting system is indeed the tested and certified software. Lastly, there are requirements governing how wireless communications are to be secured. The TGDC concluded that, for now, the use of wireless technology introduces severe risk and should be approached with extreme caution. Wireless communications are currently permitted in the VVSG if security measures and contingency procedures are in effect.

The TGDC-approved version of the VVSG 2005 was sent to the EAC in May 2005. Following that, the EAC conducted a 90-day public review and received thousands of comments; NIST provided technical assistance to the EAC in addressing these comments. The EAC published its version of the VVSG on December 13, 2005. This version included changes to the TGDC-approved version, reflecting the EAC's additional review.

2007 VVSG

Immediately after completing its work on the VVSG 2005, NIST and the TGDC began work on what is now called the VVSG 2007, currently planned for delivery to the EAC in July 2007.

The VVSG 2007 builds upon the VVSG 2005 but takes a fresh look at many of the requirements. It will be a larger, more comprehensive standard, with more thorough treatments of security areas and requirements for equipment integrity and reliability. The TGDC will consider updated requirements for accessibility and requirements for usability based on performance benchmarks. They will also consider updated requirements for documentation and data to be provided to testing labs, and for testing laboratory reports on voting equipment. The requirements will be structured so as to improve their clarity to vendors and their testability by testing labs.

The VVSG 2005 included a discussion of voting systems with Independent Verification (IV). IV means that the voting systems produce a second record of votes for ballot record accuracy and integrity. For VVSG 2007, the TGDC will update this discussion for consideration as new requirements. The TGDC will also consider a number of updated requirements dealing with voting equipment integrity and reliability.

NIST is aware that, in addition to the VVSG 2007, an open test suite needs to be developed so that the requirements in the VVSG 2007 can be tested uniformly and consistently by all of the testing labs. The development of a test suite is a major

undertaking and once complete, will add significantly to the trust and confidence that voting systems are not only being tested correctly, but are robust, secure and work correctly. Test suite development is planned to begin in fiscal year 2007.

Laboratory Accreditation

I will conclude my remarks with the status of NIST's third major item under HAVA, laboratory accreditation. NIST has been directed to recommend testing laboratories to the EAC for accreditation. In order to accomplish this, NIST is utilizing its National Voluntary Laboratory Accreditation Program (NVLAP). NVLAP is a well-established laboratory accreditation program that is recognized both nationally and internationally.

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 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.

Laboratories seeking accreditation to test voting system hardware and software are required to meet the ISO/IEC 17025 criteria and to demonstrate technical competence in testing voting systems. To ensure continued compliance, all NVLAP-accredited voting system testing laboratories will undergo periodic assessments to evaluate their ongoing compliance with specific accreditation criteria.

NVLAP has received applications thus far from five laboratories. We are conducting on-site visits and examining their qualifications to test voting systems and be granted NVLAP accreditation. NVLAP is working to submit the qualified labs from the five applications to the EAC for accreditation in early 2007.

Conclusion

NIST is pleased to be working on this matter of national importance with our EAC and TGDC partners. NIST has a long history of writing voluntary standards and guidelines and developing test suites to help ensure compliance to these standards and guidelines. NIST is using its expertise to work with our partners to produce precise, testable voting system guidelines and tests that will reduce voting system errors and increase voter confidence, usability, and accessibility.

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

BIOGRAPHY FOR WILLIAM JEFFREY

William Jeffrey is the 13th Director of the National Institute of Standards and Technology (NIST), sworn into the office on July 26, 2005. He was nominated by President Bush on May 25, 2005, and confirmed by the U.S. Senate on July 22, 2005.

As Director of NIST, Dr. Jeffrey oversees an array of programs that promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve quality of life. Operating in fiscal year 2006 on a budget of about $930 million, NIST is headquartered in Gaithersburg, Md., and has additional laboratories in Boulder, Colo. NIST also jointly operates research organizations in three locations, which support world-class physics, cutting-edge biotechnology, and environmental research. NIST employs about 2,800 scientists, engineers, technicians, and support personnel. An agency of the U.S. Commerce Department's Technology Administration, NIST has extensive cooperative research programs with industry, academia, and other government agencies. Its staff is augmented by about 1,600 visiting researchers.

Dr. Jeffrey has been involved in federal science and technology programs and policy since 1988. Previous to his appointment to NIST he served as Senior Director for Homeland and National Security and the Assistant Director for Space and Aeronautics at the Office of Science and Technology Policy (OSTP) within the Executive Office of the President. Earlier, he was the Deputy Director for the Advanced Technology Office and chief scientist for the Tactical Technology Office with the Defense Advanced Research Projects Agency (DARPA). While at DARPA, Dr. Jeffrey advanced research programs in communications, computer network security, novel sensor development, and space operations.

Prior to joining DARPA, Dr. Jeffrey was the Assistant Deputy for Technology at the Defense Airborne Reconnaissance Office, where he supervised sensor development for the Predator and Global Hawk Unmanned Aerial Vehicles and the development of common standards that allow for cross-service and cross-agency transfer of imagery and intelligence products. He also spent several years working at the Institute for Defense Analyses performing technical analyses in support of the Department of Defense.

Dr. Jeffrey received his Ph.D. in astronomy from Harvard University and his B.Sc. in physics from the Massachusetts Institute of Technology.

Chairman EHLERS. Thank you for your testimony. Next, we recognize Ms. Kiffmeyer.

STATEMENT OF MS. MARY KIFFMEYER, SECRETARY OF STATE FOR MINNESOTA

Ms. KIFFMEYER. Chairman Ehlers and Chairman Boehlert and Members, thank you for the opportunity to address the U.S. House of Representatives Committees on House Administration and Committee on Science. The opportunity to inform the Committees of the needs of the states regarding *"Voting Machines: Will the New Standards and Guidelines Help Prevent Future Problems?"* is very important to me, and to other election officials in other states.

Minnesota has long been a leader in elections in this country. We have led the Nation in voter turnout for several years, including the important 18- to 24-year-olds, but one reason for that high involvement is that Minnesotans have demanded that elections meet the highest standards of accuracy, access, integrity, and privacy. So, the implementation of HAVA has only helped to assist in this process.

In the implementation of HAVA in Minnesota, access and privacy are being greatly increased through the use of disability accessible voting equipment. In the process of evaluating potential equipment, accuracy and integrity were deemed important objectives, along with the 2005 VVSG. In addition, the Secretary of State and all major parties came to the conclusion that Minnesota should hold to a long-established requirement of paper ballots for elections.

To what extent are these guidelines being used for Minnesota and why? Minnesota chose to use the 2005 Voluntary Voting System Guidelines in order to be in line with the best information we could get on election systems. In 2005, the State of Minnesota published a request for proposal for the statewide purchase of HAVA-compliant voting equipment, both assistive and vote tabulating equipment. In preparation of the RFP, the 2005 VVSG were used to establish accessibility and usability requirements for the assistive voting equipment, and the RFP required that all equipment purchased under the contract comply with the 2005 VVSG.

At the time the RFP was published, the 2005 VVSG were not yet adopted. Therefore, the final contract required that the voting equipment vendor would be responsible for bringing the systems into compliance with the VVSG upon final adoption by the EAC.

The Minnesota State Plan also called for the state to make grants to counties from HAVA funds for the purchase of this equipment. Counties were required to prepare plans that they would purchase with this grant funds. Many counties already had voting tabulating equipment. However, it was learned that the vendor would not be upgrading the older equipment to the 2005 VVSG.

Consequently, the state made the choice to permit the use of grant funds to replace this older equipment, with the intent to bring all voting equipment in the state up to the 2005 VVSG standards.

Finally, due to security concerns raised during the comment period for the adoption of the 2005 VVSG, it was decided in the interests of Minnesota voters who shared these concerns for security, that Minnesota would only permit the use of paper ballots in its elections. Therefore, statutes were amended in the 2006 legislative session, implementing this strict paper ballot requirement.

Are the VVSG comprehensive enough, in the 2005 guidelines, to guide purchasing decisions? No, the security standards of the 2005 VVSG are not sufficiently comprehensive to ensure security in our election systems. The use of technology for voting increases the risk that security of the voting system will be breached if proper safeguards are not taken.

I believe that more comprehensive treatment in two areas alone would increase confidence in the electronic voting systems. First is the use of wireless components. Because of concerns with wireless components in the polling place, wireless components should only be turned on after the polls close and voting is complete, or strict security guidelines are developed.

Also, to provide for maximum trust in election systems in the United States, I believe that a voter-verified paper audit trail should be highly considered required in the VVSG. In Minnesota, I am pleased to say we have the ultimate voter-verified paper trail, the actual ballots that the voters have marked. This standard will help provide assurance that the elections process is being conducted in an accurate and fair manner. I believe that voters should be able to verify their votes in complete confidence that they are counted as cast, and that a VVPAT is necessary for purposes of a recount, and that of an audit trail.

The current VVSG is good, for as far as it goes, but it needs to be evaluated after the next election, to see how the equipment functioned, and what would be better. Any necessary modifications need to be made with an emphasis on software changes and hardware security changes first. The cost of implementing new hardware could be a burden on the taxpayers, and should be avoided if at all possible.

So, what do these TGDC need to do to make it more likely that states will update the equipment? Time is an issue. The next effective date is too close for election administrators to both evaluate the current system and propose improvements. Through study of the effectiveness and the conduct of elections, we will be able to have more information to make the improvements necessary in the next versions. Caution should be given to large capital expenditures that would waste today's money.

Human factors are extremely important, and I have sufficient testimony as well that is written today that I could submit, seeing my time has concluded.

Thank you very much for the opportunity to testify today.

[The prepared statement of Ms. Kiffmeyer follows:]

PREPARED STATEMENT OF MARY KIFFMEYER

Chairman Ehlers and Chairman Boehlert and Members, thank you for the opportunity to address the U.S. House of Representatives Committees on House Administration and Committee on Science. The opportunity to inform the committees of the needs of the states regarding *"Voting Machines: Will the New Standards and Guidelines Help Prevent Future Problems?"* is very important to me and to other election officials in other states. Minnesota has long been a leader in elections in this country.

Minnesotans have led the Nation in voter turnout for several years now including the important 18- to 24-year-old segment of the voting population. One reason for high involvement is that Minnesotans have demanded that elections meet the highest standards of accuracy, access, integrity, and privacy. So, the implementation of HAVA has only helped to assist in this process.

In the implementation of HAVA in Minnesota, access and privacy are being greatly increased through the use of disability-accessible voting equipment. In the process of evaluating potential equipment, accuracy and integrity were deemed important objectives, along with the 2005 VVSG. In addition, the Secretary of State and all major parties came to the conclusion that Minnesota should hold to a long-established requirement of paper ballots for elections.

Q. To what extent are the 2005 Voluntary Voting Systems Guidelines (VVSG) being used by Minnesota and why? If Minnesota is not adopting to the 2005 VVSG, what standards are you using for voting equipment purchasing decisions and operation, and why did you select these standards?

A. Minnesota chose to use the 2005 Voluntary Voting Systems Guidelines in order to be in line with the best information we could get on election systems. In 2005, the State of Minnesota published a Request for Proposals (RFP) for the statewide purchase of HAVA-compliant voting equipment, both assistive-voting equipment and vote-tabulating equipment. In preparation of the RFP, the 2005 Voluntary Voting System Guidelines (VVSG) were used to establish accessibility and usability requirements for the assistive voting equipment and the RFP required that all equipment purchased under the contract comply with the 2005 VVSG. At the time the RFP was published, the 2005 Voluntary Voting System Guidelines had not yet been adopted. Therefore, the final contract required that the voting equipment vendor would be responsible for bringing the systems into compliance with the Voluntary Voting System Guidelines upon final adoption by the EAC.

The Minnesota State Plan called for the state to make grants to counties from HAVA funds for the purchase of this equipment. Counties were required to prepare plans for the voting equipment they would purchase with these grant funds. Many counties already had vote-tabulating equipment; however, it was learned that the vendor would not be upgrading the older equipment to 2005 VVSG standards. Consequently, the state made the choice to permit the use of grant funds to replace this older equipment with the intent to bring all voting equipment in the state up to the 2005 VVSG standards.

Finally, due to security concerns raised during the comment period for the adoption of the 2005 VVSG standards, it was decided, in the interest of Minnesota voters who shared these concerns for security, that Minnesota would only permit the use of paper ballots in its elections. Therefore, statutes were amended in the 2006 legislative session implementing this strict paper ballot requirement.

Q. Are the 2005 VVSG comprehensive enough to guide states' voting equipment purchasing decisions and voting systems operation during elections? If so, why, and if not, why not?

A. No, the security standards of the 2005 VVSG are not sufficiently comprehensive to ensure security in our election systems. The use of technology for voting increases the risk that security of the voting system will be breached, if proper safeguards are not taken. More comprehensive treatment in two areas alone would increase confidence in electronic voting systems. First is the use of wireless components. Because of concerns with wireless components in the polling place, wireless components should only be turned on after the polls close and voting is complete or strict security guidelines are developed. Also, to provide for maximal trust in election systems in the United States, I believe that a voter-verified paper audit trail should be highly considered required in the VVSG. (In Minnesota, I am pleased to say, we have the ultimate voter-verified paper trail: the actual ballots that voters have marked.) This will help provide assurance that the elections process is being conducted in an accurate and fair manner. I believe that voters should be able to verify

their votes in complete confidence that their votes are counted as cast. And a VVPAT is necessary for purposes of a recount and that of an audit trail.

The current VVSG is good for as far as it goes, but it needs to be evaluated after the next election to see how the equipment functioned and what would be better. Any necessary modifications need to be made with an emphasis on software changes and hardware security changes first. The cost of implementing new hardware could be a burden on the taxpayers and should be avoided if at all possible.

Q. What do the Elections Assistance Commission and Technical Guidelines Development Committee (TGDC) need to do to make it more likely that states will update equipment using the latest VVSG? Do the 2005 VVSG need to be changed or improved in any way to make them more useful to the states? If so, what changes or additional information would you recommend for the VVSG? If not, why not?

A. Time is an issue. The next effective date is too close for election administration to both evaluate the current system and propose improvements. Thorough study of the effectiveness of the equipment in the conduct of elections must be evaluated. After that study ideas and suggestions must be given regarding the improvement of the election process. This takes time and the current timeframe is much too short.

In addition, caution should be given to large capital expenditures to replace equipment. If at all possible software changes and upgrades that would improve the process would be preferred and allow the hardware changes to take affect later in order to make maximum use of current expenditures by the Federal Government, states and local jurisdictions.

Q. How important are human factors, such as those described in the National Institute of Standards and Technology (NIST) 2004 report "Improving the Usability and Accessibility of Voting Systems and Products," *in your selection of voting equipment? Is this report, together with the 2005 VVSG, having an impact on voting systems and elections, and if so, how? If not, why not?*

A. Human factors were extremely important in the development of voting equipment requirements for the State of Minnesota. In the early stages of HAVA, our state worked closely with the disability community to seek their advice as to the human factors in their voting experience. We considered them the experts.

When it was decided that the state would be acquiring new voting equipment, one of the first actions taken was to form a diverse group of citizens to assist the Secretary of State in defining the requirements for voting systems to be used in Minnesota. A Voting Equipment Proposal Advisory Committee (VEPAC) was established for this purpose. This group included members with different disabilities for their input on accessibility and usability, local election administrators, and citizens motivated to improve the election process in the state. This committee researched the election equipment study reports, including the report, "Improving the Usability and Accessibility of Voting Systems and Products," and made recommendations to the Secretary of State that were incorporated into the final equipment requirements of the state voting equipment contract. Members of the committee then helped score RFPs and select equipment. Accessibility and usability of the equipment eventually chosen was of the greatest importance in its ultimate selection in addition to the critical base requirements of security, accuracy and integrity.

Thank you for the opportunity to testify before your committees and your willingness to hear from those who administer elections in the states. I would like to reemphasize that no matter what modifications may be made to the VVSG, it must incorporate the need for access, accuracy, integrity, and privacy. And for the best use of funds already invested both now and in the future, please give the needed time for evaluation of the current situation of the election systems prior to implementation of new standards.

Chairman EHLERS. And thank you very much. Ms. Lamone.

STATEMENT OF MS. LINDA H. LAMONE, ADMINISTRATOR OF ELECTIONS, MARYLAND STATE BOARD OF ELECTIONS

Ms. LAMONE. Chairmen, Members of the Committee, I am a lawyer by training, not a physicist, but I will try to overcome that deficiency.

Chairman EHLERS. We would appreciate that.

Ms. LAMONE. One of the things I think everyone needs to remember when we are talking about the issue that is before the Com-

mittee today, that the voting process is really a four-pronged, and a very large enterprise.

Not only do you have the voting equipment in place, and that seems to be the focus of a lot of people, but you also have to have an examination of the processes that surround the election, the security, which is a huge issue in Maryland, and of course, all the people.

And one of the things that concerns me about some of the dialogue that is occurring around the country, not necessarily here, is that we tend to lose focus on the huge number of absolutely wonderful people that we have working in elections across the country, from people like me, I am not that wonderful, but people like, in my position, down to my employees, the county people, the town people, and most importantly, the poll workers. And they are a very important prong to this process, and we need to make sure that they feel like they are a part of it, and a welcome part of it.

The other part of this whole thing, of course, is also the voters. What are we doing to make sure that they feel confident that we are doing our job well, and not trying to undermine their confidence, which I think a lot of the discussion is tending to do.

You have heard from three of my distinguished colleagues about some of the issues with the guidelines. I think one of the most important things we need to remember is that this is an evolution. It is not a simple step to improve the process. In Maryland, we started, in 2001, with the General Assembly of Maryland passing a law requiring a uniform statewide voting system, and it has taken me until this year to fully implement law, with Baltimore City becoming the last jurisdiction. So, in the fall of this year, every voter in Maryland will be voting on touchscreen voting.

The amount of money that it has taken me and the State of Maryland to implement that decision of the General Assembly is huge. Not only do I have over $50 million invested in the voting system, I have many, many more millions invested in security procedures, security processes, that we necessarily have to take to ensure the integrity of this voting system.

If, for some reason, the existing system that we have in Maryland is not compliant with any future guidelines issued by, through the cooperation of NIST and the EAC, will the taxpayers of my state be willing to spend another $50 million on voting systems? Now, I suggest to you that that is going to be a very tough decision on the part of my governor and my General Assembly. So, that is something that we all have to keep in the back of our minds when we are talking about this. And a lot of the other states are going to be in the same position. Georgia has a statewide system. They use the same system that I do, and a lot of the counties are out there purchasing, or have purchased for this upcoming fall elections, because they had to, under the *Help America Vote Act.*

I would just like, and I know it is going to come up, so I might as well hit it right on the head, the verified paper trail has, for me, two main issues. One, it is going to stifle, and it already has, to some extent, the development of any other kind of independent verification technologies. I have seen some things out there that are still prototypes that I would love to see go onto the market, be-

cause they would provide me with all kinds of wonderful tools, as well as providing a way to audit and verify the election.

The other thing that has me greatly concerned about it is its impact on the disabled voters, particularly those with vision problems or blind voters. They have no way of verifying in privacy what that piece of paper said, and it seems to me that one of the major thrusts of the *Help America Vote Act* was to assist this huge population of people, who either can't read, don't know how, or can't read because they can't see.

I think in this debate, we need to keep them in our minds, because we certainly have done everything we can in Maryland to reach out to this population.

[The prepared statement of Ms. Lamone follows:]

PREPARED STATEMENT OF LINDA H. LAMONE

Thank you for the opportunity to address the Committee on House Administration and the Committee on Science on the impact of the voting systems guidelines adopted by the U.S. Election Assistance Commission in December 2005. As the Chief Election Official in Maryland and an active member of the National Association of State Election Directors, federal voting system standards have historically provided state and local election officials with a level of assurance that a voting system accurately counts and records votes and meets the minimum performance and testing standards. The 2005 Voluntary Voting Systems Guidelines (VVSG) enhance the prior voting system standards and, by raising the minimum standards, will provide greater assurances to election officials, candidates, and the voting public.

Application of Federal Voting Systems Standards in Maryland

Under section 9–102 of the Election Law Article of the *Annotated Code of Maryland,* a voting system in Maryland cannot be State certified unless an approved independent testing authority has tested the voting system and shows that it meets the performance and test standards for electronic voting systems. Although Maryland's law does not require that a voting system meet a *specific* version of the standards, the current language enables the State of Maryland to have voting systems tested against the most recent standards without having to amend the statute each time the standards are revised.

The State of Maryland began its implementation of a statewide, uniform voting system in 2002. The request for proposals required that "all equipment and software proposed must comply with the Federal Election Commission's voting system standards regarding DRE and optical scan equipment."[1] Since Maryland's voting system was procured and implemented in twenty-three of twenty-four jurisdictions before the voluntary voting system standards were released for comment, the voting system met the current standards at the time—the 1990 and later the 2002 standards.

As section 9–102 of the Election Law Article includes the VVSG and any subsequent revisions, no additional steps are necessary for the State to adopt these guidelines. Once the independent testing authorities begin testing against the VVSG, future software versions of the State's uniform voting system will be tested against these guidelines.

Impact of 2005 Standards on Purchasing & Operational Decisions

As every jurisdiction should know that the VVSG are the only federal standard against which voting systems will be tested starting December 2007, the ability of a voting system to meet the VVSG should be a critical factor for a jurisdiction selecting a voting system. With at least forty-seven states requiring local jurisdictions to comply with federal standards and guidance, the majority of states recognize the importance of federal standards and guidance.[2] That being said, I suggest to you that whether the VVSG are "comprehensive enough" is not a factor guiding voting system purchasing decisions (although it may be factor in determining whether ad-

[1] See Section 2.1, Request for Proposals: Direct Recording Electronic Voting System and Optical Scan Absentee Voting System for Four Counties, Project No. SBE–2002.01, *www.elections.state.md.us/pdf/procurement/rfp.pdf.*

[2] "States and the District of Columbia Reported Requirements for Local Jurisdictions to Use Federal Standards for Voting Systems," Appendix X, *The Nation's Evolving Election System as Reflected in the November 2004 General Election,* GAO–06–450, June 2006.

ditional testing is required); the paramount inquiry is whether the voting system *meets* the guidelines.

Improve Likelihood of States to Accept VVSG

It is my opinion that the VVSG will become *de facto* mandatory for several reasons. First, the majority of states require compliance with federal guidelines. These states laws may already require compliance with new guidelines once they become effective.

Second, jurisdictions using old voting systems (i.e., punch card voting system and mechanical lever machines) can no longer use those systems if they accepted federal funds under the *Help America Vote Act of 2002.* As vendors will not likely risk losing potential clients by selling voting systems that do not meet the VVSG, they will most likely only be offering voting systems that meet the VVSG. As a result, the majority, if not all, of voting equipment on the market for the 2008 elections will most likely meet the VVSG.

Third, according to the U.S. Election Assistance Commission, voting systems will no longer be tested against prior versions of the guidelines once the VVSG are in effect. Once testing against prior guidelines ends, new voting systems and upgrades to existing systems will need to meet the VVSG or risk not being certified. With no other guidelines against which to test, there will no longer be different standards of certification (i.e., meets 2002 standards but not VVSG, etc.)

Lastly, the political pressure against purchasing or using a system that does not meet the guidelines will be high. With the litigious nature of advocacy groups, it will be difficult for jurisdictions to justify selecting and using a voting system that does not meet the guidelines.

Although I believe that most states will accept the VVSG, there is one additional enhancement to the guidelines that could provide an additional incentive. In addition to certification by the U.S. Election Assistance Commission, many states have a state certification process. To the extent that the VVSG could be revised to include state-specific certification requirements, state election officials could accept the certification by the U.S. Election Assistance Commission as the basis of state certification. This joint certification would reduce the resources needed to conduct state certification without a reduction in confidence in the voting system.

Human Factors & Voting Systems

Under Maryland law, a system's "ease of understanding for the voter" and "accessibility for all voters with disabilities recognized by the *Americans with Disabilities Act"* are required considerations for State certification of a voting system.[3] Although usability of voting systems generally gets lost in the on-going debate about voting systems, the ability of a voter to understand how to vote is equally important as the security of a voting system.

The new usability guidelines in the VVSG are an important addition. The new requirements and the expected usability guidelines in the next version of the VVSG, coupled with recent studies by the National Institute of Standards and Technology (NIST) and other academics, will only enhance the usability of voting systems.[4] Although Maryland's voting system vendor has incorporated findings of prior usability studies into its voting systems, I expect that greatest impact of these requirements and studies will be in future voting systems and software upgrades.

Conclusion

It is important to consider the VVSG as a long-term strategy to improve voting systems in the United States. These guidelines cannot be viewed as a panacea with an immediate and dramatic impact on elections; their impact will be gradual and will not be known for several election cycles.

Voting system vendors need time to make the required software and hardware changes to their products. Similarly, independent testing authorities need time to develop the necessary performance and test guidelines to use during testing. Although the guidelines are referred to as the "2005 VVSG," the U.S. Election Assistance Commission recognized that the infrastructure would need to develop before the VVSG could be effective. For this reason, the Commission made the guidelines effective in December 2007. For these reasons, the first elections when voting systems tested against the VVSG would most likely be used are the 2010 elections.

Equally important, State and local jurisdictions typically consider voting systems as long-term investments. Maryland, for example, has projected a fifteen-year life

[3] *See* § 9–102(d)(6) and (10), Election Law Article, *Annotated Code of Maryland.*

[4] See Herrnson et al., A Project to Assess Voting Technology and Ballot Design, *www.capc.umd.edu/rpts/VoteTechFull.pdf.*

cycle for its current voting system. When the VVSG become effective, some jurisdictions might be faced with the following choice—either scrap a voting system that does not meet the VVSG or procure a voting system that does. Although federal funding offset some of the expenses associated with purchasing and implementing a new voting system, it cannot cover all of the on-going maintenance costs or costs of a new system.

Also, the involvement of the NIST in the election arena is new. NIST's leadership of the Technical Guidelines Development Committee has been critical in updating the voting system standards, and its establishment of the National Voluntary Laboratory Accreditation Program will impact future testing against the standards. As their role has just begun and continues to evolve, it is important to allow NIST to put into place standards and procedures to impact voting system certification.

In conclusion, I would like to compare the process of improving voting systems to the process of improving air quality. When the U.S. Congress enacts a law to limit air pollution, the date by which the affected industry must comply is often ten years down the road. This delayed effective date allows the industry to evaluate options, develop technologies that will enable them to comply with the mandates, and implement the necessary changes to the industry's infrastructure.

I believe this is how voting system technology should be viewed. In the meantime, however, the VVSG are a good first step, but they must be viewed as the first step of many. Like cleaning our air, improving voting systems takes time, and I caution you not to expect overnight changes to voting systems.

BIOGRAPHY FOR LINDA H. LAMONE

Linda H. Lamone was appointed by the Governor to be the State Administrator of Elections on July 1, 1997. As the State Election Administrator, Ms. Lamone, by statute, has been charged with maximizing the use of technology in election administration. Since her appointment, Ms. Lamone is overseeing the second development and implementation of a statewide voter registration system and a mandate for a uniform statewide voting system. Additionally, Ms. Lamone has administered the development of a sophisticated candidate and campaign finance management program and an election management system that creates and certifies each ballot layout for the State of Maryland.

Ms. Lamone serves on the Executive Committee of the National Association of Secretaries of State and the U.S. Election Assistance Commission's Standards Board and Advisory Board. She is also Vice Chair of the Attorney Grievance Commission of Maryland and Chair of the Character Committee for the Fifth Appellate Circuit and the Select Committee on Gender Equality.

Chairman EHLERS. Thank you very much. Dr. Wagner.

STATEMENT OF DR. DAVID WAGNER, PROFESSOR OF COMPUTER SCIENCE, UNIVERSITY OF CALIFORNIA AT BERKELEY

Dr. WAGNER. Chairmen, Committee Members, thank you for the opportunity to testify today. My name is David Wagner. I am an Associate Professor of Computer Science at UC Berkeley. My expertise is in computer security and electronic voting.

In my research into electronic voting, I have come to the conclusion that the federal standards process is not working. The federal testing labs are failing to weed out machines with serious security and reliability problems. We know that the federal testing labs have approved machines that have lost thousands of votes. We know that the testing labs have approved machines that have serious reliability problems.

How do we know that? Well, the State of California, my home state, does its own reliability testing, using a methodology that is more rigorous than occurs at any level of federal testing, and when the State of California went to test one federally approved system last year, they discovered mechanical and software reliability problems so severe that if those machines had been used in a real elec-

tion, on election day, 20 percent of those machines would have failed.

Fortunately, California is on top of things, and was able—has been able to detect and fix these problems before they impact an election, but it raises questions about how the testing labs came to approve a system like this.

Also, the federal testing labs, we know, are approving machines that have security problems. We know that because Finnish researcher Harri Hursti, an outsider, has found serious security vulnerabilities in federally approved voting systems. And in my own research, when I was commissioned to analyze one federally approved voting system, I too found security vulnerabilities that the federal testing labs had overlooked.

So, in short, the testing labs aren't getting the job done, and what is more, so far, the federal standards, even the 2005 federal standards, have yet to address these problems. So, that is the first of several shortcomings in the federal standards that I wanted to highlight today.

The second is that it is my opinion that the standards are not sufficiently grounded in a solid understanding of the scientific and engineering principles. There is a broad consensus among the technical experts who have studied these issues that today, the best tool we have for protecting the reliability and the security of our elections is the use of voter-verified paper records, along with routine manual audits of those records.

We know that computers can fail. We know that computers can make mistakes, and part of the problem with paperless voting machines is that they don't provide any independent way to go back and reconstruct the voter's intent if voting software should prove faulty, or be tampered with.

This is not a minority opinion. For instance, recently, the Brennan Center, in collaboration with a large group of technical experts and election officials, has completed a comprehensive, 150-page analysis of some of the threats facing voting systems. Their conclusion was that without voter-verified paper records, a single person may be able to switch votes on a large scale, possibly undetected, and potentially even swing a close election.

So today, I don't know of a single colleague in the computer security community who believes it is possible to have full confidence in election outcomes without paper, given our current state of our voting equipment. However, this consensus among technical experts has yet to be reflected in the federal voting standards. So, this is one example, and there are many others, of how the federal standards are lagging behind the best scientific and engineering understanding.

The consequence of these shortcomings is that the federal standards are not sufficient to guarantee that federally approved voting systems are able to adequately protect the integrity of our elections, either against unintentional failures, or against deliberate tampering.

I see that I have used up most of my allocated time. There were a number of other points I wanted to make. In my written testimony, I have discussed some of the steps that the EAC could take to remedy these problems in the short term, as well as some meas-

ures that election officials could take before these November elections, to help as much as possible, and I would welcome the chance to discuss this topic further with the Committee Members.

Thank you.

[The prepared statement of Dr. Wagner follows:]

PREPARED STATEMENT OF DAVID WAGNER

Thank you for the opportunity to testify today. My name is David Wagner. I am an associate professor of computer science at U.C. Berkeley. My area of expertise is in computer security and the security of electronic voting. I have an A.B. (1995, Mathematics) from Princeton University and a Ph.D. (2000, Computer Science) from U.C. Berkeley. I have published two books and over 90 peer-reviewed scientific papers. In past work, I have analyzed the security of cell phones, web browsers, wireless networks, and other kinds of widely used information technology. I am a member of the ACCURATE center, a multi-institution, interdisciplinary academic research project funded by the National Science Foundation[1] to conduct novel scientific research on improving election technology. I am a member of the California Secretary of State's Voting Systems Technology Assessment Advisory Board.[2]

Background

Today, the state of electronic voting security is not good. Many of today's electronic voting machines have security problems. The ones at greatest risk are the paperless voting machines. These machines are vulnerable to attack: a single person with insider access and some technical knowledge could switch votes, perhaps undetected, and potentially swing an election. With this technology, we cannot be certain that our elections have not been corrupted.

Studies have found that there are effective security measures available to protect election integrity, but many states have not implemented these measures. The most effective defense involves adoption of voter-verified paper records and mandatory manual audits of these records, but only 13 states have mandated use of these security measures. (At present, 27 states mandate voter-verified paper records, another eight states use voter-verified paper records throughout the state even though it is not required by law, and the remaining 15 states do not consistently use voter-verified paper records. Of the 35 states that do use voter-verified paper records statewide, only 13 require routine manual audits of those records.[1]) Voter-verified paper records provide an independent way of reconstructing the voter's intent, even if the voting software is faulty or corrupt, making them a powerful tool for reliability and security.

Problems

The federal qualification process is not working. Federal standards call for voting machines to be tested by Independent Testing Authorities (ITAs) before the machines are approved for use, but the past few years have exposed shortcomings in the testing process. The ITAs are approving machines with reliability, security, and accuracy problems. In the past several years:

- ITA-approved voting machines have lost thousands of votes. In Carteret County, NC, voting machines irretrievably lost 4,400 votes during the 2004 election. The votes were never recovered [2]. In 2002, vote-counting software in Broward County, Florida, initially mis-tallied thousands of votes, due to flaws in handling more than 32,000 votes; fortunately, alert election officials noticed the problem and were able to work around the flaws in the machines. In 2004, the same problem happened again in Broward County, changing the outcome on one state proposition [3,4], and in Orange County [5]. In Tarrant County, Texas, an ITA-approved voting system counted 100,000 votes that were never cast by voters [6].
- ITA-approved machines have suffered from reliability flaws that could have disrupted elections. California's reliability testing found that one ITA-approved voting system suffered from mechanical and software reliability problems so severe that, if it had been used in a real election, about 20 percent

[1] This work was supported by the National Science Foundation under Grant No. CNS–052431 (ACCURATE). Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author and do not necessarily reflect the views of the National Science Foundation.

[2] I do not speak for UC–Berkeley, ACCURATE, the California Secretary of State, or any other organization. Affiliations are provided for identification purposes only.

of machines would have experienced at least one failure during election day and probably would have had to be taken out of service [7].

- ITA-approved machines have been found to contain numerous security defects that threaten the integrity of our elections. Over the past several years, we have been inundated with revelations of security flaws in our voting systems from academics (e.g., Johns Hopkins University, Rice University [8]), industry consultants hired by election administrators (e.g., SAIC [9], Compuware [10], InfoSENTRY [11], and RABA [12]), and interested outsiders (e.g., Finnish researcher Harri Hursti [13,14]). None of these flaws were caught by ITAs. In the past five years, at least eight studies have evaluated the security of commercial voting systems, and every one found new, previously unknown security flaws in systems that had been approved by the ITAs. In my own research, I was commissioned by the State of California to examine the voting software from one major vendor, and I found multiple security flaws even though the software was previously approved by ITAs [15]. One of these flaws was discovered at least three times by independent security experts over a period of nine years (once in 1997, again in 2003, and again in 2006), but was never flagged by the ITAs at any point over that nine-year period [16].

All of these defects were ostensibly prohibited by federal standards [17], but the ITA testing and federal qualification process failed to weed out these problematic voting systems. The consequence of these problems is that the federal qualification process is at present unable to assure that voting systems meet minimum quality standards for security, reliability, and accuracy.

Federal standards have so far failed to address these problems. The 2005 VVSG standards do not remedy the demonstrated failures of the process to screen out insecure, unreliable, and inaccurate machines.

These failures have exposed structural problems in the federal qualification process:

- The ITAs are paid by the vendors whose systems they are evaluating. Thus, the ITAs are subject to conflicts of interest that raise questions about their ability to effectively safeguard the public interest.
- The process lacks transparency, rendering effective public oversight difficult or impossible. ITA reports are proprietary—they are considered the property of the vendor—and not open to public inspection. Also, if a voting system fails the ITA's tests, that fact is revealed only to the manufacturer of that voting system. In one widely publicized incident, one Secretary of State asked an ITA whether it had approved a particular voting system submitted to the ITA. The ITA refused to comply: it declined to discuss its tests with anyone other than the voting system manufacturer, citing its policy of confidentiality [18].

  In addition, the secretive nature of the elections industry prevents independent security experts from performing their own analysis of the system. Technical information about voting systems is often considered proprietary and secret by vendors, and voting system source code is generally not available to independent experts. In the rare cases where independent experts have been able to gain access to source code, they have discovered reliability and security problems.
- Testing is too lax to ensure the machines are secure, reliable, and trustworthy. The federal standards require only superficial testing for security and reliability. For instance, California's tests have revealed unexpected reliability problems in several voting systems previously approved by ITAs. In my opinion, California's reliability testing methodology is superior to that mandated in the federal standards, because California tests voting equipment at a large scale and under conditions designed to simulate a real election.
- Many standards in the requirements are not tested and not enforced. The federal standards specify many requirements that voting systems must meet, and specify a testing methodology for ITAs to use, but many of the requirements are not covered by that testing methodology. The ITAs only apply whatever tests are mandated by the standards. The consequence is that the federal standards contain many requirements with no teeth. For instance, Section 6.4.2 of the 2002 standards requires voting systems to "deploy protection against the many forms of threats to which they may be exposed;" the security vulnerabilities listed above appear to violate this untested requirement. Likewise, Section 6.2 requires access controls to prevent "modification of compiled or interpreted code;" three of the major vulnerabilities revealed in the past two years have violated this requirement. These requirements ap-

pear to be ignored during ITA testing and thus have little or no force in practice.

- Parts of the voting software are exempt from inspection, reducing the effectiveness of the federal testing. The federal standards contain a loophole that renders Commercial Off-the-Shelf (COTS) software exempt from some of the testing. The COTS loophole means that the security, reliability, and correctness of those software components are not adequately examined. COTS software can harbor serious defects, but these defects might not be discovered by the federal qualification process as it currently stands.
- Even if an ITA finds a serious security flaw in a voting system, they are not required to report that flaw if the flaw does not violate the VVSG standards. Thus, it is possible to imagine a scenario where an ITA finds a flaw that could endanger elections, but where the ITA is unable to share its findings with anyone other than the vendor who built the flawed system. Relying upon vendors to disclose flaws in their own products is unsatisfactory.
- There are disincentives for local election officials to apply further scrutiny to these machines. Some local election officials who have attempted to make up for the gaps in the federal qualification process by performing their own independent security tests have faced substantial resistance. After one Florida county election official invited outside experts to test the security of his voting equipment and revealed that the tests had uncovered security defects in the equipment, each of the three voting system vendors certified in Florida responded by declining to do business with his county [19]. The impasse was resolved only when the State of Florida interceded [20]. In Utah, one election official was pressured to resign after he invited independent security experts to examine the security of his equipment and the testing revealed security vulnerabilities [21,22]. The barriers to performing independent security testing at the local level heighten the impact of shortcomings in the federal standards.
- If serious flaws are discovered in a voting system after it has been approved, there is no mechanism to de-certify the flawed system and revoke its status as a federally qualified voting system.

The 2005 VVSG standards do not address these structural problems in the federal qualification process. The 2005 VVSG standards were drafted over a period of approximately three months. With such an extremely constrained time schedule, it is not surprising that the 2005 standards were unable to satisfactorily address the fundamental issues raised above.

The shortcomings of the 2005 VVSG standards have several consequences:

- We are likely to continue to see new security and reliability problems discovered periodically. The security and reliability of federally approved systems will continue to be subject to criticism.
- Shortcomings at the federal level place a heavy burden on states. The 2005 VVSG standards do not provide enough information about the reliability and security of these machines to help states and counties make informed purchasing decisions. This places an undue burden on local election officials. Some states are doing their best to make up for gaps in the federal process, but many states do not have the resources to do so.

  Also, the increased scrutiny at the state level has the potential to subject vendors to dozens of involved state-level certification processes that have been instituted to make up for the gaps in the federal process, increasing the compliance burden on vendors.
- Millions of voters will continue to vote on voting machines that cannot be independently audited. This may diminish confidence in election results. In the event of any dispute over the outcome of the election, it may be impossible to demonstrate whether the election was accurate. Allegations of fraud may be difficult or impossible to rebut, due to the fact that today's paperless voting machines do not generate and retain the evidence that would be required to perform an effective audit. The lack of openness and transparency regarding voting system source code, testing, and equipment may spawn further distrust in voting systems.
- Voting equipment may still be subject to security and reliability problems, even if they comply with the 2005 VVSG standards. Many of the security and reliability defects described above would not have been prevented even if the 2005 VVSG standards had been in force when the machines were evaluated.

Approval under the 2005 VVSG standards is not a guarantee of security or reliability.

Recommendations

The Technical Guidelines Development Committee (TGDC) and the Election Assistance Commission (EAC) could improve the VVSG standards and begin to address these shortcomings by taking several steps:

- Mandate voter-verified paper records and mandatory manual audits. Stop approving paperless voting machines. Today's paperless voting machines are not auditable. There is no effective way to independently check whether their results are accurate or to detect electronic fraud. The inability to audit these machines greatly heightens the impact of security problems. Ensuring that election results can be independently audited would go a long way to reducing the impact of security defects in voting equipment. The 2007 VVSG should mandate voter-verified paper records and automatic manual audits of those records after every election.
- Broaden the focus beyond functionality testing, and embrace discipline-specific methods of testing voting equipment. Today, the standards primarily focus on functionality testing, which evaluates whether the machines implement all necessary functionality. Standards need to be expanded to incorporate technical evaluations of the security, reliability, and usability of these machines. The standards must incorporate the different forms of evaluation these disciplines each require. For instance, security evaluation is unique, in that it must deal with an active, intelligent adversary; functionality concerns the presence of desired behavior, while security concerns the absence of undesired behavior. Consequently, system security evaluations should always include an adversarial analysis, including a threat assessment and a source code review. The testing methods in the standard should be updated to reflect the state of the art in each discipline. Special attention will be needed to ensure that the testing team has sufficient expertise, time, and resources to perform a thorough evaluation.
- Eliminate conflicts of interest in the federal testing process. ITAs should not be paid by the vendors whose systems they are testing. Several financial models are possible, and all deserve consideration. For instance, one possibility is for the EAC to collect a fee from vendors, as a condition of eligibility for the federal qualification process, to cover the costs of hiring ITAs to evaluate the system under consideration.
- Reform the federal testing process to provide more transparency and openness. All ITA reports should be publicly available. The documentation and technical data package provided to ITAs should be made available to the public or to independent technical experts so that they can independently cross-check the ITA's conclusions and exercise public oversight of the testing process. Also, the right of the public to observe elections is rendered less meaningful if those observing are unable to understand what it is that they are seeing; under the current rules, observers have no access to the documentation for the voting system they're observing, which partially limits their ability to effectively monitor the administration of the election.
- Require broader disclosure of voting system source code. The secrecy surrounding voting source code is a barrier to independent evaluation of machines and contributes to distrust. To enhance transparency, improve public oversight and hold vendors accountable, voting software should be disclosed more broadly. At a minimum, source code should be made available to independent technical experts under appropriate non-disclosure agreements. In the long run, source code should be publicly disclosed. Source code disclosure does not prevent vendors from protecting their intellectual property; vendors can continue to rely on copyright and patent law for this purpose.

  Keeping source code secret does not appreciably improve security: in the long run, the software cannot be kept secret from motivated attackers with access to a single voting machine. However, disclosing source code more broadly could enhance public confidence in elections and is likely to lead to improvements to voting system security.
- Incorporate closed feedback loops into the regulatory process. Standards should be informed by experience. At present, there is no requirement for reporting of performance data or failures of voting equipment, no provision for analyzing this data, and no process for revising regulations in a timely fashion in response. The 2007 VVSG should incorporate a framework for col-

lecting, investigating, and acting on data from the field and should provide a mechanism for interim updates to the standards to reflect newly discovered threats to voting systems. For instance, the FAA requires airplane operators to report all incidents (including both failures and near-failures), uses independent accident investigators to evaluate these reports, and constantly revises regulations in response to this information. Adopting a similar framework for voting systems would likely improve voting systems.

- Strengthen the evaluation of usability and accessibility. The discipline of usability has developed methods for usability testing—such as user testing with actual voters or poll workers, as well as heuristic evaluation by usability and accessibility experts—but these methods are not currently reflected in the VVSG standards. They would represent a valuable addition to the standards. In addition, usability experts have suggested it would be helpful to move away from the current emphasis on functional requirements and towards an evaluation regime based primarily on assessing performance against some quantitative metric of usability [23]. The 2005 VVSG standards are a positive first step towards addressing human factors issues, but there is room for further improvement.
- Increase the representation of technical experts in computer security on the TGDC. The appointment of Prof. Ronald Rivest to the TGDC was warmly welcomed by security experts: Rivest is extremely qualified and very highly respected among the computer security community. However, at present, Rivest is the only member of the TGDC with substantial experience in the area of security. Appointing more TGDC members with security expertise would improve the ability of the TGDC to develop effective standards.
- Ensure that standards are grounded in the best scientific and engineering understanding. Too often, decisions have been made that do not reflect the best judgment of the relevant experts. For instance, in 2004 the premier professional organization for computing professionals surveyed their members about e-voting technology. 95 percent of respondents voted for a position endorsing voter-verified paper records and expressing concerns about paperless voting technologies [24]—yet two years later, this overwhelming consensus among technical experts has yet to be reflected in federal standards.

For further information, I refer readers to the ACCURATE center's "Public Comment on the 2005 Voluntary Voting System Guidelines," [25] which I have attached as an appendix to this testimony.

In the short-term, adopting the recommendations of the Brennan Center report on e-voting is the most effective and practical step election officials could take to make existing voting systems as secure and reliable as possible for this November. These recommendations include:

- Conduct automatic routine audits of the voter-verified paper records;
- Perform parallel testing of voting machines;
- Ban voting machines with wireless capability;
- Use a transparent and random selection process for all audits; and,
- Adopt procedures for investigating and responding to evidence of fraud or error.

For further information, see the Brennan Center report [26].

In addition, I encourage election officials to pay special attention to their voter registration systems. In many states, voter registration processes are in a state of flux, due to the HAVA requirement that statewide registration databases be in place this year. These databases could significantly improve elections if implemented well; if implemented poorly, however, they could disenfranchise many thousands of voters. See the USACM report on voter registration databases [27].

Summary

In summary, the 2005 VVSG standards contain significant shortcomings regarding the security, reliability, and auditability of electronic voting. Members of the computer security community are available to help devise better solutions.

Notes

1. "The Machinery of Democracy: Protecting Elections in an Electronic World," Brennan Center Task Force on Voting System Security, June 27, 2006. Since that report was written, Arizona has adopted voter-verified paper records and routine manual audits of those records statewide.

2. "Computer loses more than 4,000 early votes in Carteret County," Associated Press, November 4, 2004.
3. "Broward Ballot Blunder Changes Amendment Result," Local 10 News, November 4, 2004.
4. "Broward Machines Count Backward," *The Palm Beach Post,* November 5, 2004.
5. "Distrust fuels doubts on votes: Orange's Web site posted wrong totals," *Orlando Sentinel,* November 12, 2004.
6. "Vote spike blamed on program snafu," Forth Worth Star-Telegram, March 9, 2006.
7. "Analysis of Volume Testing of the AccuVote TSx/AccuView," Report of the California Secretary of State's Voting Systems Technology Assessment Advisory Board, October 11, 2005.
8. "Analysis of an Electronic Voting System," Tadayoshi Kohno, Adam Stubblefield, Aviel D. Rubin and Dan S. Wallach, May, 2004.
9. "Risk Assessment Report: Diebold AccuVote–TS Voting System and Processes," Science Applications International Corporation, September 2, 2003.
10. "Direct Recording Electronic (DRE)Technical Security Assessment Report," Compuware Corporation, November 21, 2003.
11. "Security Assessment: Summary of Findings and Recommendations," InfoSENTRY, November 21, 2003.
12. "Trusted Agent Report: Diebold AccuVote–TS System," RABA Innovative Solution Cell, January 20, 2004.
13. "Critical Security Issues with Diebold Optical Scan," Harri Hursti, Black Box Voting, July 4, 2005.
14. "Critical Security Issues with Diebold TSx," Harri Hursti, Black Box Voting, May 11, 2006.
15. "Security Analysis of the Diebold AccuBasic Interpreter," Report of the California Secretary of State's Voting Systems Technology Assessment Advisory Board, February 14, 2006.
16. "Connecting Work on Threat Analysis to the Real World," Douglas W. Jones, June 8, 2006.
17. For instance, the security vulnerabilities appear to violate the requirements of Section 6.4.2 and Section 6.2 of the 2002 FEC standards.
18. "Election Officials Rely on Private Firms," *San Jose Mercury News,* May 30, 2004.
19. "Election Whistle-Blower Stymied by Vendors," *Washington Post,* March 26, 2006.
20. "Sort of fixed: Broader election flaws persist," *Tallahassee Democrat,* April 15, 2006.
21. "Cold Shoulder for E-voting Whistleblowers," *The New Standard,* May 17, 2006.
22. "New Fears of Security Risks in Electronic Voting Systems," *The New York Times,* May 12, 2006.
23. "Public Comment on the 2005 Voluntary Voting System Guidelines," ACCURATE Center, submitted to the United States Election Assistance Commission, September 2005.
24. "ACM Recommends Integrity, Security, Usability in E-voting, Cites Risks of Computer-based Systems," USACM, September 28, 2004.
25. *http://accurate-voting.org/accurate/docs/2005_vvsg_comment.pdf*
26. "The Machinery of Democracy: Protecting Elections in an Electronic World," Brennan Center Task Force on Voting System Security, June 27, 2006.
27. "Statewide Databases of Registered Voters: Study of Accuracy, Privacy, Usability, Security, and Reliability Issues," commissioned by the U.S. Public Policy Committee of the Association for Computing Machinery, February 16, 2006.

Chairman EHLERS. Thank you very much, and after those comments, perhaps we should have more distance between you and Mr. Groh in the seating arrangement.

We will now call on Mr. Groh.

STATEMENT OF MR. JOHN S. GROH, CHAIRMAN, ELECTION TECHNOLOGY COUNCIL, INFORMATION TECHNOLOGY ASSOCIATION OF AMERICA

Mr. GROH. Good afternoon. My name is John Groh, and I am a Senior Vice President with Election Systems & Software, one of the voting system vendors in the United States.

I am here to provide testimony on the part of, or on behalf of the Information Technology Association of America, and its Election Technology Council, which is a subset group. ITAA is one of the oldest, the Nation's oldest and largest trade associations for the information technology industry, representing approximately 325 companies. The Election Technology Council consists of companies which offer voting system technology hardware products, software, services, to support the electoral process.

These companies have organized within ITAA to work together to address common issues facing our industries as a valued stakeholder. Current members of the ETC are Advanced Voting Solutions, Danaher Guardian Voting Systems, Diebold Election Systems, Election Systems & Software, Hart InterCivic, Perfect Voting Systems, and Sequoia Voting Systems, along with UniLect Corporation. Our membership is open to all companies that are interested in the voting environment.

Our member companies have a great stake in the conduct and the outcome of this process. Indeed, voting solutions provided and supported by our members account for over 90 percent of the voting systems the marketplace uses today. Our members employ over 2,000 dedicated citizen employees, who work hard to support the success of American elections.

The ETC is pleased to respond to your request for a vendor perspective on the issues surrounding the implementation of the 2005 Voluntary Voting System Guidelines, and the national voting system certification and testing process. My written testimony is much longer, but I would like to provide a few detailed responses to specific issues.

First, I would like to acknowledge the very strong partnership and alliance that the vendor community has with two important organizational leaders in this area: the United States Election Assistance Commission, and the National Institute of Standards and Technology, as well as the Technical Guidelines Development Committee. Both of these groups should be commended for the focus and urgency with which they have moved forward with the Voluntary Voting System Guidelines. It has been a tremendous task to do this in a short period of time, that was challenged with everyone in this.

Comments on the 2005 Voting System Guidelines process. Turning to the specific issues of the VVSG, it is important to first underscore the respect we have for the standards making process, and our very belief, our real belief that a dynamic standards process is key to motivating innovation and continued enhancement of voting technology.

Having said that, there are several realities that the voting system vendors believe must be acknowledged and accounted for in laying the groundwork for successful rollout of the 2005 VVSG. Issues our members wish to raise to your attention include: one,

the need to consider fiscal and operational feasibility; two, the impact of certification and testing; three, the need for continuing funding streams; and four, the need for a phased-in implementation.

Let me touch first on the fiscal operational feasibility. There is a discernible trend in the development of the 2005 Voluntary Voting System Guidelines to push the envelope of the voting system capabilities. While vendors can develop and deliver most of what is required in the VVSG, such requirements will come at a cost. Eventually, addition of system features and functions will be constrained by what the market will be willing to pay or able to pay. A balance needs to be struck between the development of new requirements and future versions of VVSG, and the fiscal and operational realities that the states and the counties and the United States that run elections have to deal with.

The second issue, on the impact of certification and testing on the guidelines. Certification and testing will be critical to achieving full compliance with the 2005 standards. To achieve federal certification of systems under the 2005 VVSG by December of 2007, which is the effective date, the new certification process will likely need to be in place before the end of this year, with accredited testing labs ready to test, and tests defined for every applicable requirement for the 2005 guidelines. This is an extremely aggressive timeline for the vendors, as well as many of us sitting at this table.

First, although the voting system features and functions addressed for the first time require the development of a new certification test, some of the 2005 Voluntary Voting System Guideline requirements have no test defined to date. Second, once the tests are in place, we would have to expect a learning curve, and unforeseen difficulties associated with the change.

Then, some tests may add prohibitive delays or costs in the certification process, and depending on the nature of the problem, this may require modification to the guidelines or the testing process itself. All of these challenges will require some flexibility, as the revised guidelines and certification process are implemented. The alternatives will be a possibly unattainable or untestable standard.

I have other comments, but my time is up, and so I will yield to the floor for questions.

[The prepared statement of Mr. Groh follows:]

PREPARED STATEMENT OF JOHN S. GROH

Good afternoon, Chairmen Ehlers and Boehlert, Ranking Members Millender-McDonald and Gordon:

My name is John Groh and I am a Senior Vice President with Election Systems & Software. I am here to provide testimony on behalf of the Information Technology Association of America (ITAA) and its Election Technology Council (ETC). The ITAA is one of the Nation's oldest and largest trade associations for the information technology industry, representing approximately 350 companies. The Election Technology Council consists of companies which offer voting system technology hardware products, software and services to support the electoral process. These companies have organized within the association to work together to address common issues facing our industry. Current members of the ETC are: *Advanced Voting Solutions, Danaher Guardian Voting Systems, Diebold Election Systems, Election Systems & Software, Hart InterCivic, Perfect Voting System, Sequoia Voting Systems,* and *UniLect Corporation.* Membership in the ETC is open to any company in the election systems marketplace.

The ETC is pleased to respond to your request for vendor perspective on issues surrounding the implementation of the 2005 Voluntary Voting Systems Guidelines (2005 VVSG) and the national voting system certification and testing processes.

Our member companies have a great stake in the conduct and outcome of this process. Indeed, voting solutions provided and supported by our members account for over 90 percent of voting systems in the marketplace today. Our members employ over 2,000 dedicated citizen employees, who all work hard to support the success of American elections.

First, I would like to acknowledge the very strong partnership the vendor community has with two important organizational leaders in this effort: the U.S. Election Assistance Commission (EAC) and the National Institute of Standards and Technology (NIST)/Technical Guidelines Development Committee (TGDC). Both should be commended for the focus and urgency with which they have moved to implement the requirements of the *Help America Vote Act of 2002* (HAVA), the roll-out of the Voluntary Voting Systems Guidelines, and the transition to a new voting system certification process.

Comments on the 2005 Voluntary Voting Systems Guidelines Process:

There are several realities that voting system vendors believe must be acknowledged and accounted for in laying the groundwork for a successful roll-out of the 2005 VVSG. The delays at the beginning of the EAC–NIST ramp-up period set the guidelines development process back by about 12–18 months. The effort to issue the VVSG was unparalleled in terms of the scope and speed of a technical guidelines development for voting systems, and possibly for any comparable technology. Indeed, similar efforts have taken many years to complete. However, the initial delays compounded an already uncertain situation and many State and local governments chose to delay purchases of HAVA-compliant voting equipment in anticipation of the new guidelines.

Given the amount of installation work now being undertaken, and despite the complexity and politics involved with voting systems procurements, the implementation of new voting systems that meet the requirements of HAVA is generally going smoothly. With primaries and general elections now looming, elections officials must exercise caution against taking shortcuts in important areas such as training, testing, and preparation.

Many, if not most, of the problems that are experienced in the U.S. electoral process today are not directly technological, but involve humans and their interactions with technology. Reports of problems in the 2006 primary elections have been largely attributable to insufficient training and preparedness in the polling place. Those closely involved in voting know that it is an exercise with a thousand moving parts and most of those parts are processes conducted by human hands.

The voting systems installation situation currently facing states and local governments is unique. Once this work is complete, the hardware may be in place ten years or more. While the immediate burdens of procurement and installation will surely diminish, the ongoing management and support of the large quantity of new systems, combined with the upcoming VVSG effective dates and roll-out of a new certification process, presents many new challenges and issues to elections officials and their vendor partners. Issues our members wish to raise to your attention include:

- What is feasible both fiscally and operationally?
- The impact of certification and testing on the guidelines
- The need for continued funding streams
- The need for phased implementation

What Is Feasible Both Fiscally and Operationally?

There is a discernible trend in the development of the 2005 VVSG to "push the envelope" of voting system capabilities. While vendors can develop and deliver most of what is required in the VVSG, such requirements will come at a cost. Eventually, addition of system features and functions will be constrained by what the market will be willing and able to pay. A balance needs to be struck between the development of new requirements in future versions of the VVSG and fiscal and operational realities in the states.

Those overseeing development of new voting systems guidelines should follow the old adage: "perfect should not be the enemy of good." While we always strive towards perfection, we believe that making perfection the operating standards will have unintended consequences. What may be perfect for an aspect of security may be a limiting factor on usability. There may need to be compromises to find a "good"

and balanced system that can actually be produced, certified and made affordable to jurisdictions using taxpayers' money.

The Impact of Certification and Testing on the Guidelines

As new voting systems certification and testing processes are rolled out, there will be a learning curve that will cause delays in the implementation of the guidelines. Once the guidelines are actually applied by a test lab against a voting system, it is likely that the complexity of the guidelines and conflicts between some requirements in the 2005 VVSG will be discovered. As instances are discovered, further interpretation and revision of the guidelines will become necessary. Some examples that we know of to date are:

- The subjective interpretation that will be required in the area of testing systems for accommodating cognitive disabilities (no one system can accommodate all disabilities and there is no list of disabilities defined for the labs to use in their testing.)
- The addition of a standard port to read the DRE memory without compromising security using an independent system that hasn't been established.
- Requirements that need to be tested, yet no tests are yet defined (e.g., usability, benchmarks are still being studied by NIST.)

Voting systems features and functions addressed for the first time in the 2005 VVSG have mandated the development of new tests. Some of the 2005 VVSG requirements have no tests defined to date. It is likely that the development and initial implementation of new tests will run into unforeseen difficulties and delays to determine objective and effective parameters. Some tests may add prohibitive delays or costs to the certification process. Depending on the nature of the problem, this may require modification to the guidelines or to the testing process itself.

These situations will demand some flexibility in revisions to the guidelines and certification processes. The alternative will be to find some voting systems, or even a generation of voting equipment, uncertifiable against a possibly unattainable or untestable standard. If that equipment can readily meet the requirements spelled out in HAVA, such a result would be a poor outcome and one that may force states to squander federal and state monies already appropriated, disbursed and spent on HAVA compliant equipment.

Need for Continued Funding Streams

One shortcoming of the *Help America Vote Act of 2002* is the lack of a mechanism for continued funding to the states and election jurisdictions. Under the 2005 VVSG and future iterations of the guidelines, it is almost certain that states and election jurisdictions will be required to purchase and deploy new voting systems hardware and—more likely—firmware and software to be compliant with the new guideline iterations. While much of the expense for new systems compliant with the 2002 Voluntary Voting System Standards (2002 VVSS) was covered by the first HAVA appropriations, much of the continuing expense for modifications and upgrades demanded by changes in the 2005 VVSG and future iterations will fall to the states and local governments.

In many states, the most significant expense not covered by federal money was for Voter Verified Paper Audit Trail (VVPAT) equipment. The purchase of VVP AT printers was not anticipated by HAVA, and not enough money appropriated for it. In many states, legislative mandate has made the VVP AT a necessary voting system component. The additional cost of these devices has diverted monies from other important aspects of HAVA, such as voter education and user training.

The increasing complexity required of voting systems by the guidelines is creating a need for more user training. As I stated above, the vast majority of problems experienced with voting systems are attributable to insufficient training and preparedness in the polling place. Some of these problems will decrease as elections officials and other system users move along the technology learning curve. But funding the necessary training will move elections jurisdictions more rapidly along the learning curve, expediting the drive to problem-free elections.

Need for Phased Implementation

The voting systems market will take some time to adopt fully the new guidelines and certification process. For evidence of the time it takes for the marketplace to completely adjust to and absorb a new standard from release to widespread adoption, one need look no further than the case of the 2002 VVSS. It took more than three years from the initial release to adoption on a near-national basis. This lengthy adoption period was not for a lack of trying on the part of states and vendors but rather recognition that the process to make encompassing changes requires

the time to do it right. The funding that HAVA provided facilitated the adoption of the 2002 VVSS by the states. As there currently are no federal funds earmarked to facilitate the implementation of 2005 VVSG compliant voting systems, the nationwide adoption of the 2005 VVSG may take even longer.

Given that the 2005 VVSG adoption process may take at least two to three years to complete, our members have recommended a phased implementation of the guidelines be taken under consideration by the EAC.[1] This is a critically important issue which merits consideration by all interested parties.

Our members believe that equipment certified under the 2002 VVSS is HAVA-compliant. However, much of that equipment will not be compliant with the 2005 VVSG at the time the new guidelines become effective in December 2007. It is our position that voting systems certified to meet 2002 VVSS that are HAVA-compliant and have been proven in the field to provide the customer and the voter with a satisfactory level of usability, reliability, accuracy, and security should be grandfathered under the 2005 VVSG. Many of the issues raised regarding 2002 VVSS compliant equipment can likely be addressed through operational procedure changes and software modifications.

If equipment certified under the 2002 standard is not grandfathered under the 2005 guidelines, the cost burden to the customer will be onerous as jurisdictions will have to replace their existing 2002 VVSS and HAVA-compliant equipment with 2005 VVSG compliant equipment. Without some type of grandfathering provisions under the 2005 VVSG, additional federal funds will be necessary to cover the cost of replacement equipment and upgrades. Jurisdictions should be able to get at least a ten to fifteen year return on investment from their existing equipment and not be forced to replace it every time a new version of the guidelines are implemented.

Comments on National Voting Systems Certification and Testing Processes:

The EAC provided the states and NIST a 24-month transition window after the adoption of the 2005 VVSG on December 14, 2005 to migrate to a new set of voting system guidelines and certification process. This migration has already begun and the EAC approved adoption of an interim set of federal certification procedures at its July 13, 2006 meeting. To facilitate federal ITA certifications before the December 2007 deadline, the new certification process will likely need to be in place before the end of this year, with accredited testing laboratories ready to test, and tests defined for every applicable requirement in the 2005 VVSG.

There are several important issues that should be addressed in the migration to new certification and testing processes, including:

- Testing Frequency and Repetition
- Developing New Uniform, Economical Testing Practices
- Certification for Systems Developed under a Previous Standard

Testing Frequency and Repetition

As the EAC and NIST move forward in the design and implementation of a new certification process, our members believe the EAC should give serious consideration to the fundamental issue of testing frequency and repetition. State and county election officials, and their vendor partners, face an ever-increasing volume of federal qualification and state testing activity. Reducing the cost and delay imposed by continual—and often repetitive—testing should be a primary consideration of the new certification process. By combining the federal level ITA certification testing and basic state level tests, the system certification process could be made more streamlined and uniform, saving valuable time for election officials and reducing redundant non-value added costs for everyone.

Developing New Uniform, Economical Testing Practices

Not only is testing voting systems for the purpose of obtaining federal and State certifications becoming too frequent and overly costly, the situation may soon be aggravated by the need for new and fairly complex tests mandated by the 2005 VVSG. The guidelines put forth several new requirements for which no appropriate tests currently exist. According to experts in the standards and testing field, the most challenging tests may prove to be in the areas of system usability and security.

Further, the advent of state-mandated volume testing has dramatically increased costs of certification in some states. Volume testing incorporates the use of at least 100 DREs, each unit counting hundreds of ballots over the course of days to emulate

[1] ETC testimony before the U.S. Election Assistance Commission, February 2, 2006; *http://www.electiontech.org/downloads/ETC%20Groh%20EAC%20Testimony%20-%202.2.06%20-%20Final.pdf*

the election-day experience at a polling site. While the goals of this type of testing are worthy, cost increases have resulted.

Without the development of new tests that are uniformly applied from testing lab to testing lab, and designed from the outset to diminish the need for repetitive tests, a potentially vast new area of vendor expense may be created. Testing expense has the potential to drive up voting system costs significantly and slow the entry of new systems into the market. The ETC believes that the EAC, NIST, and other concerned groups should quickly take steps to begin work on developing more uniform and economical testing for voting systems.

Certification for Systems Developed Under a Previous Standard

In previous communications with the EAC, we have asked the Commission to recognize and retain the good and common elements of the pre-existing NASED voting system certification procedures. We expect that the EAC certification process will likely incorporate several elements of the NASED procedure.

One element of the current NASED certification process that the EAC has indicated it will carry forward is the discontinuation of certifying voting system platforms that were certified under a previous standard. It is important that Members of Congress understand the economic and election performance impacts of such a step on state and county election administrators, the voters and vendors.

We know that stopping any and all certification of systems certified under the 2002 VVSS, on a certain date, without an allowance for state required enhancements or to fix errors found, will impose major economic consequences on states or election jurisdictions which have recently purchased voting systems under those standards. Due to the many meaningful changes made under the 2005 VVSG, there may be no way to economically retrofit some voting systems. Such equipment may have to be discarded and new procurements undertaken with new purchase costs to the election jurisdictions.

In addition to cost and other economic impacts, the EAC should consider election management and performance issues in setting transition policy for systems certified under the 2002 VVSS. States and jurisdictions make voting system acquisitions with an expectation of a 10- to 15-year service life. This timeframe allows the customer to refresh technology when it becomes near-obsolete or to take advantage of technology upgrades as they become available in the market. As states and jurisdictions introduce new technology, they must move along the learning curves for system usage, support, and training. Changes to hardware platforms can impact the training that the customer has invested in its poll workers as well as associated voter education programs.

Concluding Remarks:

In providing this testimony, our intention is to give Members of the Committees vendor perspective on the roll-out of new voting systems guidelines and certification processes to the vendor community and, as we see it, to the states and election jurisdictions—our valued customers whom we serve.

It is our belief that the adherence to standards and rigor of the certification process is critical to maintaining the integrity of our elections. State adoption of the federal Voluntary Voting System Guidelines is what makes the standard effective.

The Election Technology Council and its members are committed to working with the EAC, NIST, and our customers, to see the 2005 VVSG and a new certification process through to successful implementation. Further, we look to EAC and NIST as the bodies best positioned and armed to tackle the tasks at hand. We hope that other parties interested in working on elections equipment and administration issues would similarly recognize the importance of the EAC and NIST initiatives and refrain from launching parallel and—in some instances—conflicting initiatives.

Above all, we are responsive to customer needs and are committed to providing safe, secure, accurate, reliable and accessible voting systems under any standard or certification program. We only ask that the *appropriate time be allowed* so it can be *done right* and that the *funding and costs of implementation be considered* when creating new guidelines and certification processes. We all recognize and accept that with new voting system technology comes complexity and need for changes in election administration, poll worker skills and increased voter education and outreach programs.

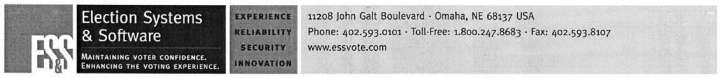
We are all involved in this process together, and by working together we can improve the process of voting, voter access and participation.

BIOGRAPHY FOR JOHN S. GROH

John Groh came to Election Systems & Software in 1995 to focus the company on a growth strategic plan that included development of new products, pursuing international markets for election automation, and growth through acquisitions. During this period ES&S has grown from 40 associates to well over 400; with a customer base that has grown from 600 local jurisdictions to more than 2,300 worldwide. The company's product offerings now cover the entire spectrum of end-to-end integrated voting systems—in paper, and electronic form.

John S. Groh functions in several roles at ES&S, including President of ES&S International, Senior Vice-President of Voter Registration Sales, and Senior Vice President of Marketing, Communication & Public Relations. Additionally in his role as Senior Vice-President of Government Relations he has served as ES&S' liaison with the U.S. Election Assistance Commission and has participated in the NIST–TGDC process of creating the new voting system guidelines. Further still, he represented ES&S at NASS and NASED events, and serves as spokesperson for ES&S on policy issues.

Mr. Groh currently serves as the Chairman of the Information Technology Association of America's (ITAA's)—Election Technology Council. He has offered testimony twice in front of the EAC on the HAVA implementation process.



Election Systems & Software, Inc. (ES&S) is the world's largest and most experienced provider of total election management solutions. For more than three decades, ES&S – as an election-only company and the industry leader – has grown to support a customer base of more than 1,700 jurisdictions in the United States. Based on the primary voting tabulation system installed within the United States, ES&S customers represent approximately 42% of registered voters in the United States.

ES&S is a privately held company and does not publicly disclose specific financial information. The bulk of ES&S' revenues, however, are generated from voting systems sales and services to states, counties and local jurisdictions. ES&S does not generate any revenue through sales to the federal government or grants from the federal government.

DISCUSSION

Chairman EHLERS. Thank you, and thank you all for staying within your time limits. I think that may have set a record for this committee.

The panel is being joined by Mr. Skall, from NIST, who will assist in answering technical questions addressed to Dr. Jeffrey.

I will begin the first round of questions, and recognize myself for five minutes.

First of all, I just want to comment on, I believe it was Ms. Lamone, you referred to the poll workers, as I recall, and I have always admired the incredible dedication of the poll workers, who come out at minimal pay, for incredibly long hours, a difficult job, and do it year after year after year, and I have the highest respect for them.

And partly for that reason, partly for other reasons, when we had the fiasco a few years ago in the Presidential election, and people were talking about solutions, I repeatedly heard people say, "Well, we have to train the poll workers better, and we have to train the

voters better." And I am a former professor. I have great respect for education, but I always said "Bunk." If you are having people who do something twice a year on average, in some cases less, you can train all you want, but they are not going to remember for six months or a year, just precisely what they have to do. You have to design the systems so that they are intuitive and operation is self-evident, and that is where the term human factors come in. So, I have pushed very hard on having human factors done first.

HUMAN FACTORS AND HAVA GUIDELINES, TECHNOLOGY

And Dr. Jeffrey, on that point, one of NIST's earliest products under HAVA was its Human Factors Report, partly, I suspect, because of my insistence on it. To what extent have the findings of this report been incorporated into the 2005 guidelines, and what kinds of guidelines remain to be written?

Dr. JEFFREY. Thank you, sir.

The 2004 report listed ten major recommendations on human factors, and these included incorporating the U.S. Access Board requirements and suggestions into the guidelines, developing performance-based, as opposed to design-based usability requirements, and looking at usability testing for voting systems.

Half of those, of the ten recommendations, have made it into the 2005 VVSG. The other half are being addressed, and will be addressed in the 2007 version. And I would just like to add that part of those usability requirements are not just for the voters, but they also include usability for poll workers, though it is not as comprehensive as for the voters, but it is included in there.

Mr. BAIRD. Mr. Chairman, could we check and see if the witnesses' mikes are all turned off.

Chairman EHLERS. Pardon?

Mr. BAIRD. We are getting some—it is this one over here.

Chairman EHLERS. I am sorry. Could you just turn off all your mikes for the moment, please. I am sorry, I can't hear you. Members turn off their mikes, too, unless you are speaking, yes. Yeah, just wait until the things really get rolling here. Okay, well, I appreciate your answer to that.

Are there other guidelines that you are preparing on human factors?

Dr. JEFFREY. On human factors, the other five recommendations. Actually, Mark, if you want to add the additional ones beyond the 2004 report.

Mr. SKALL. Yes. We are, again, in the 2007 proposed standard, we are adding looking at each usability requirement, again, as Dr. Jeffrey said, we are making them performance-based, adding actual testing benchmarks, and doing research to update all the accessibility and usability requirements that were contained in 2005.

Chairman EHLERS. Thank you. Mr. Groh, just to what extent has this better understanding of human factors affected the way that countries have, companies have designed their equipment, and to what extent have you been able to incorporate the human factors into your products?

Mr. GROH. Well, I think it has been a multi-step approach. The first hurdle was to meet and manage and adapt systems that would allow states and counties to get an accessible voting system. Acces-

sible voting systems are a difficult hurdle to cross over, because no single system will manage every voter with a disability issue that they face. But we have attempted to provide as many of them as we possibly can.

Because the 2005 Voluntary Voting System Guidelines were still in development during all of 2005, and were not issued until January 1, or the January timeframe of '06, we were looking at and waiting for the final draft and the final guidelines to come out, and so, we have just begun to create the next level, or the next wave of accessibility, as well as human factors issues with it. And we are looking for the performance and the testing criteria, because that is what will drive us as to how we build the technologies, because we want it to fit within the guidelines, and we want it to pass the testing.

Chairman EHLERS. Thank you very much. My time has expired. I want to pursue that a little more later on, with a few other witnesses, but at this time, I recognize the gentlewoman from California, Ms. Millender-McDonald, for five minutes.

Ms. MILLENDER-MCDONALD. Thank you so much, Mr. Chairman.

Mr. Groh, were you saying that because of the lateness or just recently receiving the standards and whatever, you are now just beginning to design or to look into the software or whatever needs to be done, in terms of the testing? I was kind of talking when——

Mr. GROH. No, my question was in regards to the human factors element, or human interface, and the ease of human interface, or as Chairman Ehlers put out earlier, the intuitiveness that would be there. And as technology evolves, there is new technology that is available today, our cell phones that we have in our pockets today, from five years ago are——

Ms. MILLENDER-MCDONALD. Okay.

Mr. GROH.—greatly different, as are voting technologies or voting systems.

What we focused on initially was the accessibility component of the 2002 and the HAVA requirements, because they were known. The accessibility and human factors component was not completed in time for us really to effectively apply those——

Ms. MILLENDER-MCDONALD. Okay. That is what I heard.

Mr. GROH.—in this timeframe.

Ms. MILLENDER-MCDONALD. All right. Very well. Thank you so much.

SECURITY IN ELECTRONIC VOTING

What we have heard from all of you, or what I have heard from all of you, is security. That is one of the words I have heard from each of you, security, and in hearing that, it is extremely important, as Ms. Lamone said, about security is a big factor with the people whom we all serve, and with those voters who are out there, who is depending upon voting machines, or whatever the methodology is, to have security in their voting.

Given all of this, we are also hearing from Dr. Wagner, who said, and I am just underscoring all of these different things that I am hearing, the state of electronic voting security is not good. He states that, and yet, Dr. Jeffrey, you were said to state that the testing labs that you have begun to do, or have successfully been

done, seem to have been, or working toward some successful conclusions.

What can we do, each of you, to ensure that security is foremost in our voting system? Voters are very concerned that their vote is not being counted, and that is why they want a paper trail, so that they can ensure at least some methodology of security of their voting. Will you each answer to me, and to us, why is it that Dr. Wagner says the electronic voting security is not good, and he also said that it seems that the federal standards are no long applicable, and I might be putting some words in your mouth, but if you can each respond to that?

In conclusion, Ms. Lamone stated that there are four prongs to this whole notion of voluntary voting standards, and the whole notion of voting period. And one is that of people. And my recent legislation is putting more money into the till for, to train more poll workers to be well trained for upcoming elections, because we do find that the average voting age poll worker is 72, and that the training has been very ineffective and inefficient.

Will you please speak to the security part of this, and if, by Dr. Wagner's assessment that the federal standards are out of whack, or not working, then what are we going to do in terms of security?

Dr. JEFFREY. Well, thank you very much.

Ms. MILLENDER-MCDONALD. Throw it out there, and whichever one falls——

Dr. JEFFREY. Okay.

Ms. MILLENDER-MCDONALD.—we will hear from one or the other.

Dr. JEFFREY. Let me start, and clarify a couple points. One is the role of the testing and the accreditation. NIST is actually brand new to this process. Under the *Help America Vote Act,* the accreditation of laboratories, the laboratories that do the independent testing, is completely different, and so, we are on a brand new process. The old accreditation process which was done by NASED, the National Association of State Election Directors. That was a phenomenal process that they put into place, in terms of being run, set up by essentially volunteers within the organization, with minimal resources, and they basically did a yeoman's job of getting the first level of accreditation and testing going.

Under the HAVA, where NIST is now involved in helping to do the accreditation in the labs, we are using a very different process, a much more rigorous process, to initiate that. We have, within NIST, a program called NVLAP, which is, well, I won't bore you with the acronym, but it is an internationally recognized process for having independent testing labs be accredited to have the level of competence to make these kind of tests.

I will give you some examples of some of the differences. Under the NASED, when an independent testing lab was accredited, it was accredited once, and that was good forever. Under NVLAP, they have to be accredited, and once they are accredited annually for the first three years, and then biannually after that. So they have to maintain proof that they are still competent to do that. There are also the people who go do the accreditation are internationally recognized experts in the validation and accreditation of the labs' process. So, there is a series of things that are going on in the testing to change them.

One last point I would like to make on that as well that is different is that just the fact of going from the 2002 standards to, ultimately, the 2007, the clarity and precision in those standards are going to be so improved that right now, there is a lot of ambiguity, which makes testing difficult. That is being fixed. That is one of the things that is specifically being addressed. That will help significantly, and will help minimize a lot of the problems that were mentioned, as well as the open test suite that will be developed for that.

Chairman EHLERS. The gentlewoman's time has expired. If there is further time, we will take further answers to this next. We will have more than one round, I am sure.

But since we have so many, I want to make sure everyone has a chance.

Chairman Boehlert is next, and recognized for five minutes.

VOLUNTARY NATURE OF STANDARDS

Chairman BOEHLERT. I would like to be quite basic, and I look at the title of the hearing: "Will the New Standards and Guidelines Help Prevent Future Problems?" I think what we are all looking for, some way to guarantee the integrity of the system.

And I guess my basic question is, how can standards and guidelines which are voluntary guarantee anything?

Ms. LAMONE. They call them voluntary, but there is not a vendor that is going to sell a viable product in the United States that is not going to have their system tested against them, because most of the states require our voting systems to meet the standards.

So, for the states that don't want to participate, their vendors are going to have met, and had their equipment tested anyway. So, I think focusing on the word voluntary is probably not the right way. You need to see what and how the states are—because I think most of us are going to adhere to them, and I know all the vendors will.

Chairman BOEHLERT. You all agree with that answer? Is that satisfactory for all of you?

Ms. DAVIDSON. You know the other thing I think that we need to remember is we have been working with the players, the counties, the states, so they feel comfortable with those, and the more that they see how useful they are, the more states will join it. And we have over 40 states now that are already in some type of a process with the federal accreditation of the standards.

Chairman BOEHLERT. Well, counsel advises me that what you say is not true. When will the manufacturers start only selling to the standards. They are not doing that now. Mr. Groh.

Mr. GROH. Well, to represent all of the manufacturers, one is public opinion is the strongest approach that drives us, as well as the state election directors and the secretaries of state. I know of no state that does not demand and require that you have gone through a certification, a federal certification process.

Today, the one that exists is under the 2002 Voluntary Voting System Standards. It will soon be upon us that will under a new set of standards and a new set of test procedures. So, for us, as Ms. Lamone mentioned or stated, it is very correct. No way would we be able to sell to any jurisdiction in the United States something

that had not been through the appropriate accreditation and the recognized accreditation process.

Chairman BOEHLERT. Which is inadequate right now, as we all know. And that is why we have got the problems enumerated in Dr. Wagner's testimony. Dr. Wagner, do you agree with what you are hearing?

Dr. WAGNER. Well, I think one problem we have is that even the new 2005 standards have significant shortcomings. And the second problem we have is that there are delays in these standards being adopted. The 2005 standards will not become, will not take effect until 2007, and so, we can expect to see quite a few years delay until this influences the majority of voting systems used in the U.S.

PAPER TRAILS AND MANDATORY AUDITS

Chairman BOEHLERT. Those are years wasted. Let me get right to the heart of another question, and it is brought up the commentary in Dr. Wagner's excellent testimony. And the recommendations are to mandate voter-verified paper records, and mandatory manual audits. Sounds pretty good to me. Anybody care to comment on it? Ms. Kiffmeyer.

Ms. KIFFMEYER. Yes, Mr. Boehlert, without a doubt, even a state such as Minnesota, which has adopted those standards, because they were not ready, we have complied with them, but it is just simply a matter of time until we actually do that.

But you are exactly right, that it is a real issue, and it is more a function of time then it is lack of willingness of either the vendors or the states to comply with them, and I think that is an important recognition.

Chairman BOEHLERT. Come sit in the Congress of the United States and hear some of our colleagues tell us repeatedly we don't want government mandates, this is wrong, and we don't need paper trails, and you have got some of the vendors that are saying the same thing. We don't need paper trails. I kind of think it is we need something that is auditable, that we can check to make sure that, you know, things worked the way they were intended to work.

So, I grant you, we need a little more time, but this is—what about paper trail, what about all these paper trail recommendations? I mean, so many, you embraced them, obviously.

Ms. KIFFMEYER. Absolutely, Chairman Boehlert, without a doubt. Recognizing the reality of the situation we were in today, the option for us was to do the actual, even better than the paper audit trails, to do the actual paper ballots, because the environment we are in right now today gave us that greatest level of security. But even there, Minnesota has chosen to do a source code review. We have chosen to do post-election audits as well, because we want to wrap the whole system.

I mean, it is a system. There are many components, not just the technology, not just the box, but there are the people, those poll workers, a very important part of that aspect as well. And the aggressive training that we are doing in that area as well. The procedures and the aggressiveness of interoffice and working together with the locals, to make sure we have that all wrapped with the procedures and all of those things. And it is a situation that we have wrapped all of that together.

That is what we have chosen to do in Minnesota, and I wish that we were all in that stage right now, but the reality and the facts are that the standards, the implementation and those things are the reality, and I think that most have tried to comply with those realities in the best way they could at this time.

But we are not stopping. This is not the conclusion.

Chairman BOEHLERT. Well, count Ms. Kiffmeyer as for a paper trail. Dr. Wagner, we know you are for it, because you recommended it. Ms. Davidson, yes or no?

Ms. DAVIDSON. I was Secretary in Colorado when we passed paper trails, and we had an audit of that paper trail, with the machine. So, I can only speak of myself. I am not speaking as an agency, but just so that you know where I really came from.

You know, one thing I would like to add is when we rethink——

Chairman BOEHLERT. Not too quick, because my time is up, but——

Ms. DAVIDSON. Okay. You go ahead.

Chairman BOEHLERT. I just—so, you are for a paper trail. That is three to nothing now. Now, Dr. Jeffrey.

Dr. JEFFREY. As a representative of the TGDC, we put in the guidelines specifically for technical hardware. We don't make policy calls, in terms of what should be implemented, but if one does implement the paper trails, we put in the guidelines to help ensure that they will meet the levels of security and accessibility and openness. But we defer to the EAC for the policy calls.

Chairman BOEHLERT. So, I could have said, that is the official answer, but let us get the answer as a citizen. The citizen Jeffrey, rather than the head of——

Chairman EHLERS. The gentleman's time has expired.

Chairman BOEHLERT. Oh, boy oh boy. Did he tell you one on that one.

Dr. JEFFREY. Fellow physicists.

Chairman EHLERS. Yes. Okay. The next is the Ranking Member of the Science Committee, and I believe he has left, so next in line is Ms. Hooley, the gentlewoman from Oregon.

Ms. HOOLEY. Thank you, Mr. Chair. I am one of these people that, having talked to a lot of people in my district, they really care about the integrity of the election system, and want to make sure that there is some way to go back and verify and recheck and make sure that their vote counted.

ROLE OF EAC

I have a lot of questions. I am going to direct most of my questions to Ms. Davidson. The EAC collects data on how systems perform in actual elections. For example, do you collect information on failure rates and other problems? If so, how is this information used to improve standards? There have been several incidents of security, reliability, and usability flaws discovered in the independent testing authority approved voting equipment, either during elections, or during state certification. When flaws are uncovered, what is the process for ensuring that the same mistakes are not repeated in the future? This is a multipart question I am asking you. Has the EAC published any report or analysis on how or why flaws were not discovered during inspection and testing?

The premier professional organization for computing professionals, the Association of Computing Machinery, surveyed their members about evoting technology; 95 percent of respondents voted for a position endorsing voter-verified paper records, and expressing concerns about paperless voting technologies. If the computer scientists are concerned about security and reliability of voting machines, and recommend that all voting systems produce a voter-verified paper record that can be audited, why hasn't the EAC taken a stronger position?

Ms. DAVIDSON. Okay, let me see if I can start.

Ms. HOOLEY. Remember all of those.

Ms. DAVIDSON. No, I am sure I won't. And you are certainly welcome to help me——

Ms. HOOLEY. Right.

Ms. DAVIDSON.—with the questions. You know, first of all, our process of taking over the certification process from NASED is beginning Monday morning. This will be the first time that the Federal Government has had anything to do with the certification process. So that is number one.

And yes, we do intend to go out and review any type of problem that is in the field, whether it is a mechanical problem, just an error by a judge or somebody that programmed the equipment. To really look into what kind of the issues they are, and keep a record of what the issues are out there. We do not know, and I am sad to say, we do not have any background at all, and we have not given any written documents saying what——

Ms. HOOLEY. Okay.

Ms. DAVIDSON.What those scenarios are, because we don't have any way of even capturing that right now. But that is part of our process that will be in place as we get certifications that come from NVLAP to us before we certify the independent test authorities.

But in the process, obviously, we have decertifying for the first time. We have never had a decertifying process before, and this type of process. So, the decertifying will be very important. If there is a system that is not working, and it is failing, one, we can notify all of the states that have that equipment. We are asking for all of the vendors to tell us exactly what they have in every state, so that we have a record of each individual type of equipment being used in every jurisdiction of the United States.

So, that will start our information, and knowing what is going on. You know, there are a lot of other questions that go in there, that you have asked.

Ms. HOOLEY. But it is not very long until the election of 2006. I mean, that is right around the corner in a couple of months. So, I am concerned about this next election, and what happens, and what happens when you have a machine that goes down during the election. I know that the election workers know how to help a person redo their ballot, but I will give them some assistance, but what happens if you have a breakdown of the equipment during an election?

I mean, how do we know what is going to happen? And then, again, the last question was will the EAC take a stronger position on some kind of a paper verification system?

Ms. DAVIDSON. Okay. First of all, the first one that you asked is what are we going to do before the 2006 election.

Ms. HOOLEY. Right.

Ms. DAVIDSON. Obviously. Part of the certification requires that if equipment goes down, that the information on the machine—the votes on them—are able to be taken and retrieved. So, that is part of the testing. We need to make sure that voters know that if something happens to a piece of equipment, that information is still there, and is available to go into the count at the end of the night.

The other thing is the EAC looked at people asking us to take a strong position on it. The EAC didn't feel we had the authority to take that type of position, because we are only an assistance commission in that area, and we really feel that we have not ever supported any vendor or any type of equipment. There is also testing that is going on currently of what other types of independent tests there are available. So, taking a position on one particular type, would be inappropriate for us to do at this time.

Ms. HOOLEY. Well, I don't think you are talking about one piece of equipment or one vendor, when you say you would support paper verification.

Ms. DAVIDSON. Well, that is true, but knowing——

Ms. HOOLEY. I mean, that is a general principle, as opposed to a specific kind of technology.

Ms. DAVIDSON. You know, I think that what we definitely support is verification. What form of verification is being studied now and the decision must be left up to the states.

Ms. HOOLEY. So, a paper trail or verification is possible with the kind of voting machines that are out there.

Ms. DAVIDSON. That is true.

Ms. HOOLEY. And the state could do that.

Ms. DAVIDSON. That is exactly right, and over 20, I think it is about 26 states have some sort of verification, paper verification, the VVPAT verification in their law right now, or in their rules and regulations. And besides that, they also have an audit mechanism in one way or another.

Ms. HOOLEY. Okay, thank you.

Chairman EHLERS. Next, I am pleased to recognize the father of HAVA, Congressman Ney from Ohio, who guided the bill through all the shoals and difficulties and the sharks, I might add, of the Congress, and managed to get the bill passed. I am pleased to recognize him for five minutes.

Mr. NEY. The child has been well behaved, but it has gotten a little older, so we have to judge whether it is unruly or not at this time, so—I want to, just to ask for some quick answers, because I have got a few things to go through, if we can.

DR. WAGNER'S STUDY

Dr. Wagner, I was interested, when you said about that you had looked at what the testing board did, and you found some things they didn't uncover. Do you have something available on that you can give us as a committee?

Dr. WAGNER. Certainly. I would be pleased to provide you with a copy of the report that we wrote. The report is publicly available.

Mr. NEY. Thank you. Have you went back to the testing board to say look, how did you miss this, or——

Dr. WAGNER. The tests, I have not gone back to the testing labs. The testing labs have a relationship with the vendor, not with outsiders.

Mr. NEY. Or the EAC. Does the testing lab have any relationship with the EAC?

Ms. DAVIDSON. The test lab will have a relationship with the EAC, and we are setting up the procedures right now of what the test labs will make public information, and——

Mr. NEY. So, you will be able to go back and say, look, Dr. Wagner did this study. Here is what he says, and what do you say about that? And that will—that would be, I think, would be a good counterbalance and check on the system. You will be able to do that?

Ms. DAVIDSON. We will be able to do that in the future.

EAC'S GUIDELINES TO STATES

Mr. NEY. Okay. The question I had, Commissioner Davidson, and thank you for the job you do on the EAC, the guidelines were delayed for 24 months, and as Ms. Lamone said, some won't be, the voting systems won't be tested, I guess the 2005 guidelines won't be done until 2010.

So, what would the EAC be doing in the interim to help make decisions with states to assist them on what they are going to do about their voting systems? Are there any plans for that?

Ms. DAVIDSON. The first thing we did was a gap analysis in July of 2005, to make sure that the states met the HAVA requirements. Then, at that time, we adopted the VVSG in December of 2005. We looked at the timeframe, and decided to follow what the FEC had done with the 2002 Guidelines, and create the two-year gap, which allows the vendors time to produce what is required in the standards, and it allows the states to change their laws and procedures, because a lot of our states only have legislation every two years. So, that was the process we took.

Mr. NEY. I had a question, actually, anybody else that would want to, but Ms. Kiffmeyer, Ms. Lamone, Mr. Groh, and Dr. Wagner. Do you think the 2005 Voting System Guidelines are an improvement over the previous voting standards, and do you have ideas, maybe not for today, my time won't allow it, but ideas how they could be improved? But basically, do you think they are an improvement over previous voting standards or not? Dr. Jeffrey, I didn't mean to exclude you too, if you want to.

Dr. WAGNER. I will start. I think they are definitely an improvement. They are a good start. There is a long way to go. They were drafted over a period of only three months, and that is not really sufficient time to address some of the substantive issues.

Ms. KIFFMEYER. I think in general that is what we would all say. It was a good start. It is not where we want to end up, not where you want us to end up, not where the voters want us to end up, but you have got to start from somewhere, and in the time constraints, it was a step forward.

Dr. JEFFREY. I certainly agree. We actually are working on updates to that. We think that the '05 are improvements over the '02,

but there are clearly issues that we have already identified, that the TGDC is working, include things like security, audit control, new security testing, much of what Dr. Wagner has talked about in his testimony, are issues that we are actively addressing.

PAPER TRAILS

Mr. NEY. Let me just close by saying, you know, when Congressman Hoyer and I began this journey on this bill, and it went to the Senate with Senator Dodd and McConnell and Bond, and over here with Congressman Hoyer and Blunt and others, you know, everybody was alarmed about the cheating, the potential discrepancies, the hanging, the dimpled, and the pregnant chads and all that we knew about. The bill far went beyond that.

Frankly, there wasn't a lot of discussion about a paper trail during those deliberations, and my state does a paper trail. We never said you couldn't. My state does a paper trail, and I know this about voting systems, and as, you know, this hearing. But we tried to make the bill premise easier to vote and harder to cheat.

Again, my state does a paper trail. I think it is something that can be looked at. Frankly, when it was introduced, I have had discussion with Mr. Holt when it was introduced, to have moved at that point in time, I think, would have caused total chaos in the system. If you can go to China and put a card in an ATM and your money is secured, and nobody can hack into that system, we ought to be able to have tests and security, which I think EAC ought to look at in the future, and the final issue of whether we can have a paper trail or not.

Just let me say in conclusion, I want to thank Linda Lamone for her work on this, from its inception, and the job that you did for us to be able to get the bill. Also, there is still $900 million owed to the locals by this Federal Government. We give $5 billion overseas to grow democracies, that is great. Congressman Hoyer and I, and I would hope I would get everybody on both sides of the aisle to try to get that other $900 million to the states for the systems.

Thank you, Mr. Chairman.

Chairman EHLERS. The gentleman's time has expired. Next, I am pleased to recognize a minority Member of the House Administration Committee, and that is the gentlewoman from California, Ms. Lofgren.

Ms. LOFGREN. Thank you, Mr. Chairman.

And I think this is an important hearing, and certainly, there is nothing really more important that goes just to the essence of our democracy than making sure that every vote that is cast is counted accurately. And the concern that exists, that that is not happening, is just devastating for a vigorous democracy. So, I think one of the most important things that we can do here, in Congress and with our partners in state and local government, is to make sure that every American knows that this is all on the up and up, and then, as I think the chairman or someone said, you know, you can win or lose an election, and if you know it was fair, you can deal with that, but if you think there was something unsavory or corrupt, it is a disaster for our country.

So, having said that, I know that we are going to have a hearing on the paper trail issue. I am so glad that we are. It has been a

long time coming, and I think it is very important that we do that. I won't dwell on that, as a consequence today, but I am interested, Dr. Wagner, in your comments. You mentioned, and because I am from California, I am aware that the testing that we have done there is more vigorous than has been required, and that we found, with that higher level of testing, there is a very high failure rate, 20 percent or so. I mean, you know, or a quarter that fails.

The thing—that is not good, it is not acceptable, but one thing about it is that if it fails, it fails in a kind of unbiased way. That is different than the concern about someone hacking a system, or intentionally skewing the outcome of an election through hacking or a virus or a Trojan, for example, if you were able to manipulate the outcome of a vote in that way.

Do you have concerns about that latter issue, or is it just about the reliability of systems overall?

Dr. WAGNER. Well, I have concerns both about the reliability, as well as the potential for deliberate fraud. You are right. I have high praise for the State of California. I think if every other state followed California's lead, we would be in a lot better position.

There is some potential here, even with unintentional failures, that this could cause biases. For instance, there have been cases where more affluent areas have had higher technology voting systems, and so, if there is some correlation between——

Ms. LOFGREN. Right. Right.

Dr. WAGNER.—then that could potentially influence the results. But I am also concerned about the integrity of the elections and protection against deliberate fraud, and I think there are some serious issues there as well. And we have a long way to go to bring the testing up to snuff.

Ms. LOFGREN. Have you taken a look at—there are some who have talked to me, from—I come from Silicon Valley, and this is a high interest item in the Valley, people in the technology industry and computer scientists, who suggested to me that even the California systems are susceptible to viruses or to hacking today. Do you believe that is correct, and if it is, what, if you were sitting in my seat, what would you do about it?

Dr. WAGNER. Well, we should recognize that none of the voting systems are perfect, and they never will be. And it is true that some of the California systems have some, are not perfect either, but the State of California has gone a long way in instituting rigorous use procedures, procedural mitigations to make up for problems in the technology, and I have confidence in the California equipment, as a result of that. We have to recognize that places a heavy burden on our poll workers and our election administrators. This is very complex and not easy.

VOLUNTARY OR MANDATED INDEPENDENT TESTING LABS

Ms. LOFGREN. Would you recommend that the—right now, we have these independent testing labs that really don't report out publicly, and are not transparent, in my judgment, in the way that the California system is. Would you suggest that a system similar to California for testing be either suggested or mandated, for the states and localities, and that the results of testing of systems be made public?

Dr. WAGNER. I think California has got a pretty good story on reliability, and if we adopted California's reliability tests at the federal level, that would go a long way on reliability. On security, the issue is very much still up in the air. There is a lot of challenges there, to make sure that we can have confidence in the software. So, I think that is one we still have to work out.

Ms. LOFGREN. Let me ask Mr. Skall, you are the technical expert, I understand, from NIST. Do you agree with Dr. Wagner, or do you have differences that you would like to bring to our attention?

Mr. SKALL. No, I think he is absolutely correct. Computer systems in general, you can never have 100 percent assurance they will work correctly. What you do through testing is increase your level of assurance, and we are working through tests, and coming up with more specific requirements, to increase our level that they work correctly.

And as far as public availability of test reports, I think most people would agree that would certainly improve the process. That is something we have discussed within the TGDC, and something we have discussed with the EAC, and it looks like that is one of the things that will be recommended in the near future.

Ms. LOFGREN. Thank you. I see my time has expired, Mr. Chairman.

Chairman EHLERS. The gentlewoman's time, indeed, has expired. Let me just take just a moment to enter into the record two items that appeared recently in the press, not that these are the most excellent articles, but they certainly illustrate the concerns.

And it is a June 7 article from *Roll Call* by Mr. Ornstein, and a May 30 article in the *Washington Post* by Mr. Goldfarb. Without objection, those will be placed in the record.

[The information follows:]

Forget Flag Burning. Tackle the Real Issues, Like Voting Machines
By Norman J. Ornstein
Roll Call
Publication Date: June 7, 2006

For those of us who are fiercely protective of Congress' prerogatives--and the responses I've received to my column on the raid of Rep. William Jefferson's (D-La.) office suggest we are in the minority--it is still hard to defend the current operators of the Congressional franchise.

This month, the Senate is embarrassing itself, and the rest of us, by dropping any real focus on the immediate issues facing the country at home and abroad to waste weeks of precious and limited floor time on the diversions (doomed diversions, at that) of banning same-sex marriage and flag burning. Can anyone say with a straight face that these issues are more urgent than energy, health care, the budget deficit, homeland security, pensions, hurricane preparedness, the war in Iraq or the balance between fighting terror and protecting civil liberties?

There is no flag burning or flag desecration crisis. Actually, there is no flag burning. As for the issue of marriage, it is being handled by the states--and if it turns out that states' actions or those of judges move in a direction that defies popular opinion, there is ample time to focus on an enhanced federal role then.

Of course, the debate on these two constitutional amendments is a charade; nobody believes they will pass the Senate. But there's a cost in precious time and the reinforcement of cynicism about the seriousness of Congress.

Even worse is the fact that the House leaders' reaction to the Jefferson raid represents the only time they recently have shown an interest in Congressional integrity or responsibilities. Where is the oversight? We remain on course for the House to be in session for the fewest days in our lifetimes, and that means not just a shrunken amount of floor debate or action but also fewer committee meetings and dwindling attention to the myriad problems facing the country.

Here is one issue that is crying out for Congressional focus: election procedure and reform.

Congress responded to the election crisis in 2000, albeit belatedly, with the first major federal intervention in elections: the Help America Vote Act. It was a major accomplishment, but huge problems remain in the election system, and new ones have emerged in the aftermath of HAVA. And none of the people who wrote HAVA have shown the slightest interest in addressing them.

I don't want to get into the underbrush here. Instead, let me focus on the biggest flashpoint: voting machines. Chances are, anybody reading this column also reads widely about politics and knows about the multiple problems and controversies here. States and localities have moved to fulfill HAVA's mandate, using federal money, to update their voting machines and make sure there will be no more hanging chads or questions of election outcomes because of faulty, outdated or rigged machines, or monstrosities such as butterfly ballots.

But the process has backfired because of the unintended consequences of the (well-intentioned) move to expensive modern electronic machines, mostly of the touch-screen variety. These are known as direct-recording electronic systems.

As the DREs expanded in use, computer experts began to uncover security vulnerabilities. The more experts have focused on the machines, the more vulnerabilities they have found. The more they have pointed out the problems, the more the companies that make the machines have brushed aside complaints or stonewalled about the problems.

Then, with suspicions raised, another issue arose--the fact that most of the DRE systems purchased by election districts come without a paper trail, making recounts questionable and adding to the distrust many feel about the machines. Many jurisdictions are now moving to equip their DREs with paper trails, but doing so is very expensive, and HAVA has not provided additional money for it.

Many jurisdictions have decided to move in another direction: the less expensive optical-scan systems that use paper ballots, in which voters mark their choices by filling in ovals or other shapes, and then the ballots are read by optical scanners. Optical-scan machines have many advantages, but they also have problems--unintentional undervotes, voter error, questionable results (where the ovals are not completely filled in or are ambiguous), printing errors and limited access for handicapped voters.

There is no perfect answer here. There are real questions about how vulnerable the machines really are to tampering, and we cannot forget that disasters have occurred in the past with punch cards, lever machines and other older technology. The debate is vigorous and widespread among academic and election experts. But it is virtually nonexistent in Congress.

This is not a small problem. We survived a crisis of confidence in governance in 2000 with no disastrous effects. Despite the controversies, most Americans accepted the outcome of the election. But things have deteriorated seriously since then. We have deep political divisions in the country and a continuing prospect of very close elections at all levels. More and more Americans are deeply suspicious about the integrity of the system, and in this combustible environment, the last thing we need is an election in which a substantial proportion of Americans believe the outcome was rigged.

The problems, of course, go beyond the machines. But the machines are pivotal. There may be a solution out there: hybrid machines, in particular the AutoMARK system from Election Systems and Software. These machines have all the advantages of the DREs with the concrete, reassuring presence of an optical-scan paper ballot. Voters can check their ballots physically to make sure the ballot reflects their intentions. They are expensive (about $6,000 per machine), but not much more than the DREs with printer attachments.

Expense should not be the big factor here. We need to move with dispatch to ensure that any future close election is not marred by serious allegations of fraud or misconduct. We can afford the best machines; we cannot afford a systemic crisis. So here is a challenge to Rep. Vernon Ehlers (R-Mich.) and Sen. Trent Lott (R-Miss.), the respective chairmen of the relevant House

and Senate committees: Hold some hearings, quickly, on these issues. Come to a consensus conclusion. Provide the money necessary to make the system work and train the people required to implement it. And do it now, before the inevitable disaster.

Norman J. Ornstein is a resident scholar at AEI.

Debating the Bugs of High-Tech Voting
Test of Software in Machines Renews Security Concerns

By Zachary A. Goldfarb
Special to The Washington Post
Tuesday, May 30, 2006; A15

The already-cantankerous debate over high-tech voting machines, which have been installed in great numbers in recent years, is growing more intense and convoluted as primaries get underway and the midterm election nears.

A coalition of voting rights activists and prominent computer scientists argues that some of the machines are not sufficiently secure against tampering and could result in disputed elections, while voting machine vendors and many election officials say that view is exaggerated.

The latest dispute occurred several weeks ago after it was discovered at a test in Utah that someone with a reasonable knowledge of computer code could gain access to and tamper with the system software on a popular brand of voting machine manufactured by Diebold Election Systems. The developments prompted California and Pennsylvania to send urgent warnings to counties that use Diebold's touch-screen voting systems to take additional steps to secure them.

But the vastly differing assessments of the severity of the problem offered by computer scientists, Diebold and election officials made clear that four years after Congress passed a law to improve the reliability of elections, Americans still lack definitive word on whether the nation's voting machines are secure.

In California, David Jefferson, a computer scientist at Lawrence Livermore National Laboratory who consults with the state on its elections, said he was "stunned when he found out" about the vulnerability identified in the Utah test and agreed with the "frequently expressed opinion that this is the worst vulnerability that we have ever seen."

But Diebold spokesman David Bear said it was a "functionality" that company engineers had built into the voting machines so their software could be easily updated, and it only becomes a vulnerability if an unauthorized person gains unfettered access to the machine, and there are safeguards against that happening.

State officials tried to strike a middle ground. "There certainly are potential security vulnerabilities that have arisen," said Jennifer Kerns, a spokeswoman for California's secretary of state. "But you have to be realistic about it: When you're administrating elections, there's a very low risk of any" tampering.

By passing the 2002 Help America Vote Act and spending more than $2 billion to upgrade voting machines nationwide, Congress hoped to avoid this kind of exchange.

HAVA was a response to the contested 2000 presidential election in Florida, which had brought the use of old punch-card voting machines into focus.

The newer technology, such as touch-screen and optical scan systems, held the promise of making voting more secure, transparent and accessible. But as the new technology was implemented, voting rights activists raised questions about whether vendors had paid enough attention to security. Activists pushed for the use of technology that still provided a paper record.

Many of the criticisms of voting technology were originally dismissed as exaggerations promulgated by partisans displeased with election results. But the criticisms have been viewed with increasing gravity as prominent computer scientists have rallied behind them. Although it has not been shown that an election was compromised by a security flaw, several elections since 2000, including in this year's primaries, have experienced problems with the technology that have delayed results.

The federal Election Assistance Commission, which was created to help states implement HAVA's wide-ranging requirements, says it is in the midst of strengthening the process of federal certification for election systems. States and localities also have their own procedures.

But voter groups have been unimpressed. They have pursued legal action to try to stop states from using the equipment, including in Arizona, California and New Mexico. Activists are also considering suits in Colorado, Florida, Missouri and Pennsylvania.

Unlike many colleagues in his field, Michael I. Shamos, a computer science professor at Carnegie Mellon University who has worked on election issues for about 20 years, has not generally been seen as a friend of the activists.

In 2004, they assailed Maryland's decision to buy Diebold touch-screen machines and asked a court to stop the state from using them. Shamos testified that with a few additional steps, the machines could be used without problem, and the court agreed.

Now, Shamos wonders. He is confident in his testimony and believes most security holes can be plugged. But he wonders whether Diebold cares enough about security and the sanctity of elections.

"There's a broader philosophical question that's been worrying me more and more lately," Shamos said. "What are these companies really doing? They don't seem to have embraced the seriousness with which people in this country take their elections. It's been kind of an adversarial thing where companies want to make profits, and they just haven't spent enough time and energy designing secure systems."

Bear says that is not true, and he repeats a frequent refrain about why the security concerns are overblown: "It's based on the premise that you have some nefarious or evil election official that's willing to commit a felony and break the law."

To which Shamos responds: "You don't want the success or failure of an election to be based on the individual."

© 2006 The Washington Post Company

Chairman EHLERS. Next, I am pleased to recognize the gentleman from Minnesota, Mr. Gutknecht, for five minutes.

Mr. GUTKNECHT. Thank you, Mr. Chairman, and I am going to thank you and Dr. Wagner for your comment you made just a minute ago, and that is that there is no perfect system. I think we have to be careful we don't try to artificially set a standard that is virtually impossible to meet.

VERIFICATION OF VOTER IDENTITY

I also want to call everybody's attention, in just a few minutes, the buzzers are going to go off, and we are going to go over and vote, and in terms of paper trail, and I want everybody here to know that I support the concept of paper trails, but do understand, we are going to vote, and we are going to vote with these little cards, okay, and this little voting card has an embedded computer chip, so that when I put it in the slot, it will know that it is me, or it will know that I or somebody using this card is putting that into the machine that represents me. But it has my picture on it, it has a hologram, and as I say, it has got an embedded computer chip. I want to call your attention to that, because one of my concerns is not so much that our voting machines don't work correctly. I think there is also the element that is of growing concern to some of us, that not only that every vote counts, but only those people who are eligible to vote actually go to the polls, and this is sort of something, I guess, we don't really want to talk about, but making sure that the people who are voting are who they say there are.

And Ms. Kiffmeyer, you know, in Minnesota, we still have a little bit of, we have a little more of a problem, or potential problem; I don't want to say it is a problem, but I have some concern about this, because we have same-day voter registration. We also have the system where people can literally come in and vouch for people at the polls, and so far, there is not a whole lot of evidence that that has been abused, but it is kind of difficult to, you know, say that it couldn't be abused, and what I am concerned about is some kind of verifiable ID system, where you have a photograph and/or something else.

Ms. Kiffmeyer, I wonder if you could talk a little bit about that concern, and I will just leave it open-ended. What are some of your thoughts about that?

Ms. KIFFMEYER. Chairman Ehlers, Chairman Boehlert, and Representative Gutknecht. Certainly, that is the case, as you have stated, in Minnesota. I think integrity, in all aspects of the election system, those entitled to vote get a vote, those who aren't, the system owes it to have integrity in that part. And just as we do in election equipment, we want a provable issue, provable to the standard of a recount in a close election.

It is a transactional load unlike any other, where you separate the voter from the vote, so you need to be sure that both sides of the transaction are very important, both who is voting, in regards to the integrity of that aspect of the system, and also, the counting of the ballots, when that is completed, and to the standard of a recount. And I think those are very important components. I think issues such as the ID, issues such as the voter-verified paper trail, or an actual ballot, those are components of integrity in all aspects

of the election. Those who are guiding the polling place are poll workers, their training, those issues, all of those are certainly very important, and the one you bring up, as well, is something that I think in Minnesota is an area that we need to make some improvements on, to come up to the standards, as other states as well.

Mr. GUTKNECHT. Let me just add one other, go to a different subject, because if I recall correctly, and I hate to sound like a bean counter who has served on the Budget Committee for eight years, but I believe this bill actually authorized $2.3 billion. I have not been here so long that I still think that that is a lot of money.

STATE ROLE IN FEDERAL ELECTIONS

I guess the question I would have for some of the folks who may represent the states—I mean, the integrity of our elections is certainly a federal issue—is an important issue at the federal level, but it is no less important to the states and local units of government, and I am wondering: what do you see as their role in terms of picking up their end of whatever costs there are of buying, acquiring new technology for our elections?

Ms. LAMONE. The costs of complying with HAVA is far more than what Congress has appropriated, and in Maryland, what we have done with the voting system, and anything connected to the voting system, the county must pay half of it by law, and believe me, they have been screaming bloody murder as a result of that, because, as I said, the costs associated not only with the voting units, but all the security procedures, and the multi-layered testing that we do, before, during, and after the election, costs money, and it is very expensive to try and do the California model, because I think California copied me.

Mr. GUTKNECHT. Excellent staff work. Before I go to Ms. Kiffmeyer, the staff tells me that we actually have appropriated $3.0 billion, so anyway. Ms. Kiffmeyer.

Ms. KIFFMEYER. Chairman Ehlers, Chairman Boehlert, and Congressman Gutknecht. In regard to that question, you are right, $3 billion. But I remember when we were having the discussion with HAVA, and that the Federal Government money was really there to close the gap, because there was a tremendous need, and to help get at that, but it was also a very important issue, that we leave it to the states to continue, as they always have been, it has been a state responsibility to take care of elections, and it has usually been a local responsibility, as it is in Minnesota, to pay for that equipment, and it is a cooperative relationship.

But it is a state responsibility, and it always has been, and my concern is that while we appreciate the federal money at this point, and the $3 billion in Minnesota, we were able to use that money, in addition to the five percent match, to totally cover the costs of that election equipment, and some money for licensing, maintenance, training, and some operating money as well, especially in the first three years, and then after that.

But we were able to structure it, and also, the additional money that we used on the state level through my office, in designing systems that will support and reduce the overall cost of elections. So, we worked very hard to stay within that fiscal restraint, and we in the State of Minnesota really want to carry forward that. So, I

would appreciate the additional $900 million, as was originally discussed, to help conclude that on that part of it, but nonetheless, I appreciate your concern, and that $3 billion, but I also respect states' rights.

Mr. GUTKNECHT. Thank you.

Chairman EHLERS. The gentleman's time has expired. Next, we are pleased to recognize the gentleman from Washington, Mr. Baird, for five minutes.

Let me just interject. It appears that votes are going to appear fairly soon, so we are going to—I hope we can wrap this up before the votes, because it is going to take us at least 45 minutes to vote.

So, Mr. Baird, you are recognized for five minutes.

Mr. BAIRD. I thank the Chair.

I want to begin by commending my good friend and colleague, Rush Holt, for his legislation, and I want to thank the many folks who have come here today to express support.

LEGISLATION THAT ADDRESSES VOTING ISSUES

It has been six years since the most contested election in many decades in this country, and my recollection is that the most objective and comprehensive analysis after that election revealed that had all the votes been accurately cast and counted, a different outcome would have resulted.

Six years later, we still have not enacted legislation to prevent that from happening again, and a commonsense bill that would require a paper trail has not been brought to a vote. And I would just have to ask—I do not, for the life of me, understand why, if we truly care about counting people's votes, the majority party has not brought this up so that representatives of the people can exercise the people's will and insist on a paper trail, so that we know our votes are counted fairly.

Having said that, I have a concern about the time it takes to put one of these institutions, or these implementations in place. My concern is this. This Congress passed a law that requires that following the catastrophic event with large losses of numbers of Members of the Congress, we would be required within 49 days to elect new Members to this body. In other words, select candidates, have a primary, have a general election in 49 days.

VOTING SYSTEMS IN CONTEXT OF KATRINA AND EMERGENCY SITUATIONS

From your knowledge of what it takes to train poll workers, implement these systems, verify the systems, distribute the equipment, et cetera, could you tell me if you think that is reasonable, and I would just contextualize that by pointing out that post-Katrina events in Louisiana took them more than six months to have an election, and even then, it was subject to great controversy. So, I would appreciate any insights into that.

Ms. DAVIDSON. I will ask my colleagues to join in. Obviously, what took place in Orlando, I mean, excuse me, in Louisiana was unprecedented. They even had to start building files of their voters. Things like voter registration forms had been destroyed amongst

everything else. So, it did take a long time, and they did a tremendous job in carrying that process through, and having that election.

I think that one of the things that we really need to think about in the process is, it just went right out of my head. So, I will let somebody else go ahead, and then, I will jump——

Ms. KIFFMEYER. Chairman Ehlers, Chairman Boehlert, and Congressman, as well. Your point is very valid. What can we do in 49 days? In Minnesota, we had the tragic death of Senator Wellstone eleven days before election day, but it was already scheduled. But nonetheless, we had to get a new candidate, we had to get names on the ballot, get it done, and we did a hand count of that U.S. Senate race alone, statewide, that night, and had the results by 2:00 a.m. in the morning.

So, I think we as a state feel very confident, but I think one of the best things in regards to HAVA is the requirement of every state to have a central voter registration system. The ability, through technology in this particular area, is very, very helpful in regards to conducting an emergency election, but it also requires a system around that, such as our state has, which is a five deep backup, so that we are able to pull the plug, as we practice routinely, and keep that voter registration system available to us anywhere within the Nation at any time, should that happen.

I think that, again, it is an issue of time, those central voter registration systems. I mean, you can do a paper ballot. There are things that you hand count, and you would still have equal treatment of voters, but having that voter list and all those components will be a challenge, and certainly, I think that our state is ready to do it. I think you might underestimate the ability and the resilience of our country in that kind of catastrophic situation, which could have many things, would I even be here to do that? So we will do that.

Mr. BAIRD. You mean to tell me that you are confident that if a nuclear weapon were detonated in some of our major cities, we could—or several nuclear weapons, we could confidently have a valid election, reflecting the will of the people, within 49 days of that event?

Ms. KIFFMEYER. I think in any circumstance like that, sir, it would be extremely difficult, without a doubt. Absolutely without a doubt. But you have a country that needs to move forward, and we have to do the best we can under those extremely challenging circumstances.

MILITARY PERSONNEL AND VOTING

Ms. DAVIDSON. And I will add, the one thing that I think is one of the biggest problems that we have is our overseas and military that is abroad.

Mr. BAIRD. I was just going to ask that next question.

Ms. DAVIDSON. So, that is one of our biggest areas, and we are doing a study on overseas and military, what states are doing currently, and making sure that they have their right to vote. There is electronic transmittal of those ballots over, and some states require that they mail them back, to make sure that we cut down on that timeframe. Because obviously, time getting ballots over there and back, is running around 40 days, that is what we are told.

STANDARDS FOR FAILURE RATE

Mr. BAIRD. Mr. Chairman, I appreciate the comments. One final question left for me by Mr. Holt that I just want to get on the record, and I don't think there will be time to answer it, is this. He points out that apparently, under the Voluntary Voting System Guidelines, there is an acceptance of a 9.2 percent failure rate of all voting machines used in any 15 hour period. I am curious if that is actually the standard that we have set, a 9.2 percent failure rate, and if that is an acceptable standard, I am very puzzled by that. That is, by the way, far less than an incandescent light bulb.

Mr. SKALL. Yes, that comes from the existing standards, and we are researching right now to actually update that, to make a much more acceptable failure rate.

Mr. BAIRD. Given that many of us have lived or died on less than a percentage point margin in elections, including yours truly, I would kind of like to see a little higher level of reliability.

Mr. SKALL. Yes, we agree.

Chairman EHLERS. The gentleman's time has expired, and I certainly share his feeling that we should. I would just like to point out the issue of the paper trail has come up repeatedly. For those who came here later, we do plan a hearing on that some time in September, but I also wish to point out that a paper trail can also be altered, either mistakenly or intentionally, and I would also remind everyone that—and I am not against a paper trail, I don't want you to misinterpret this, but I would point out that the big problems we had in Florida with the Presidential election also involved paper ballots, and that did not resolve the problem.

Mr. BAIRD. Mr. Chair—if I may.

Chairman EHLERS. No, I want to move on. I don't want to get into a debate. I just wanted to point out we are having a hearing on this later. I also want to point out to Mr. Gutknecht, before he leaves, he brought up a very important point about ensuring that the correct people are voting. We have had one hearing on Mr. Hyde's bill requiring proof of citizenship to register to vote, and a photo ID to vote. We will be conducting hearings throughout the United States in the next month, and so, we expect to get good testimony on that.

With that, we have Mr. Diaz-Balart.

Mr. DIAZ-BALART. Thank you very much, Mr. Chairman.

First, I want to clarify something. Then, I have two questions. Just to clarify something, because a lot of times, things get thrown out there, and they become facts, and they are not. After the election in Florida, a number of media outlets, including the Herald and USA Today and a bunch of others did their own recount, and they all agreed that the result was the same. I just want to make sure that the facts are out, and I would be more than willing to share with anybody who would like to see that.

VULNERABILITIES OF PAPER TRAILS AND FOREIGN INVESTMENT IN VOTING EQUIPMENT

But I have two questions. And I want to thank the chairman and this committee for this hearing, and also, for the hearing that we are going to have on paper trails. You are absolutely right, Mr.

Chairman, that we have had some issues in the past with paper trails. There is no panacea. However, though it doesn't mean that paper trails will make things perfect, obviously, and we have heard some of the possible problems without having the paper trail. Does anybody have any reason to not have paper trails? Can paper trails be worse, if we have them? And I know there is an issue of cost. That is one question.

And secondly, does anybody have any heartburn, or some concerns about the possibility of some of either hardware or software companies being owned by foreign investors, including some who may not have a tradition of favoring the democratic process? And we have read a number of articles about that.

And those are my two questions, and I would like to kind of do them quickly, so we can hopefully get some good answers. Thank you, Mr. Chairman.

Ms. DAVIDSON. Well, on the foreign investors, because of the rigorous process that we are putting into place, each vendor or manufacturer will have to register the people that are involved with their organization, all of the top people. Those will be checked to see if there is anybody that has not been, you know, that is put on record that they cannot do business in the United States. So that is public information. So, we want to make this a more open process than what it has been in the past, because we do feel that the citizens need to be aware of all the issues.

Mr. DIAZ-BALART. Do you—anybody want to add anything to that?

Mr. GROH. Well, and let me take a crack at some of this. As the vendor, it is difficult for me a lot of times to speak up, because I think the most important people at this table in a hierarchy are the Election Assistance Commission, and Commissioner Donetta Davidson has a stellar background, having been a local county election official, Secretary of State, now sitting on that commission brings a depth and wealth of knowledge. And if you go down from the Honorable Mary Kiffmeyer, and Linda Lamone, who has a reputation that excels and exceeds all of her colleagues, they can speak much better to this.

As a vendor community, it is our responsibility and role to meet the standards that we have in front of us. We do not feel, as a vendor community, we should stand up and say we are for or against something. Our challenge and job is to enhance the voting process for all voters, maintain voter confidence, by meeting the standards that are out there, that the ITAs test to.

As far as the ownership component of it, I think if you have good standards, and you have a good testing process, and the decisions are made through an RFP process at the state and county level, it should be for them to determine that. As a company, I am based in Omaha, Nebraska. I am a U.S. based company, but I also want to do business globally in other parts of the world. And my fear is that if I become, you know, constrained to others coming in, and doing business here, and don't allow it, the same is going to happen to me. So, there is a balance that has to be struck, and I think that is through the testing, the certification, the request for proposal, and that evaluation process, and then, people like Mary Kiffmeyer,

who will go through a process that is very rigorous, in determining who they are going to buy from.

Ms. LAMONE. I had asked you your—I guess your first question.

Chairman EHLERS. Is your microphone on?

Ms. LAMONE. I think so, yes. We commissioned a study, the State of Maryland did, with the University of Maryland of Baltimore County, to look at the various verification technologies available, or in prototype. And including the paper trail, and the conclusion of the multiple disciplinarian team was that none of them were ready for primetime, including the paper trail, and I will be happy to leave a copy of the study with the committee. It is on our web site. It is on the University's website, but I think they did a very thorough job, and provided some very valuable information, and we had it done for the policy-makers of the State of Maryland.

Ms. KIFFMEYER. And I would also like to make a statement at this time that it is really about the voters and their confidence in the systems, because we as a system act on their behalf, and I think it is very important in making decisions that it is the citizens and the voters, and their sense, not only on election day, but after election day, in a close recount, that they have confidence.

Mr. DIAZ-BALART. Chairman, I believe I am out of time. I do want to clarify that, to make sure that it was the Opinion Research Center, University of Chicago, conducted a survey in Florida for eight news companies. They examined 99 percent of all the ballots in the 67 counties, and that included the Herald, CNN, and others. I just want to make sure that when things are said, that we stick to the facts. I had a colleague who used to say don't allow the facts to confuse the issue. I want to thank this chairman for never letting that happen. Thank you, sir.

Chairman EHLERS. Well, I appreciate you getting that into the record. I am aware of that. I found it fascinating they spent $150,000 for it, hoping to get a story out of it. The result was headlines on page Z27. But nevertheless, it verified it.

The bells have rung for votes. At least, I assume that is a vote. Yeah, okay. So, this is an opportune time. The other remaining Members have indicated that they would forego their opportunity to question, rather than coming back again at 5:00, when it will take us at least 45 minutes for the series of votes.

Ms. MILLENDER-MCDONALD. Mr. Chairman. May I just ask—okay.

Chairman EHLERS. Just one moment. I just wanted to make one wrap-up comment. We have talked a great deal about standards and security, but I want to make certain that we also recognize that the key item is accuracy. We want to count the votes accurately, and secondly, we don't want any fraud whatsoever, and so, I will be pursuing those issues in the months ahead.

Mr. NEY. Mr. Chairman.

Chairman EHLERS. I—yes, we have a few people who want to make comments. We will first go to the Ranking Member.

Ms. MILLENDER-MCDONALD. Only, Mr. Chairman, that there is a Member on our committee who wishes to raise at least——

Chairman EHLERS. All right.

Ms. MILLENDER-MCDONALD.—a question, and then, perhaps, at least for the record. Mr. Brady.

Chairman EHLERS. All right. All right. I will recognize him in just a moment. Mr. Ney asked——

Mr. NEY. I just want to, without objection, I would like to enter a statement into the record reaffirming Ms. Lamone's statement about including all the considerations of persons who have a form of a disability, if we go down the path of a paper trail.

Chairman EHLERS. Without objection, so ordered.

[The information follows:]

BOB NEY
18TH DISTRICT, OHIO
2438 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515
(202) 225-6265
FAX: (202) 225-3394
E-MAIL: bobney@mail.house.gov
www.ney.house.gov

Congress of the United States
House of Representatives
Washington, DC 20515–3518

COMMITTEES:
HOUSE ADMINISTRATION
FINANCIAL SERVICES
CHAIRMAN, SUBCOMMITTEE ON HOUSING AND COMMUNITY OPPORTUNITY
TRANSPORTATION AND INFRASTRUCTURE
DEPUTY WHIP

Statement on Voting Access for Persons with Disabilities

I was pleased to co-author and see signed into law the Help America Vote Act in 2002. This legislation was crafted to make it easier for everyone, including persons with disabilities, to vote. Specifically, these individuals would be able to enjoy more independence and privacy when casting their vote.

By requiring that every precinct across America have at least one voting mechanism accessible to a person with disabilities by the beginning of this year, the federal government is making strides to provide everyone with the necessary accommodations needed to enjoy one's voting privilege. While strides have been made, continued funding and oversight is needed to ensure that these requirements are continued to be enforced. Voting is a privilege that should not be denied to anyone, especially on the basis of a disability. I look forward to working with my colleagues to ensure that efforts are continued and improvements made.

Bob Ney
Member of Congress

DISTRICT OFFICES:

146A WEST MAIN STREET
SAINT CLAIRSVILLE, OH 43950
(740) 699-2704
FAX: (740) 699-2769
TOLL FREE (VALID IN OHIO ONLY):
(866) 4-OHIO-18

51 EAST SECOND STREET
CHILLICOTHE, OH 45601
(740) 779-1634
FAX: (740) 779-1641

HILTON-FAIRFIELD BUILDING
152 2ND STREET, NE, #200
NEW PHILADELPHIA, OH 44663
(330) 364-6380
FAX: (330) 364-7675

200 BROADWAY
JACKSON, OH 45640
(740) 286-1430
FAX: (740) 286-7630

3808 JAMES COURT
SUITE 4
ZANESVILLE, OH 43702
(740) 452-7023
FAX: (740) 452-7191

PRINTED ON RECYCLED PAPER

And I am now pleased to recognize our final questioner, Mr. Brady, the gentleman from Pennsylvania.

Mr. GREEN. There will be one additional person, if we have time.

POLL WORKERS AND HUMAN ERROR

Mr. BRADY. Thank you, Mr. Chairman. I will be short and brief, so maybe my colleague can also get a question in.

I would just like to commend and thank Ms. Lamone for recognizing our poll workers and our committee people. In the city of Philadelphia, we have 1,700 poll workers, 1,700 polling districts, 17,000 poll workers that do an excellent job. And I often wondered, a lot of times, when they get criticized, what would happen if we called the election off? What would happen if the poll workers didn't get to the machines, didn't get to the polling place, didn't get to the chairs? You can't do nothing to them, three quarters of them are volunteers. The other quarter gets paid less than $100 for 15, 16 hours a day work. Our training there is excellent. They get two or three sessions prior to every election, and they do an excellent job.

So, my issue is this problem is not human. It is not a human problem. It is not a problem with people working when they—or not working. It is a mechanical or an electronic problem that we need to fix. Ironically, in Arizona, I heard today that, on the radio that they are having a lottery for anybody, they are going to put on a referendum on the ballot, that if you do vote, you have a chance to win a million dollars. There is a lottery pick that you get one chance, if you vote once. If you vote twice, you get two chances. So—once in the primary, and once in the general, all I am saying. A lot of you people from Philadelphia, you are talking about voting twice.

VOTER CONFIDENCE AND TURNOUT

But my point is, we are trying to increase voter turnout, and yet, we wind up losing the confidence of the people that do come out, and do come out and vote. We just need to fix this problem. I commend and thank the chairman for having these hearings. Thank you for your input, the information, we are going to need a lot more of it. We do need to have a failsafe, when somebody comes out to vote, that who they vote for, they voted for, and not somebody else, that their vote does count, and we need to instill the confidence back in the American people, and I look forward to being a part of the next set of hearings where we do talk about a paper trail, or whatever we come up with that can fix this problem.

So, thank you, and thank you for your participation.

Chairman EHLERS. And thank you for your comments, and the gentleman from Texas, Mr. Green, wishes to ask a question.

Mr. GREEN. Yes, thank you, Mr. Chairman, and I am honored to be with you, Mr. Chairman, and thank you for holding this hearing, and the Ranking Member as well.

Friends, it is my opinion that we live in a world where it is not enough for things to be right, they must also look right. And to most Americans, it doesn't look right to cast an electronic ballot, and not have some verification that is audible and tangible. They

want to see that their vote was cast properly, and they want a verification process that allows that proper audit to take place.

Most Americans believe that if you can go to a service station, and you can purchase gasoline, and get a receipt on demand at the point of contact, they believe that you should be able to get some sort of tangible evidence of your vote, so that you can place that in some container someplace, in the event there is some malfunction in the electronic process.

This really is not asking too much. It is not a question of will or way, it is a question of will. Do we have the will to abide by the will of the American people? My position is eventually, we will abide by the will of the people. We cannot continue to have elections questioned in this country. This is the greatest country in the world, not because we have tall buildings, but because we have a process by which we can verify the elections that we all honor, and if we lose that faith in our system, we can lose our government.

So, let us stand up for the government. That is what I am going to do, and I am going to vote for some verifiable system that probably will include paper, since I haven't heard anything that—talk of anything that can substitute for paper. In this country, we honor paper. Our IDs are on paper. When we go over and vote today, there will be a paper verification of our votes today. Let us continue to honor paper, and make real the great American ideal of every vote counting and counting every vote.

Thank you, Mr. Chairman.

Chairman EHLERS. I thank the gentleman for his comments. The gentleman from Colorado, did you have anything you wanted to say? Apparently not. I—before we bring the hearing to a close——

Ms. MILLENDER-MCDONALD. There is one other thing.

Chairman EHLERS. Oh, I am sorry. Mr. Udall, yes.

Mr. UDALL. Chairman Ehlers, I appreciate the opportunity just to say a couple of words. I wanted to first acknowledge our former Secretary of State, Donetta Davidson, who is here, and I am going off script a little bit, but I would tell you, as an elected official, she had to identify with one of the major political parties in the State of Colorado, but she was widely respected by both political parties for her sense of fairness and her principles, and her ability to get the job done, and I know she has that reputation nationally.

And if I could, I would like to submit for the record a longer introduction that I intended to make of her as the panel began.

Chairman EHLERS. Without objection, so ordered.

[The prepared statement of Mr. Udall follows:]

PREPARED STATEMENT OF REPRESENTATIVE MARK UDALL

I would like to welcome all of our witnesses and thank the Chairman for the opportunity to introduce one of our witnesses today, Commissioner Donnetta Davidson.

I am pleased that she is joining us for this hearing as she has extensive experience in elections on the local, State, and national level.

Commissioner Davidson started her career with elections as the Clerk and Recorder of Bent County in Colorado and later became Director of Elections for the Colorado Department of State.

Through this position she handled several issues with local elections such as special district and school district elections.

In 1999, while serving as the Clerk and Recorder of Arapahoe County in Colorado, she was appointed by Colorado Governor, Bill Owens as the Colorado Secretary of State.

She was later elected to this position and served four terms.

Commissioner Davidson has served as President to both the National Association of Secretaries of State and the National Association of State Elections Directors.

On a federal level, she served on the Federal Election Commission Advisory Panel. And in 2005 she was unanimously confirmed to her current position as commissioner to the U.S. Election Assistance Commission.

Commissioner Davidson clearly has a wealth of experience with election systems and I am eager to hear your thoughts on this country's efforts to establish standards in our voting machine system.

Commissioner—welcome, and thank you for joining us today.

Mr. UDALL. And I also had a series of questions that I wanted to direct to the panel that they could answer within the time limit that we have defined for them, and I would ask unanimous consent to submit those questions.

Chairman EHLERS. So ordered. And any Member can do that. I will get to that in just a moment.

Mr. UDALL. Thank you, and I will yield back all the time I have remaining.

Chairman EHLERS. The gentleman yields back his time. Before we bring the hearing to a close, I want to thank the witnesses. You have been a superb panel, and I wish we had more time, and I certainly wouldn't mind sitting around a table with you, and just getting into more depth on these issues, and I believe our Ranking Member, Ms. Millender-McDonald, would feel the same way.

This has been a highly educational hearing for everyone here, and I really appreciate your objectivity and your helpfulness in your responses. Many of these issues will be continued through other hearings. I hope that ultimately, we develop as nearly perfect a system as one can develop.

If there is no objection, the record will remain open for additional statements from the Members, and for questions to be submitted by the Members to the panel, and for answers from these followup questions from any members of the panel. So, you may hear from us with some questions. We would appreciate your responses. All of that will be entered into the record.

Without objection, so ordered.

Finally, thank you once again for being such great witnesses. Thank you for your helping us.

The meeting is adjourned.

[Whereupon, at 4:08 p.m., the Committee was adjourned.]

Appendix 1:

Answers to Post-Hearing Questions

ANSWERS TO POST-HEARING QUESTIONS

Responses by Donetta L. Davidson, Commissioner, Election Assistance Commission

INTRODUCTION

Following the hearing and the testimony provided by the witnesses, the U.S. Election Assistance Commission (EAC) feels that it is important to provide some basic information about the history of voting systems, voting system certification and the role of EAC to clarify some misunderstandings or misconceptions that were put forth at the hearing.

Voting system standards and voting system testing are not new concepts. In 1990, the Federal Election Commission (FEC) published the first set of voting system standards (1990 VSS), following a Congressional mandate and feasibility study. These standards were voluntary. States were not required to use systems that met the 1990 VSS. States could adopt the standards by statute or regulation and thereby make them mandatory for voting systems used in the state.

The FEC was not authorized or funded to develop a companion program for testing voting systems to those standards. That testing process was developed and implemented in 1994 by the National Association of State Election Directors (NASED), a trade association of state election directors. This group of volunteers established a testing program, including accrediting laboratories to test voting systems to the voting system standards, a process for review of the reports generated by the laboratories, and a means of assigning and tracking qualification numbers.[1] NASED did not receive federal funding to administer its testing process. In addition to this voluntary national qualification program, states also began developing and implementing their own certification programs in which they reviewed voting systems for conformance with standards established in that state.

In 2002, the FEC adopted a new set of voting system standards (2002 VSS). These standards were also voluntary. They updated and expanded upon the 1990 VSS. At this point, the Federal Government still had not entered the voting system testing arena. NASED continued to qualify voting systems against the 1990 and 2002 VSS. It was not until the *Help America Vote Act of 2002* (HAVA) was passed that the Federal Government was given a role in testing voting systems.

HAVA took several actions with regard to voting systems. First, HAVA required that all voting systems used in elections for federal office meet the requirements of Section 301(a). Specifically, those systems must:

- Allow voters to review and alter a selection prior to casting the ballot;
- Produce a permanent paper record of the election which could be used in an audit or recount;
- Be accessible to individuals with disabilities, allowing them to vote with privacy and independence;
- Provide ballots in languages required by Section 203 of the *Voting Rights Act* in covered jurisdictions; and
- Meet the error rate standard established in the 2002 VSS.

HAVA did not set out a method of determining compliance with these requirements.

Second, HAVA required the EAC to adopt a new set of voting system guidelines.[2] These guidelines were to be voluntary, just as the 1990 and 2002 standards were voluntary. Third, HAVA required the EAC to provide for the testing and certification of voting systems and for the accreditation of laboratories to test those voting systems. Participation by the states in the certification program, like the voting system guidelines, is voluntary. However, states may incorporate this requirement by statute or regulation, thereby making the EAC certification a requirement for voting systems used in the state.

On December 13, 2003, more than a year after the passage of HAVA, the EAC Commissioners were appointed and the agency was established. The EAC embarked on a partnership with the National Institute of Standards and Technology (NIST) to develop a set of testable standards against which voting systems could be measured. In July 2004, the Federal Advisory Committee required by HAVA to work with NIST on the voting system guidelines held its first meeting. The Technical Guidelines Development Committee (TGDC) is a Federal Advisory Committee that

[1] NASED implemented a "qualification" procedure in which voting systems were qualified against the standards developed by the FEC. The term "certification" was reserved for the processes of reviewing voting systems that were conducted by the various states.

[2] The term "guidelines" was used instead of "standards."

consists of 15 members. The membership of the TGDC was dictated by HAVA and includes four technical advisors appointed jointly by NIST and the EAC as well as the representatives of the following organizations:

- EAC Standards Board;
- EAC Board of Advisors;
- Architectural and Transportation Barrier Compliance Board;
- American National Standards Institute (ANSI);
- Institute of Electrical and Electronics Engineers (IEEE); and
- National Association of State Election Directors.

The TGDC and NIST worked over the next nine months to produce a draft set of voting system guidelines. The EAC published the draft guidelines, held hearings in three locations in the U.S. and established a user-friendly and accessible online tool for collecting comments. Comments were accepted for 90 days. During that period, the EAC received more than 6,500 separate comments from the public, academia, industry and the election community. The final version of the 2005 Voluntary Voting System Guidelines (VVSG) was adopted by EAC on December 13, 2005.

At the same time, the EAC and NIST had already begun work on an accreditation program for laboratories that would be used to test voting systems. The EAC and NIST partnered to use the National Voluntary Laboratory Accreditation Program (NVLAP) already in place at NIST to review and accredit laboratories. NIST sought applications from laboratories beginning in July 2005. To date, five applications have been received. Assessments of these laboratories are underway, and NIST anticipates having recommendations on three of the five laboratories by December 2006, with the remainder by Spring of 2007. The EAC has also developed an interim accreditation program to assure that there will be accredited laboratories in place to test modifications to voting systems prior to the upcoming 2006 elections. In addition, the EAC engaged the assistance of an expert on laboratory accreditation to review the laboratories that were previously accredited by NASED against the International Standard Organization's (ISO) protocol for laboratories, ISO 17025. To date, the EAC has accredited one laboratory under its interim accreditation program.

While the EAC focused its efforts on developing a new set of voting system standards and establishing a process for accrediting laboratories, NASED continued to serve the election community by operating its voting system qualification program. On July 24, 2006, the EAC began its certification program. There are two phases to the EAC's voting system certification program. The first focuses on reviewing modifications to voting systems previously qualified by NASED prior to the November 2006 elections. The EAC recognizes that voting system certification is a very technical, complex and time-consuming process. As such, it would be impossible to retest every voting system prior to the November 2006 elections. Knowing that there would be changes and modifications needed to adapt voting systems for the upcoming elections, the EAC developed a process through which modification to voting systems would be provisionally certified based upon a review of the modification and integration testing. These provisional certifications expire in December 2006. At that time, the EAC will have begun the second phase of its voting system certification program.

Phase two of the EAC's program begins a new era in voting system testing and certification. All voting systems will be eligible to apply for EAC certification, regardless of whether the system had previously been qualified by NASED. The process begins with registering of the manufacturer, which includes disclosure of certain business information that will be used to determine if any conflicts of interest exist. Once a manufacturer is registered, the manufacturer will submit its system for testing by one of the EAC accredited laboratories. The laboratory will then provide a testing report to the EAC, where it will be reviewed by a committee of technical experts to assure that the laboratory conducted the proper test and that the voting system conforms to the voting system standards or guidelines. If a voting system successfully passes the testing and review and no conflicts of interest exist, the system will be granted an EAC certification.

In addition to this certification process, the EAC is incorporating two other features into its program: (1) a quality assurance program, and (2) a decertification process. Through its quality assurance program, the EAC will visit and review production of voting systems at the manufacturer's facility to assure that the manufacturer is producing the same system that was certified by the EAC. In addition, the EAC will visit states and local jurisdictions to assure that manufacturers are delivering the same system that was certified by the EAC.

The EAC decertification process will allow knowledgeable individuals such as election officials, technicians, and manufacturers to report instances where they believe voting systems failed to conform to the standards or guidelines. The EAC will investigate the complaints and determine if evidence exists to suggest that a voting system fails to comply with the standards or guidelines. If a system is found to be out of compliance, the EAC will begin the decertification process which will result in decertification if the manufacturer fails to bring all such systems into compliance.

Questions submitted by Chairman Vernon J. Ehlers and Chairman Sherwood L. Boehlert

Q1. In his testimony, Dr. Wagner recommended that the Technical Guidelines Development Committee (TGDC) and the Election Assistance Commission (EAC) take the following actions to improve security and reliability of voting systems. For each recommendation listed below, please answer these questions: Do you agree with the recommendation? If so, what is the EAC doing to implement the recommendation? If not, why not?

A1. In his testimony, Dr. Wagner inaccurately characterized the function of the EAC, the intent of the HAVA, and the current role of the Federal Government in monitoring and reviewing voting systems. Some of Dr. Wagner's suggestions were legitimate. However, they do not take into account several issues such as the authorities vested in the various branches of government, programs or processes that are not operated by the Federal Government, and federal programs currently in place. The EAC has been and will continue to be willing to speak with Dr. Wagner and others to discuss their ideas and inform them of the legal, fiscal, and practical limitations under which the EAC and the system of election administration in this country work. Through the following responses, the EAC will correct the inaccurate statements as well as clarify the misconceptions put forth regarding the method in which elections are administered.

a. Mandate voter-verified paper records and mandatory manual audits.

The EAC received its authorization from Congress regarding its duties, responsibilities and powers. HAVA specifically limited the EAC's power to develop *voluntary* guidelines and guidance for the states. HAVA recognized that the administration of elections is decentralized, being operated by the states and local governments. HAVA did not seek to upset that balance of power and limited the EAC's authority so that this agency would also respect that balance. The EAC was given no regulatory authority, except as it relates to the National Voter Registration Form, and that is the same authority previously held and exercised by the FEC. As such, the EAC is not authorized to mandate voter-verifiable paper audit trails (VVPAT). In addition, VVPAT is not one of the voting system requirements listed in 301(a) of HAVA.

However, recognizing that many states have imposed VVPAT requirements for voting systems used in their states, the EAC, NIST and the TGDC developed testable standards that could be used to evaluate VVPAT components. The VVPAT testing standards were included in the 2005 VVSG. In addition, EAC also recognized that the free market system had developed other forms of independent verification, such as witness systems, cryptographic systems and split processing systems. There are several companies that market witness systems and at least one company that currently markets a cryptographic system. As such, the EAC has charged NIST and TGDC with developing testing standards for these independent verification systems.

In conclusion, the EAC has no authority to mandate VVPAT or any other kind of voting technology. In elections, one size does not fit all. In our decentralized election system, states and counties have countless different types of voting equipment for various reasons, and election officials choose voting equipment that best fits the needs of their respective voters. The EAC believes it is best to continue to allow election officials the freedom to choose from different technologies that offer the same benefits. Mandating VVPAT would possibly stifle the development of technology and the innovation of election administrators throughout the country. In addition, such a requirement does not recognize the ability of the states to choose voting systems and technologies that best serve the needs of their respective voters.

The authority and the decision as to whether to mandate VVPAT rests with Congress. The EAC is poised to provide information from election officials that have used VVPAT and research that NIST has conducted on VVPAT and other independent verification methods.

b. Expand standards from focusing primarily on functionality testing to incorporate technical evaluations of the security, reliability, and usability of voting machines.

Dr. Wagner states "[t]oday, the standards primarily focus on functionality testing, which evaluates whether the machines implement all necessary functionality." This is an inaccurate statement regardless of whether it refers to the 2002 VSS or the 2005 VVSG. Thus, it is not clear as to what Dr. Wagner is suggesting with this recommendation. The 2002 VSS sets forth standards for testing accessibility, reliability and security. Specifically, the 2002 VSS was the first set of standards to establish requirements for voting systems to provide access to both physically and visually disabled individuals. In addition, the 2002 VSS established an error rate against which voting machines are tested as well as other tests to determine whether voting systems will reliably count votes and store results even under extreme conditions.

The 2005 VVSG significantly expand on all three categories of testing which Dr. Wagner says are lacking. Section 7 of the VVSG is devoted exclusively to security requirements, including requirements on the following security topics:

- Access Control
- Physical Security
- Software Security
- Telecommunications and Data Transmission
- Use of Public Communications Networks
- Wireless Communications
- Independent Verification Systems
- Voter Verifiable Paper Audit Trail Requirements

In addition, Section 3 of the VVSG contains the usability and accessibility requirements. These requirements were increased from 29 requirements in 2002 to 120 requirements in 2005. Reliability of voting equipment to count, maintain, and report results accurately continues to be a significant part of the 2005 VVSG as it was in the 2002 VSS. For more information on requirements see the full text of the *VVSG.*

c. Eliminate conflicts of interest in the federal testing process by establishing a new funding process whereby Independent Testing Authorities (ITA) are not paid by the vendors whose systems they are testing.

The process of testing to which Dr. Wagner refers is not a "Federal" testing process. Accordingly, to suggest that there was a conflict of interest in a "Federal" testing process is inaccurate. Testing has been conducted by NASED, a trade association of state election directors. It was neither sanctioned nor funded by the Federal Government.

As for the EAC's voting system certification program, the EAC is not currently authorized by Congress to charge a fee to manufacturers for testing or to redirect such a fee to the voting system testing labs through a contract or other arrangement to procure such testing. For a Federal Government agency to take in and redirect funds, it must have specific authority from Congress, which the EAC does not have. Furthermore, Congress has not authorized the expenditure of federal funds to test privately developed voting systems. Thus, the EAC currently anticipates operating a voting system certification process that will involve the manufacturers paying an *accredited* voting system testing laboratory directly for the services that the laboratory performs in testing that voting system. The accredited laboratory report will then be forwarded to the EAC for a determination of whether certification is warranted. If Congress changes these authorizations or funding, other options will be considered.

d. Reform the federal testing process to make all ITA reports publicly available and documentation and technical package data available to independent technical experts.

Again, Dr. Wagner refers to the prior existence of a "Federal" testing program, when the previous testing program and all testing laboratories were administered exclusively by NASED. Regardless, the EAC has already anticipated the need and legal requirements for additional disclosure of information related to voting system testing. Unlike NASED, the EAC is subject to laws that dictate what information a Federal Government agency can and cannot disclose, including the *Freedom of Information Act* (FOIA), 5 U.S.C. 552 and the *Trade Secrets Act,* 18 U.S.C. 1905. These statutes specifically preclude the release of trade secrets information and privileged or confidential commercial information.

The EAC will abide by the letter and spirit of these laws. Within their constraints, the EAC will make available information contained in testing reports and technical data packages that are legally releasable.

e. Require broader disclosure of voting system source code, at a minimum to independent technical experts under appropriate non-disclosure agreements.

To the extent that source code is a trade secret or confidential or privileged commercial information, the EAC is precluded by FOIA and the *Trade Secrets Act* from releasing that information. However, the EAC has already made provision in its upcoming certification program to have manufacturers submit the final build of the software to an escrow agent. In addition, election officials will be provided with a mechanism to compare the software that they are delivered by the manufacturer against the final build and executable code.

f. Institute a process for collecting, investigating, and acting on data from the field on performance of voting equipment, including a mechanism for interim updates to the standards to reflect newly discovered threats to voting systems.

The EAC has already anticipated a need for collecting, investigating and acting on allegations of system malfunction and nonconformance with the voting system standards. The EAC has included a decertification process in its voting system certification program that will allow informed persons (i.e., election officials, manufacturers, and poll workers) to make complaints of machine malfunction or an instance where they believe that a machine does not conform to the standards to which it has been tested and certified. Each allegation will be investigated and if evidence of nonconformance is discovered, the EAC will begin the process of decertifying the system.

It is important to note, here, that the EAC did not issue or adopt the certifications issued by NASED. Thus, the EAC has no authority to revoke those certifications or to decertify those systems. For systems that have been certified by NASED, such allegations will be considered in any review of that system for EAC certification.

g. Increase the representation of technical experts in computer security on the TGDC.

As has been previously discussed, the Technical Guidelines Development Committee is a Federal Advisory Committee established by the EAC and prescribed by HAVA. The membership of the committee is set forth in Section 221 of HAVA. The committee consists of 15 members, which include:

- The Director of the National Institute of Standards and Technology
- Members of the EAC Standards Board
- Members of the EAC Board of Advisors
- Members of the Architectural and Transportation Barrier Compliance Board
- A representative of the American National Standards Institute
- A representative of the Institute of Electrical and Electronics Engineers
- Two representatives of the National Association of State Election Directors
- Other individuals with technical and scientific expertise relating to voting systems and voting equipment.

Thus, unless Congress changes the legal structure of the TGDC, the EAC is limited in the appointments that it and NIST can make. All but four members of the TGDC are currently dictated by HAVA. The four members who were appointed jointly by the EAC and NIST based upon their technical and scientific expertise are: Dr. Ron Rivest, Professor, Massachusetts Institute of Technology, Department of Electrical Engineering and Computer Science; Ms. Whitney Quesenbery, President, Usability Professionals' Association; Mr. Patrick Gannon, President and CEO, OASIS; and Dr. Daniel Schutzer, Vice President and Director of External Standards and Advanced Technology, e-Citi, CitiGroup.

Q2. In his testimony, Dr. Wagner said that the federal standards process is not working, and that "Federal standards are not sufficient to guarantee that federally-approved voting systems are able to adequately protect the integrity of our elections, either against unintentional failures, or against deliberate tampering." Do you agree with this statement? If so, why, and if not, what is your assessment of the current state of voting equipment in terms of reliability and security?

A2. Dr. Wagner again mistakenly assumes that the Federal Government has been testing voting systems. At the time of the hearing, all voting systems were "qualified" by NASED, a non-government association, that received no funding from the Federal Government. Therefore, it is inaccurate and premature to state that the "Federal process is not working."

The EAC began its voting system certification process on July 24, 2006. The EAC has implemented the first phase of its certification process, which focuses on the need to review modifications prior to the November 2006 elections. The second phase will begin in December 2006 and will include additional processes to assure that the systems that are fielded are the same as the systems that are tested. These processes include screening manufacturers for conflicts of interest, implementing a quality control program that includes site visits to manufacturing facilities and localities that use the systems, and a decertification program to review and act on allegations that a voting system does not conform to standards.

In regards to protecting the integrity of elections, having stringent, thorough voting system guidelines against which voting systems are tested and a testing and certification program are only half of the equation. When voting systems successfully meet the guidelines, they should also be subjected to rigorous testing, evaluation, and implementation at the state level. Many states have already developed thorough state certification programs wherein they test systems for specific capabilities required by state law or according to more stringent standards than those required on a national level. In addition, states should actively participate in the acceptance process to assure that the systems that they buy and receive meet the same requirements as the systems that were tested. Finally, voting systems must be implemented using a thorough management process in which security and access procedures are applied at the locations in which the systems are operated. Those procedures include securing the location where equipment is stored, developing chain of custody for the transport of equipment, and training and protocols for those operating the equipment. The EAC's work in developing management guidelines for election administration will provide states with suggested practices on implementing and managing voting systems. The first of these management guidelines pieces was made available to election officials in June 2006 and others will be distributed before the November elections.

Q3. Will the EAC be providing an incident reporting system for the 2006 election through which election managers can report problems with voting equipment? If so, what will the process be and will the results be made available to the public or to independent technical experts? If not, why not?

A3. In 2004, the EAC collected this data as a part of its Election Day Survey. The information was made available to the public through its report on the *Election Day Survey,* which can be found on the EAC's web site. With the onset of the EAC certification program, this data will be collected through the decertification process of that program. Information on the certification program and processes will also be made available through the EAC web site.

Q4. The 2005 Voluntary Voting Systems Guidelines contain an appendix on independent dual verification systems that could perform the same functions as a voter-verifiable paper audit trail. Is this technology being used in voting systems today or is more research needed to make it operational? What are the advantages and disadvantages of this technology? To what extent are there other technologies that could perform the same function as a voter-verifiable paper audit trail?

A4. There are currently several forms of independent verification other than VVPAT on the market, including witness systems, cryptographic systems, audio verification systems, and split processing systems. There is at least one company that markets each of the alternative independent verification systems. However, there are no standards currently available to test these systems. Thus, the EAC, NIST and the TGDC have made developing testing standards for independent verification systems a priority. The current section on independent verification can be found in Section 7 of the VVSG. This section includes one form of independent verification, specifically VVPAT. The next iteration of the VVSG will include testing methods for alternative forms of independent verification.

Questions submitted by Democratic Members

Q1. Ms. Davidson, there have been several incidents of security, reliability and usability flaws discovered in Independent Testing Authority (ITA) approved voting equipment—either during elections or during state certification. When such flaws are uncovered, what is the process for ensuring that the same mistakes are not repeated in the future? Has the Election Assistance Commission published any report or analysis on who or why flaws were not discovered during inspection and testing?

A1. The ITAs that have previously tested voting systems were administered under the NASED program. When the EAC began its certification program in July 2006, the EAC reviewed the three testing laboratories accredited under the NASED program for interim accreditation by the EAC to serve in the first phase of its certification program. The laboratories were assessed by an expert in the field of voting systems and a certified laboratory reviewer to determine if the laboratories conform to ISO 17025. Of the three laboratories, the EAC has currently granted interim accreditation to one laboratory. In addition, the EAC is working with the National Voluntary Laboratory Accreditation Program (NVLAP) of NIST to review labs for accreditation to test systems under the second phase of the EAC's certification system. NVLAP is also reviewing labs according to the requirements of ISO 17025. In December 2006, NIST expects to have completed reviews of at least two of the five laboratories that have applied to the NVLAP program for accreditation.

Thus, the EAC and NIST are taking steps to assure that the laboratories that test voting systems under the EAC's certification program are qualified and apply the appropriate procedures, processes and tests to assure that voting systems tested in their facilities are adequately reviewed for conformance with the voting system standards.

Q2. Ms. Davidson, several states including California, Florida, and Georgia, appear to have more exacting certification processes than those required by the Election Assistance Commission. For example, California has adopted a "volume testing" of voting machines; machines are voted on as realistically as possible for at least six hours, to ensure that they will actually function on election day. In one case, California discovered that 20 percent of a particular Independent Testing Authority (ITA) approved machine failed this volume testing. Do you see these more extensive tests as evidence that current federal standards and certification processes need to be revised and made more robust? Will the Election Assistance Commission incorporate the more exacting certification processes of these states to revise federal testing standards and conformance tests?

A2. Again, the testing and certification program that has previously been in place to assess voting system conformance was administered by NASED, not the EAC. The EAC has developed testing standards, but is awaiting test suites or testing protocols to be developed by TGDC and NIST. If the technologists at NIST and the member of the TGDC believe that additional volume testing are necessary, we will see that reflected in the testing protocols that will be developed for the testing laboratories to implement when testing each discrete voting system.

State certification programs have existed for many years and many states like California have solid programs that focus on additional requirements of that state's certification program or additional testing in certain areas. The EAC encourages states to continue their work not only in the state certification programs, but also in acceptance testing to assure that they have field voting systems that are accurate and reliable.

Q3. Ms. Davidson, is there any clear mechanism for suspending or revoking the certification of machines with serious defects in the security, reliability, usability, or accessibility of certified when discovered? It is common in other industries to mandate recalls when products are found to have serious security or safety defects. Is this an issue that should be addressed by the Election Assistance Commission and the latest set of standards/guidelines?

A3. The EAC anticipated the need for a decertification process, and it will be implemented in phase two of the EAC's certification program. Informed individuals (i.e., election officials, manufacturers, and poll workers) will be able to report machine malfunctions and instances in which the individual believes a voting system does not conform to the voting system standards to which it has been tested. The reports will be investigated, and where evidence of nonconformance is found, the EAC will begin the process of decertifying the voting system.

It is important to note that decertification will be applied only to systems that have been tested and certified by the EAC. The EAC has not and will not adopt qualifications issued by NASED. Systems that have been previously qualified by NASED will be eligible for testing and certification under the EAC program, just like newly manufactured systems. Because the EAC has not adopted NASED qualifications, it has no authority to revoke those certifications. The EAC can, however, consider allegations of nonconformance in its review of any systems submitted under the EAC certification program.

Q4. Ms. Davidson, the General Accounting Office's June 2006 report identified five states that plan to use the Election Assistance Commission's 2005 guidelines

(Voluntary Voting Systems Guidelines, VVSG) in the 2006 election. How many voting systems have begun testing, completed testing and been certified against the 2005 standards/guidelines (VVSG)? How many systems do you expect to see certification against these standards prior to the 2006 general election?

A4. The EAC has not received any systems to be tested and certified to the 2005 VVSG. Furthermore, the EAC will not be able to accept any systems for such testing and certification until December 2006, when NVLAP has reviewed and recommended qualified laboratories for accreditation to test voting systems to the 2005 VVSG.

Q5. Ms. Davidson, the Election Assistance Commission has now assumed responsibility for certifying voting systems against current national standards/guidelines. This change was intended to improve the consistency and transparency of the certification process. What criteria, steps and personnel are being used by the EAC to certify voting systems for the 2006 elections and is this information available to the public? What qualifications are required of individuals responsible for reviewing certification of test results and recommending EAC's approval for certification?

A5. The EAC has adopted phase one of its certification program, which focuses on testing and certifying modifications to voting systems prior to the November 2006 elections. Information regarding the process for certification under phase one is available on the EAC's web site. Systems submitted with modifications during phase one will be tested to the 2002 VSS, a document which is also available to the public.

In December 2006, the EAC will launch its full certification program. By October 2006, the EAC will publish the details of that program in the *Federal Register* and on its web site for comment by the public. This program will be rigorous and thorough, and one that will include registering manufacturers, assessing manufacturers for conflicts of interest, testing according to the 2002 VSS or 2005 VVSG, quality assurance, as well as decertification, when warranted.

The EAC sought technical reviewers with the following qualifications to staff its review of the testing reports that will be provided by the accredited testing laboratories:

Minimum Qualifications. Candidates for the position must possess the following minimum qualifications:

- Bachelor's degree from an accredited college or university; or equivalent education and experience.
- Demonstrated knowledge of the VVS and/or VVSG.
- Knowledge of computer science and testing, including, but not limited to, software coding conventions, hardware, computer security, and software.
- Excellent written and verbal communication skills.
- No financial, political, or personal conflict of interest.

Preferred Qualifications. The successful candidate should also have outstanding skills and abilities in the following areas:

- At least five (5) years experience in voting software or hardware testing; voting technology development; or some combination of the two.
- Knowledge of election procedures in the United States. Familiarity with laws and procedures governing the election process.
- Knowledge of the legal, accounting, and auditing requirements for elections.
- Knowledge of quality testing, including, but not limited to International Standards Organization (ISO) (particularly ISO 17025 and ISO 9000).
- Experience with software and/or hardware testing methodologies, including, but not limited to, (1) minimum standards for test plans, (2) methods of ding testing, and (3) requirements for testing hardware and software.

Additional Considerations. Successful candidates will be required to demonstrate that they can operate as fair, impartial, and unbiased parties by certifying that they are not subject to conflicts of interest.

These persons make recommendations to the EAC's Executive Director as to which systems should be certified.

Q6. Ms. Davidson, do vendors currently provide election officials with documentation that explain the security features of the systems that they sell and the procedures

that need to been in effect for the election to be secure? If not, is this something that needs to be done?

A6. This is a question for the voting system manufacturers, as these materials would be provided under contractual agreements between themselves and the election jurisdiction purchasing the equipment.

Q7. Ms. Davidson, Dr. Wagner made a number of short-term recommendations based on the Brennan Center report that he believes could improve the security and reliability of voting equipment that will be used this November. These recommendations include routine audits of voter-verified paper records, performing parallel testing of voting machines, adopting procedures for investigating and responding to evidence of fraud or error, and banning voting machines with wireless capabilities. Would you please comment on these suggestions?

A7. In his testimony, Dr. Wagner demonstrated a misunderstanding of HAVA, the role of the EAC, voting systems, and the history of voting system certification in this country. Some of Dr. Wagner's suggestions were legitimate. However, they do not take into account several issues such as the authorities vested in the various branches of government, programs or processes that are not operated by the Federal Government, and federal programs currently in place.

The following are recommendations made by Dr. Wagner:

a. Mandate voter-verified paper records and mandatory manual audits.

The EAC received its authorization from Congress regarding its duties, responsibilities and powers. HAVA specifically limited the EAC's power to develop *voluntary* guidelines and guidance for the states. HAVA recognized that the administration of elections is decentralized, being operated by the states and local governments. HAVA did not seek to upset that balance of power and limited the EAC's authority so that this agency would also respect that balance. The EAC was given no regulatory authority, except as it relates to the National Voter Registration Form, and is the same authority previously held and exercised by the FEC. As such, the EAC is not authorized to mandate voter-verifiable paper audit trails (VVPAT). In addition, VVPAT is not one of the voting system requirements listed in 301(a) of HAVA.

However, recognizing that many states have imposed VVPAT requirements for voting systems used in their states, the EAC, NIST and the TGDC developed testable standards that could be used to evaluate VVPAT components. The VVPAT testing standards were included in the 2005 VVSG. In addition, EAC also recognized that the free market system had developed other forms of independent verification, such as witness systems, cryptographic systems and split processing systems. There are several companies that market witness systems and at least one company that currently markets a cryptographic system. As such, the EAC has charged NIST and TGDC with developing testing standards for these independent verification systems.

In conclusion, the EAC has no authority to mandate VVPAT or any other kind of voting technology. In elections, one size does not fit all. In our decentralized election system, states and counties have countless different types of voting equipment for various reasons, and election officials choose voting equipment that best fits the needs of their respective voters. The EAC believes that it is best to continue to allow election officials the freedom to choose from different technologies that offer the same benefits. Mandating VVPAT would possibly stifle the development of technology and the innovation of election administrators throughout the country. In addition, such a requirement does not recognize the ability of the states to choose voting systems and technologies that best serve the needs of their respective voters.

The authority and the decision as to whether to mandate VVPAT rests with Congress. The EAC is poised to provide information from election officials that have used VVPAT and research that NIST has conducted on VVPAT and other independent verification methods.

b. Expand standards from focusing primarily on functionality testing to incorporate technical evaluations of the security, reliability, and usability of voting machines.

Dr. Wagner states "[t]oday, the standards primarily focus on functionality testing, which evaluates whether the machines implement all necessary functionality." This is an inaccurate statement regardless of whether it refers to the 2002 VSS or the 2005 VVSG. Thus, it is not clear as to what Dr. Wagner is suggesting with this recommendation. The 2002 VSS sets forth standards for testing accessibility, reliability and security. Specifically, the 2002 VSS was the first set of standards to establish requirements for voting systems to provide access to both physically and visually disabled individuals. In addition, the 2002 VSS established an error rate against

which voting machines are tested as well as other tests to determine whether voting systems will reliably count votes and store results even under extreme conditions.

The 2005 VVSG significantly expand on all three categories of testing which Dr. Wagner says are lacking. Section 7 of the VVSG is devoted exclusively to security requirements, including requirements on the following security topics:

- Access Control
- Physical Security
- Software Security
- Telecommunications and Data Transmission
- Use of Public Communications Networks
- Wireless Communications
- Independent Verification Systems
- Voter Verifiable Paper Audit Trail Requirements

In addition, Section 3 of the VVSG contains the usability and accessibility requirements. These requirements were increased from 29 requirements in 2002 to 120 requirements in 2005. Reliability of voting equipment to count, maintain, and report results accurately continues to be a significant part of the 2005 VVSG as it was in the 2002 VSS. For more information on requirements see the full text of the VVSG.

c. Eliminate conflicts of interest in the federal testing process by establishing a new funding process whereby Independent Testing Authorities (ITA) are not paid by the vendors whose systems they are testing.

The process of testing to which Dr. Wagner refers is not a "Federal" testing process. So, to suggest that there was a conflict of interest in a "Federal" testing process is inaccurate. Testing has been conducted by NASED, a trade association of state election directors. It was neither sanctioned nor funded by the Federal Government.

As for the the EAC's voting system certification program, EAC is not currently authorized by Congress to charge a fee to manufacturers for testing or to redirect such a fee to the voting system testing labs through a contract or other arrangement to procure such testing. For a Federal Government agency to take in and redirect funds, it must have specific authority from Congress, which the EAC does not have. Furthermore, Congress has not authorized the expenditure of federal funds to test privately developed voting systems. Thus, the EAC currently anticipates operating a voting system certification process that will involve the manufacturers paying an accredited voting system testing laboratory directly for the services that the laboratory performs in testing that voting system. The report of the accredited laboratory will then be forwarded to the EAC for determination of whether certification is warranted. If Congress changes these authorizations or funding, other options will be considered.

d. Reform the federal testing process to make all ITA reports publicly available and documentation and technical package data available to independent technical experts.

Again, Dr. Wagner refers to the prior existence of a "Federal" testing program, when the previous testing program and all testing laboratories were administered exclusively by NASED. Regardless, the EAC has already anticipated the need and legal requirements for additional disclosure of information related to voting system testing. Unlike NASED, the EAC is subject to laws that dictate what information a Federal Government agency can and cannot disclose, including FOIA and the *Trade Secrets Act,* 18 U.S.C. 1905. These statutes specifically preclude the release of trade secrets information and privileged or confidential commercial information.

The EAC will abide by the letter and spirit of these laws. Within its constraints, the EAC will make available information contained in testing reports and technical data packages that are legally releasable.

e. Require broader disclosure of voting system source code, at a minimum to independent technical experts under appropriate non-disclosure agreements.

To the extent that source code is a trade secret or confidential or privileged commercial information, the EAC is precluded by FOIA and the *Trade Secrets Act* from releasing that information. However, the EAC has already made provision in its upcoming certification program to have manufacturers submit the final build of the software to an escrow agent. In addition, election officials will be provided with a mechanism to compare the software that they are delivered by the manufacturer against the final build and executable code.

f. Institute a process for collecting, investigating, and acting on data from the field on performance of voting equipment, including a mechanism for interim updates to the standards to reflect newly discovered threats to voting systems.

The EAC has already anticipated a need for collecting, investigating and acting on allegations of system malfunction and nonconformance with the voting system standards.

The EAC has included a decertification process in its voting system certification program that will allow informed persons (i.e., election officials, manufacturers, and poll workers) to report machine malfunctions or an instance where they believe that a machine does not conform to the standards to which it has been tested and certified. Each report will be investigated and if evidence of nonconformance is discovered, the EAC will begin the process of decertifying the system.

It is important to note that the EAC did not issue or adopt the certifications issued by NASED. Thus, the EAC has no authority to revoke those certifications or to decertify those systems. For systems that have been certified by NASED, such allegations will be considered in any review of that system for the EAC certification.

g. Increase the representation of technical experts in computer security on the TGDC.

As has been previously discussed, the Technical Guidelines Development Committee, is a Federal Advisory Committee established by the EAC and prescribed by HAVA. The membership of the committee is set forth in Section 221 of HAVA. The committee consists of 15 members, which include:

- The Director of the National Institute of Standards and Technology
- Members of the EAC Standards Board
- Members of the EAC Board of Advisors
- Members of the Architectural and Transportation Barrier Compliance Board
- A representative of the American National Standards Institute
- A representative of the Institute of Electrical and Electronics Engineers
- Two representatives of the National Association of State Election Directors
- Other individuals with technical and scientific expertise relating to voting systems and voting equipment.

Thus, unless Congress changes the legal structure of the TGDC, the EAC is limited in the appointments that it and NIST can make. All but four members of the TGDC are currently dictated by HAVA. The four members who were appointed jointly by the EAC and NIST based upon their technical and scientific expertise are: Dr. Ron Rivest, Professor, Massachusetts Institute of Technology, Department of Electrical Engineering and Computer Science; Ms. Whitney Quesenbery, President, Usability Professionals' Association; Mr. Patrick Gannon, President and CEO, OASIS; and Dr. Daniel Schutzer, Vice President and Director of External Standards and Advanced Technology, e-Citi, CitiGroup.

Q8. Ms. Davidson, Dr. Wagner's testimony outlines problems that we frequently see reported in news articles about problems with voting equipment. In addition to his comments on the current status of voting equipment, he makes a number of longer-term recommendations, many which focus on conformance criteria and testing of voting machines. Would you please comment on these recommendations?

A8. Please see response to question 7.

Q9. Ms. Davidson, as a former Secretary of State, would you discuss steps we can take to assure Americans that elections held in this country are accurate and secure. For example, how would you respond to the issues raised in Dr. Wagner's written testimony about the independent testing authority and conformance testing or reports from several states that have had problems with voting equipment that has been approved by an independent testing authority?

A9. Voting security is a multi-faceted issue that can only be addressed by examining each of the points of potential weakness. Certainly, security in the voting system itself is important. The EAC, NIST, and TGDC have made a good start at developing security standards for the voting equipment. Those standards are not, however, the only factor in the security equation. Election officials must be diligent in policing access to voting systems, programming equipment and equipment that provide results. Physical security of these systems is equally, if not more important, than the processes, hardware and software that protect the voting machine itself. If a bad actor does not have access to the voting system, then it is increasingly difficult to manipulate the results.

The EAC has begun developing a series of suggested practices that will focus on the physical security and administration components of conducting a secure election. The first issue of EAC's management guidelines was issued in June 2006 and was a *Quick Start Guide* for election officials to use as a checklist for accepting, testing, and securing voting systems. A more comprehensive physical security document will be released shortly to augment the initial concepts outlined in the *Quick Start Guide.*

ANSWERS TO POST-HEARING QUESTIONS

Responses by William Jeffrey, Director, National Institute of Standards and Technology

Questions submitted by Chairman Vernon J. Ehlers and Chairman Sherwood L. Boehlert

Q1. In his testimony, Dr. Wagner recommended that the Technical Guidelines Development Committee (TGDC) and the Election Assistance Commission (EAC) take the following actions to improve security and reliability of voting systems. For each recommendation listed below, please answer these questions: Do you agree with the recommendation? If so, what is the TGDC doing to implement the recommendation? If not, why not?

A1. Let me first clarify how the TGDC operates. There are 15 members on the TGDC whose membership is either specified in the HAVA statute or are chosen based upon their expertise. NIST is only allotted one slot on the TGDC as chair. Specific areas for research are determined by majority vote of the TGDC members. The next version of the Voluntary Voting System Guidelines is scheduled for July, 2007. Between now and July, 2007 the TGDC will have several plenary meetings where decisions will be made concerning the content of the July Guideline. Consequently, the decisions to implement any of Dr. Wagner's, or any other, recommendations have not yet been made and will, if appropriate, be debated among the TGDC members. My responses to the specific questions are detailed below:

a. Mandate voter-verified paper records and mandatory manual audits.

I support some form of independent verification (IV). Voter-verified paper records are one form of IV—but not the only form that could be implemented. It should be noted that VVPATs have several disadvantages, especially in terms of usability for voters and election officials, as well as accessibility. NIST is researching other types of IV systems, such as witness systems and cryptographically-based systems that have the potential to provide increased security with a reduced impact on usability and accessibility.

For the VVSG 2007, the TGDC is considering requirements for three or four different IV techniques, including voter-verified paper records. It is important to note that IV by itself will be insufficient. Robust operational procedures (i.e., concepts of operation) must also be implemented which are not technical and thus cannot be specified by the TGDC. These operational procedures must be developed and practiced at the State/local level. Best practices for operations can be captured and promulgated through the EAC and other organizations. However it should be noted that more research is needed generally in the area of independent dual verification (IDV or IV). However, there are some voting systems that utilize this technology and cryptographically-based systems that have the potential to provide increased security with a reduced impact on usability and accessibility.

b. Expand standards from focusing primarily on functionality testing to incorporate technical evaluations of the security, reliability, and usability of voting machines.

I agree with this recommendation. VVSG 2005 incorporated new requirements for the security and usability of voting machines. VVSG 2007 will consider incorporating more detailed and comprehensive requirements for security and usability as well as new requirements for reliability. These VVSG requirements will provide for a comprehensive technical evaluation of these items.

c. Eliminate conflicts of interest in the federal testing process by establishing a new funding process whereby Independent Testing Authorities (ITA) are not paid by the vendors whose systems they are testing.

NIST and the TGDC have discussed various reimbursement models for the ITAs with the Election Assistance Commission (EAC). However, this is a policy issue that is not within the purview of a technical guidelines committee and is ultimately a decision of the EAC.

d. Reform the federal testing process to make all ITA reports publicly available and documentation and technical package data available to independent technical experts.

This is a reasonable recommendation. Making summary reports publicly available is not an uncommon practice. For instance, test reports provided by Telecommunication Certification Bodies (private organizations accredited by ANSI and des-

ignated by the FCC) for equipment subject to the FCC's certification process are retained by the FCC, which makes summary information publicly available. The TGDC will consider specifying the set of testing material that should be made public. There are, however, several legal and policy issues that would need to be addressed prior to implementation. These issues are not under the purview of NIST or the TGDC, but rather the Election Assistance Commission.

e. Require broader disclosure of voting system source code, at a minimum to independent technical experts under appropriate non-disclosure agreements.

Broader disclosure of source code that can be reviewed by experts could increase the probability that errors, particularly security flaws, could be detected earlier. This is, however, a policy and legal issue that would not be appropriate in a technical guidelines document.

f. Institute a process for collecting, investigating, and acting on data from the field on performance of voting equipment, including a mechanism for interim updates to the standards to reflect newly discovered threats to voting systems.

A process for collecting data on performance of voting equipment would be very useful to document newly discovered threats, as well as to detect errors in the voting hardware and/or software. This information could then be used to either modify or generate new technical requirements to mitigate these threats or errors in updates to the guidelines.

g. Increase the representation of technical experts in computer security on the TGDC.

I agree that the TGDC is under-represented with respect to security experts. I am actively encouraging HAVA mandated TGDC organizations to consider security expertise as a qualification for their nominations to fill vacancies on the TGDC.

Q2. In his testimony, Dr. Wagner said that the federal standard process is not working, and that "Federal standards are not sufficient to guarantee that federally-approved voting systems are able to adequately protect the integrity of our elections, either against unintentional failures, or against deliberate tampering." Do you agree with this statement? If so, why, and if not, what is your assessment of the current state of voting equipment in terms of reliability and security.

A2. The new guidelines in VVSG 2005 enhance the security and integrity of voting systems by providing the first guidelines for Voter Verified Paper Audit Trails; requirements for addressing how voting system software is to be distributed; validating the voting system setup; and governing how wireless communications are to be secured. But there is more that needs to be done. Standards are a necessary but not sufficient condition to protect the integrity of our elections. In addition to standards, a comprehensive test suite to help ensure that the voting systems correctly implement the standard is necessary. NIST will begin the development of such a test suite in FY 2007. Additionally, comprehensive procedures for election officials are needed as well. Until all of these components are in place, our ability to guard against failures or tampering will not be as robust as desired.

Q3. How will you know if the Voluntary Voting Systems Guidelines (VVSG) are leading to improvements in voting systems? Are there mechanisms available to the National Institute of Standards and Technology (NIST) or the TGDC to track the performance of voting systems, ensure that standards are effective, and obtain feedback on the performance of the standards themselves? If so, what are these mechanisms? If not, what is needed?

A3. Tracking the effectiveness of security guidelines is especially difficult. The absence of known security breaches does not establish that breaches have not occurred or that they are unlikely to occur in the future. In this area, ongoing scrutiny of security specifications and testing methods is needed. This scrutiny should come from voting officials, national and state testing entities, and the public. Improvements in usability and accessibility, on the other hand, will be much easier to track through analysis of voting trends and from feedback from the community.

Q4. How do the TGDC or NIST plan to address security in the 2007 VVSG? What kinds of security tests are being contemplated and how do the compare to security tests used for computer equipment in other industries? Is security testing different from other types of testing, and if so, how?

A4. The VVSG 2007 will likely contain several chapters with significant security-related material. The security-related material that is under consideration includes: General Requirements; General Design Requirements; Voting Variations, Security & System Integrity; Cryptography; Access Control; Voting System Records Audit; System Integrity Management; System Auditing & Logging; Physical Security;

Usability; Accessibility; Hardware & Software Performance; Workmanship; Archival Requirements; Inter-operability; and Requirements by Voting Activity.

Security tests will include tests of the functionality of security features (such as access controls), reviews of security documentation, including an assessment to determine if security features function together as intended, and open-ended security testing, including penetration testing. These are common types of security testing used in many industries. Security testing is indeed different from other types of testing. In "regular" (or conformance) testing, one simply tests each requirement to ensure it is implemented according to the guideline or standard. Security testing is more difficult. In security testing, you have an unbounded field of possible security threats to address. NIST and the TGDC are researching open-ended testing and other forms of security testing as part of the overall testing strategy to be included in the VVSG 2007.

Q5. Are there any plans to issues advisories on voting equipment that does not meet the 2005 VVSG and subsequent versions? Will NIST be providing an incident reporting system or other feedback system so that lessons learned from testing laboratories can be disseminated to election officials? If so, what will the process be? If not, why not.

A5. Providing information and best practices to the election officials is the responsibility of the Election Assistance Commission.

Q6. The 2005 VVSG contains an appendix on independent dual verification systems that could perform the same functions as a voter-verifiable paper audit trail. Is this technology being used in voting systems today or is more research needed to make it operational? What are the advantages and disadvantages of this technology? To what extent are there other technologies that could perform the same function as a voter-verifiable paper audit trail?

A6. More research is needed generally in the area of independent dual verification (IDV or IV). However, there are some voting systems that utilize this technology. NIST sees voter-verified paper audit trail (VVPAT) as a type of IV system. VVPATs have several disadvantages, especially in terms of usability for voters and election officials, as well as accessibility. NIST is researching other types of IV systems, such as witness systems and cryptographically-based systems that have the potential to provide increased security with a reduced impact on usability and accessibility.

ANSWERS TO POST-HEARING QUESTIONS

Responses by Mary Kiffmeyer, Secretary of State for Minnesota

Questions submitted by Chairman Vernon J. Ehlers and Chairman Sherwood L. Boehlert

Q1. In his testimony, Dr. Wagner recommended that the Technical Guidelines Development Committee (TGDC) and the Election Assistance Commission (EAC) take the following actions to improve security and reliability of voting systems. For each recommendation listed below, please answer these questions: Do you agree with the recommendation? If so, to what extent and how is Minnesota implementing the recommendation? If not, why not?

Q1a. Mandate voter-verified paper records and mandatory manual audits.

A1a. Agree. Minnesota not only requires a voter-verified paper record it requires an actual paper ballot.

Q1b. Expand standards from focusing primarily on functionality testing to incorporate technical evaluations of the security, reliability, and usability of voting machines.

A1b. Agree. Minnesota requires a source code review that assures that the votes are accurately recorded and counted.

Q1c. Eliminate conflicts of interest in the federal testing process by establishing a new funding process whereby Independent Testing Authorities (ITA) are not paid by the vendors whose systems they are testing.

A1c. Disagree. It is like the use of the Underwriters Laboratories to grade consumer products. Even though the manufacturer pays for the testing it does not mean that the system is corrupt.

Q1d. Reform the federal testing process to make all ITA reports publicly available and documentation and technical package data available to independent technical experts.

A1d. Agree with limits. As long as the reports or documentation does not assist persons with malicious activities in mind do not get information that would assist them to do things to affect the recording and tabulating of votes.

Q1e. Require broader disclosure of voting system source code, at a minimum to independent technical experts under appropriate non-disclosure agreements.

A1e. Disagree. The wide distribution of source code could lead to the loss of source code to those who have malicious intents.

Q1f. Institute a process for collecting, investigating, and acting on data from the field on performance of voting equipment, including a mechanism for interim updates to the standards to reflect newly discovered threats to voting systems.

A1f. Agree. The accuracy and the integrity of elections are essential to the process of fair and honest elections. All new methods of ensuring the correct outcome of every election has value.

Q1g. Increase the representation of technical experts in computer security on the TGDC.

A1g. Agree. In the review of our source code there were requirements to have security experts as part of the team reviewing the source code.

Q2. In his testimony, Dr. Wagner said that the federal standards process is not working, and that "Federal standards are not sufficient to guarantee that federally-approved voting systems are able to adequately protect the integrity of our elections, either against unintentional failures, or against deliberate tampering." Do you agree with this statement? If so, why, and if not, what is your assessment of the current state of voting equipment in terms of reliability and security?

A2. The security standards of the 2005 VVSG are not sufficiently comprehensive to ensure security in our election systems. The use of technology for voting increases the risk that security of the voting system will be breached, if proper safeguards are not taken. Wireless components should only be turned on after the polls close and voting is complete or strict security guidelines are developed. Also, a voter-verified paper audit trail should be required in the VVSG to provide assurance that the elections process is being conducted in an accurate and fair manner.

Q3. What are your top three priorities for updates to the 2005 Voluntary Voting Systems Guidelines (VVSG)?

A3. Priorities for updates to the 2005 VVSG include introducing a VVPAT requirement, banning the use of wireless components during elections, and requiring post-election audits of voting systems.

Q4. If the EAC or another organization provided an incident reporting system for the 2006 election through which election managers could systematically report problems with voting equipment, would this be useful to you, and if so, how would you recommend the system be structured?

A4. An incident reporting system for the 2006 election through which election managers could systematically report problems with voting equipment would be an effective tool. In Minnesota, election judges can record any unusual events or any problems on the precinct incident log. On this form, election judges could record any problems with the voting equipment that may have taken place during the election. In terms of an incident reporting system, an effective mechanism would be for the election judges to submit the data recorded on the incident log and submit this to election managers so that voting equipment problems in all precincts are recorded and in one centralized location.

Q5. The 2005 VVSG contains an appendix on independent dual verification systems that could perform the same functions as a voter-verifiable paper audit trail. Is this technology being used in voting systems today or is more research needed to make it operational? What are the advantages and disadvantages of this technology? To what extent are there other technologies that could perform the same function as a voter-verifiable paper audit trail?

A5. Minnesota law does not allow for the use of an independent dual verification system.

Questions submitted by Democratic Members

Q1. Ms. Kiffmeyer, what documentation do your voting system vendors currently provide you that explain the security features of voting systems and the procedures required for your elections to be secure?

A1. Minnesota requires that vendors applying for voting system certification provide recommended procedures for use of the system at Minnesota elections which includes security issues.

Q2. Ms. Kiffmeyer, what additional improvements are needed (if any) voting for the voluntary guidelines and national certification process? Also, what additional steps should the Election Assistance Commission take to support efforts of states and local jurisdictions to acquire and operate accurate, reliable, and secure voting equipment?

A2. The 2005 VVSG and its strength will be tested in the elections this Fall and in elections to come even more so. The guidelines will need to be evaluated after the elections in order to ascertain how the equipment functioned and what, if any, standards need to be improved. One of the main objectives of the VVSG was to create standards by which to guide an effective elections process, and a look into what might still be lacking and how best to remedy the situation will provide both insight and a benefit to all.

Q3. Ms. Kiffmeyer, GAO recently reported that only about 15 percent of jurisdictions collect measures on voting equipment failures. Does your state collect data on voting equipment failures and what have you found from the data you've collected? What are your views on collecting this information on a national basis.

A3. The state collects data on voting equipment incidents at the local level. However, every polling place is required to keep an incident log which is returned to the counties and would include apparent issues of equipment failure. In addition to having a paper ballot system, the counties have machine backups for tallying and the incidents of machine problems are very few and usually rectified immediately on election day.

Minnesota also has a new statute this year to require a post election review of voting equipment including a hand tally to compare to the machine tally results This review will be conducted with a randomly selected number of precincts per county with additional requirements if there are sufficient enough errors found in the counting of results. This information will be collected by the state and posted on the web site.

Elections have been to this point a function of the states and local election officials and the collecting of the information should be kept to the responsibility of state and local election officials.

Q4. Ms. Kiffmeyer, Dr. Wagner made a number of short-term recommendations based on the Brennan Center report that he believes could improve the security and reliability of voting equipment that will be used this November. These recommendations include routine audits of voter-verified paper records, performing parallel testing of voting machines, adopting procedures for investigating and responding to evidence of fraud or error, and banning voting machines with wireless capabilities. Would you please comment on these suggestions?

A4. The short-term recommendations made in the Brennan Center Report are ones that will help improve both security and reliability. Routine audits of voter-verified paper records also provide an additional level of fairness and accuracy in our elections process. Procedures for investigating and responding to evidence of fraud or error are efficient tools necessary to the integrity of the process. In regards to performing parallel testing of voting machines, Minnesota does not require such a test at this time, but may in the future. As there is a valid concern for wireless components being used during voting in the polling place, Minnesota law prohibits wireless functions to take place during voting. In other words, wireless components should only be turned on after the polls close and voting is complete.

Q5. Ms. Kiffmeyer, Dr. Wagner's testimony outlines problems that we frequently see reported in news articles about problems with voting equipment In addition to his comments on the current status of voting equipment, he makes a number of longer-term recommendations, many which focus on conformance criteria and testing of voting machines. Would you please comment on these recommendations?

Q5a. Mandate voter-verified paper records and mandatory manual audits.

A5a. I agree. Minnesota not only requires a voter-verified paper record, it requires an actual paper ballot.

Q5b. Expand standards from focusing primarily on functionality testing to incorporate technical evaluations of the security, reliability, and usability of voting machines.

A5b. I agree. Minnesota requires a source code review that assures that the votes are accurately recorded and counted.

Q5c. Eliminate conflicts of interest in the federal testing process by establishing a new funding process whereby Independent Testing Authorities (ITA) are not paid by the vendors whose systems they are testing.

A5c. I agree as long as the funding is certain and long-term.

Q5d. Reform the federal testing process to make all ITA reports publicly available and documentation and technical package data available to independent technical experts.

A5d. I agree but with limits. As long as the reports or documentation does not assist persons with malicious activities in mind to get information that would assist them to breach security or make it easier to hack and to affect the recording and tabulating of votes.

Q5e. Require broader disclosure of voting system source code, at a minimum to independent technical experts under appropriate non-disclosure agreements.

A5e. I believe that the voting system source code should require security in its distribution as concerns for giving knowledge to those with malicious intents is a risk. Until the security and risk concerns can be addressed, the wide distribution of source code could lead to the loss of source code to those who have malicious intents and thus lead to greater security risk or risk of hacking. That is an ultimate possible unintended consequence. We must act carefully on this matter.

Q5f. Institute a process for collecting, investigating, and acting on data from the field on performance of voting equipment, including a mechanism for interim updates to the standards to reflect newly discovered threats to voting systems.

A5f. I agree. The accuracy and the integrity of elections are essential to the process of fair and honest elections. All new methods of ensuring the correct outcome of every election has value and every effort should be made and funded fully to accomplish that laudable goal.

Q5g. Increase the representation of technical experts in computer security on the TGDC.

A5g. I agree. In the review of our source code there were requirements to have security experts as part of the team reviewing the source code. However, election practitioners especially at the state level should also be in high representation with the technical experts. Security is more than the technological box. It is the sum total of the election system including voter registration.

ANSWERS TO POST-HEARING QUESTIONS

Responses by Linda H. Lamone, Administrator of Elections, Maryland State Board of Elections

As I stated in my testimony, it is important to recognize that the new voting system standards are the first step in an evolution, not a panacea with an immediate and dramatic impact on elections as some observers believe.

Before responding to your questions for the record, I would like to share with you some important information that seems to have been lost in the ongoing debate about voting systems.

First, it is important to understand why jurisdictions chose Direct Recording Electronic (DRE) voting systems in the first place. DRE voting systems are the most accurate voting systems. They eliminate issues of voter intent and over-votes, offer accessible voting to most voters with disabilities, and easily accommodate multiple languages.

One way to measure the accuracy of a voting system is to evaluate the number of voters who cast a ballot but did not record a vote for the highest contest on the ballot (typically President or Governor). In 2000, there were 10,553 voters in Maryland who went to the polls to vote and did not have a vote recorded for President. In 2004, there were 7,541 voters who voted but did not have a vote recorded for President.[1] This represents a *29 percent decrease* in the number of voters who voted but did not record a vote for President. As demonstrated in Maryland and other states, the transition from lever machines, punchcard, and optical scan voting systems to DRE voting systems has translated into *more* voters having their votes counted.[2] This, of course, is the reason for elections—to capture the will of the people.

Second, it is commonly accepted by computer scientists that no voting system can be made 100 percent secure. While security procedures have been standard operating procedures in election administration, it is important to recognize that paper ballots pose an equal—if not greater—security risk than DRE voting systems. Throughout this nation's history, there are countless examples of outright fraud to questionable procedures with paper ballots. While I am not questioning the integrity of elections conducted on paper-based voting systems, it is important to recognize that implementing these systems do not eliminate or even reduce security concerns. Actually, paper-based systems are more vulnerable as there is no special technical knowledge that is required to alter or remove a paper ballot.

Third, although the advocates opposing the use of DRE voting systems are organized and active, they do not represent a majority of voters in Maryland. Earlier this year, I commissioned a public opinion poll to assess what Maryland voters thought of the DRE voting system used in Maryland. Eighty-two percent of the respondents thought their votes on DRE voting systems were counted and recorded accurately, and 76 percent had a favorable opinion about touchscreen voting. Interestingly, 77 percent of the survey respondents were not even aware of the debate about electronic voting. This survey clearly shows that, in Maryland, there is no "crisis of confidence" in the voting system. A copy of the report is enclosed for your information.

Questions submitted by Chairman Vernon J. Ehlers and Chairman Sherwood L. Boehlert

Q1. In his testimony, Dr. Wagner recommended that the Technical Guidelines Development Committee (TGDC) and the Election Assistance Commission (EAC) take the following actions to improve security and reliability of voting systems. For each recommendation listed below, please answer these questions: Do you agree with the recommendation? If so, to what extent and how is Maryland implementing the recommendation? If not, why not?

A1.

---

[1] In 2000, nineteen counties in Maryland used optical scan voting systems, three counties used mechanical lever machines, one used a punchcard voting system, and one used a DRE voting system. In 2004, all twenty-four jurisdictions used a DRE voting system; twenty-three counties used the same DRE, with the remaining jurisdiction using a different DRE. In 2006, all twenty-four jurisdictions will be using the same DRE.

[2] See Stewart, Charles III, "Residual Vote in the 2004 Election," CalTech/MIT Voting Technology Project, February 2005, *http//vote.caltech.edu/media/documents/wps/vtp_wp25.pdf*

- *Mandate voter-verified paper records and mandatory manual audits.*—Because of the extensive pre-election, Election Day, and post-election testing we conduct on the State's voting system and numerous security analyses and resulting security procedures, we are confident that the voting system accurately counts and records votes. For this reason, I do not believe that a voter-verified paper record improves the accuracy of a thoroughly tested voting system.

  Additionally, I am concerned that a mandatory voter-verified paper record would stifle—and likely already has—the development of other independent verification technologies. Last winter, I contracted with two University of Maryland institutions to conduct an independent study on vote verification systems, including voter-verified paper trails. Several of the technologies were very promising and offered audit and verification tools that are not possible with voter-verified paper records. One, for example, could provide the amount of time it takes poll workers to prepare the voting unit for voting. This information could be used to enhance poll worker training and inform the vendor on how the opening process on the voting unit could be improved. Mandating voter-verified paper records would prevent the development and testing of other verification solutions.
- *Expand standards from focusing primarily on functionality testing to incorporate technical evaluations of the security, reliability, and usability of voting machines.*—I agree that all aspects of voting systems should be tested and that testing should extend beyond just functional testing. Although Dr. Wagner states that the current "standards primarily focus on functionality testing," this is not the case. Both the 2002 Voting Systems Standards and the Voluntary Voting System Guidelines (VVSG) incorporate standards for testing accessibility, reliability, and security.
- *Eliminate conflicts of interest in the federal testing process by establishing a new funding process whereby Independent Testing Authorities (ITA) are not paid by the vendors whose systems they are testing.*—The testing process under the National Association of Election Directors, the entity that previously oversaw the testing process, has been conducted with the highest integrity. Although I am open to discussing different federal testing structures, the current testing process is objective, and to suggest that there are conflicts of interest implies that the vendors have influence over the voting system testing process solely because they pay for testing. This is not the case.
- *Reform federal testing process to make all ITA reports publicly available and documentation and technical package data available to independent technical experts.*—With the EAC assuming responsibility for the voting system certification process, more information about voting system testing will be available.
- *Require broader disclosure of voting system source code, at a minimum to independent technical experts under appropriate non-disclosure agreements.*—In the EAC's upcoming certification program, voting system vendors will be required to submit a final software version to an escrow agent and allow election officials to compare the delivered software against the software version on file with the escrow agent. Maryland has previously used NIST's National Software Reference Library to compare the version of the software being used in the State against the version qualified by the National Association of State Election Directors. This comparison has been performed both before and after statewide elections and reassures election officials that no unauthorized software is being used.
- *Institute a process for collecting, investigating, and acting on data from the field on performance of voting equipment, including a mechanism for interim updates to the standards to reflect newly discovered threats to voting systems.*—It is my understanding that the EAC has developed a process to collect and investigate claims that voting systems are not performing appropriately and are not in compliance with voting system standards, and I support this effort. It is important that the EAC serve as both a resource to election officials for investigating potential voting system malfunctions and noncompliance with standards and, if necessary, initiating a decertification system if the allegations are substantiated.
- *Increase representation of technical experts in computer security on the TGDC.*—Four of the fifteen—or 25 percent—of the TGDC's current members are technical experts. (Election officials currently hold four seats on the TGDC, the same number as technical experts.) Increasing the number of tech-

nical experts at the expense of other subject matter experts would not reflect the realities of voting systems and elections administration and would alter the balance that currently exists on the TGDC. While technical experts play an important role in improving election administration, they are but one voice in the debate.

Q2. In his testimony, Dr. Wagner said that the federal standards process is not working, and that "Federal standards are not sufficient to guarantee that federally-approved voting systems are able to adequately protect the integrity of our elections, either against unintentional failures, or against deliberate tampering." Do you agree with this statement? If so, why, and if not, what is your assessment of the current state of voting equipment in terms of reliability and security?

A2. As the VVSG are not yet in effect nor being used for testing and the EAC has only just started its work in accrediting testing laboratories, I do not believe that the decision can be made that the federal standards process does not work. As I noted earlier, the voting system standard process is an evolution, and no one should have expected that the VVSG was going to improve dramatically and immediately voting systems and the testing process. It is important to give the current VVSG and future versions time to impact voting systems.

While I think the VVSG and new testing structure will improve voting systems over time, I believe that the current voting systems are reliable and secure with appropriate security policies and procedures in place. Like any information technology system, the security of the system is more than just the hardware and software; it includes the people that work with the system and the procedures that surround the system. Best practices and management standards can be shared among election officials to improve the security of voting systems.

Q3. What are your top three priorities for updated to the 2005 Voluntary Voting System Guidelines (VVSG)?

A3. As the VVSG are not yet in effect nor being used for testing and the EAC has only just started its work in accrediting testing laboratories, it is important to give both the VVSG and the EAC time to work before making significant recommendations. That being said, I recommend that future versions of the VVSG include state-specific certification requirements. This would enable state election officials could accept the EAC's certification as the basis of state certification. This joint certification would reduce the resources needed to conduct state certification without a reduction in confidence in the voting system and would greatly benefits states with less financial resources for testing. Incorporating a joint certification could also provide an additional incentive for states to adopt the VVSG.

The EAC has contracted with two experienced and well-respected election officials to develop management standards. While these management standards will cover many topics related to elections management, they will also focus on standards for voting systems. I believe that this effort has enormous potential to improve election administration and the security of voting systems. I also believe tha the EAC could provide much needed assistance to states and counties by offering best practices and assistance in negotiating contracts with voting system vendors.

Q4. If the EAC or another organization provided an incident reporting system for the 2006 election through which election managers could systematically report problems with voting equipment, would this be useful to you, and if so, how would you recommend the system be structured?

A4. Maryland collects information on reported voting system malfunctions from a variety of sources: (poll workers, voting unit technicians, State and local election officials, and vendor's help desk). Either county or State election officials follow-up on the information and determine the root cause of the problem.

A 2004 analysis of voting units from Maryland's largest jurisdiction showed that many of the voting units flagged by election officials and poll workers as requiring special attention or review were voting units that did not have the power cord properly inserted, causing the internal battery to drain, and the voting unit to eventually lose power, physical damage to the voting unit booths (which may include issues such as broken legs or cases); any voting unit that has substantially fewer ballots cast on it than others in the same precinct; or any other reason that an election judge or local election board staff member feels the voting unit needs to be analyzed, either because a problem was observed or reported by a voter. After careful review of all of the voting units referred for additional analysis, State election officials found that only .4 percent of that county's voting units had issues on Election Day.

I believe that it is important to collect this information at the national level to assist election officials with identify summon concerns and work collaboratively to address any issues. As with any national survey and the resulting conclusions based on the data, it is important that there are standard and clear definitions and that the data is used to improve the voting process, not for criticizing election officials or a specific vendor, and that election officials have time to conduct an initial review of the reported voting system malfunctions. For obvious reasons, a voting unit with a broken leg must be recorded and analyzed differently than a voting unit that freezes during voting hours. The EAC has a similar belief as it has developed a process to collect and investigate allegations of malfunctioning voting systems and systems that are in compliance with voting system standards.

Q5. The 2005 VVSG contains an appendix on independent dual verification systems could perform the same functions as a voter-verifiable paper audit trail Is this technology being used in voting systems today or is more research needed to make it operational? What are the advantages and disadvantages of this technology? To what extent are there other technologies that could perform the same function as a voter-verifiable paper audit trail?

A5. As I noted earlier, two University of Maryland institutions conducted an independent technical and usability study on four vote verification systems. The systems included in the study were VoteHere's Sentinel, SCYTL's Pnyx.DRE, MIT Professor Ted Selker's voter-verified audio audit trail, and Diebold Election Systems, Inc.'s voter-verified paper audit trail. A copy of the combined report is enclosed for your information.

The study found that none of the vote verification systems—including voter-verified paper trail—are fully developed and that implementing any one of the systems would greatly increase the complexity of the election and, as implemented in Maryland, jeopardize the secrecy of the ballot. That being said, the researchers found that each of the systems *could* provide some level of vote verification if the system was fully developed, fully integrated with the voting system, and effectively implemented. Although the conclusion of the study was to recommend against implementing any one of the participating vote verification systems, these systems might become viable with further development and testing. As a result, it is important that further development not be stifled by mandating a specific vote verification system for use.

Questions submitted by Democratic Members

Q1. What documentation do your voting system vendors currently provide you that explain the security features of voting systems and the procedures required for your elections to be secure?

A1. The State's voting system vendor provides the standard "User's Guide" for the touchscreen and a guide for the software. These documents give an overview of the security features, such as data encryption and the use of dynamic keys, provide recommendations for their use, and detailed instructions on how to use those features. For new software releases, they also provide release notes that detail new or updated security features.

With respect to the procedures required to secure elections, I believe that this is the responsibility of election officials, not vendors. While election officials should consider the vendor's recommendations for operating a secure voting system, it is ultimately the duty of election officials to implement security procedures.

In Maryland, we have contracted with outside firms to conduct a variety of security assessments and have internal resources implement the recommendations of these assessments and develop procedures to protect the election process. The agency's Chief Information Officer has significant experience in security-related matters, and a Chief Information System Security Officer is on staff to review the vendor's recommendations and develop security procedures for all aspects of the election process. These internal resources, combined with the vendor's recommendations and outside analyses, demonstrate the commitment to preserving the integrity of the election process and reducing the likelihood of any tampering with the election.

Q2. What additional improvements are needed (if any) for the voluntary guidelines and national certification process? Also, what additional steps should the Election Assistance Commission take to support efforts of states and local jurisdictions to acquire and operate accurate, reliable, and secure voting equipment?

A2. As the Voluntary Voting Systems Guidelines (VVSG) are not yet in effect nor being used for testing and the Election Assistance Commission (EAC) has only just

started its work in accrediting testing laboratories, it is important to give both the VVSG and the EAC time to work before making significant recommendations. That being said, I recommend that future versions of the VVSG include state-specific certification requirements. This would enable state election officials to accept the EAC's certification as the basis of state certification. This joint certification would reduce the resources needed to conduct state certification without a reduction in confidence in the voting system and would greatly benefits states with less financial resources for testing. Incorporating a joint certification could also provide an additional incentive for states to adopt the VVSG.

The EAC has contracted with two experienced and well-respected election officials to develop management standards. While these management standards will cover many topics related to elections management, they will also focus on standards for voting systems. I believe that this effort has enormous potential to improve election administration and the security of voting systems. I also believe that the EAC could provide much needed assistance to states and counties by offering best practices and assistance in negotiating contracts with voting system vendors.

Q3. GAO recently reported that only 15 percent of jurisdictions collect measures on voting equipment failures. Does your state collect data on voting equipment failures and what have you found from the data you've collected? What are your views on collecting this information on a national basis?

A3. Maryland collects information on reported voting system malfunctions from a variety of sources (poll workers, voting unit technicians, State and local election officials, and vendor's help desk). Either county or State election officials follow-up on the information and determine the root cause of the problem.

A 2004 analysis of voting units from Maryland's largest jurisdiction showed that many of the voting units flagged by election officials and poll workers as requiring special attention or review were voting units that did not have the power cord properly inserted, causing the internal battery to drain, and the voting unit to eventually lose power, physical damage to the voting unit booths (which may include issues such as broken legs or cases); any voting unit that has substantially fewer ballots cast on it than others in the same precinct; or any other reason that an election judge or local election board staff member feels the voting unit needs to be analyzed, either because a problem was observed or reported by a voter. After careful review of all of the voting units referred for additional analysis, State election officials found that only .4 percent of that county's voting units had issues on Election Day.

I believe that it is important to collect this information at the national level to assist election officials with identifying common concerns and working collaboratively to address any issues. As with any national survey and the resulting conclusions based on the data, it is important that there are standard and clear definitions, that the data is used to improve the voting process, not for criticizing election officials or a specific vendor, and that election officials have time to conduct an initial review of the reported voting system malfunctions. For obvious reasons, a voting unit with a broken leg must be recorded and analyzed differently than a voting unit that freezes during voting hours.

Q4. Dr. Wagner made a number of short-term recommendations based on the Brennan Center report that he believes could improve the security and reliability of voting equipment that will be used this November. These recommendations include routine audits of voter-verified paper records, performing parallel testing of voting machines, adopting procedures for investigating and responding to evidence of fraud or error, and banning voting machines with wireless capabilities. Would [you] please comment on these suggestions?

A4. I generally agree with Dr. Wagner's recommendations to the extent that election officials should implement recognized best practices and measures that verify the accuracy and integrity of the voting system. To that end, Maryland has implemented pre-election and Election Day parallel testing, has procedures for investigating and responding to allegations of fraud or error, and does not use voting systems with wireless capabilities. Although the State's voting system does not have a voter-verified paper record, there are routine audits performed after each election to verify the accuracy of the voting system. Jurisdictions that are not already planning on implementing these short-term recommendations for the upcoming November elections may not have sufficient time to implement best practices and develop and implement these recommendations.

Q5. Dr. Wagner's testimony outlines problems that we frequently see reported in news articles about problems with voting equipment. In addition to his com-

ments on the current status of voting equipment, he makes a number of longer-term recommendations, many which focus on conformance criteria and testing of voting machines. Would you please comment on these recommendations?

A5. Before responding to Dr. Wagner's recommendations, I think it is very important to recognize that many "problems" reported in the news are not voting system problems; they are, in fact, problems caused by human error. For example, in 2004, the media reported that voting systems in several Maryland precincts failed. The voting units prevented voting, because precinct-specific encoders (the device that tells the voting unit which ballot to load) were delivered to the wrong precinct. The voting system worked exactly as it should have; that is, it prevented the wrong encoder from working with the voting system. Although reported as such, this was not a voting system problem; it was simply a human mistake.

After each of Dr. Wagner's recommendations, I have provided comment.

- *Mandate voter-verified paper records and mandatory manual audits.*—Because of the extensive pre-election, Election Day, and post-election testing we conduct on the State's voting system and numerous security analyses and resulting security procedures, we are confident that the voting system accurately counts and records votes. For this reason, I do not believe that a voter-verified paper record improves the accuracy of a thoroughly tested voting system.

  Additionally, I am concerned that a mandatory voter-verified paper record would stifle—and likely already has—the development of other independent verification technologies. During our study of vote verification systems, several of the products were very promising and offered audit and verification tools that are not possible with voter-verified paper records.

  One, for example, could provide the amount of time it takes poll workers to prepare the voting unit for voting. This information could be used to enhance poll worker training and inform the vendor on how the opening process on the voting unit could be improved. Mandating voter-verified paper records would prevent the development and testing of other verification solutions.
- *Broaden the focus beyond functionality testing.*—I agree that all aspects of voting systems should be tested and that testing should extend beyond just functional testing. Although, Dr. Wagner states that the current "standards primarily focus on functionality testing," this is not the case. Both the 2002 Voting Systems Standards and the 2005 VVSG incorporate standards for testing accessibility, reliability, and security.
- *Eliminate conflicts of interest in the federal testing process.*—The testing process under the National Association of Election Directors, the entity that previously oversaw the testing process, has been conducted with the highest integrity. Although I am open to discussing different federal testing structures, the current testing process is objective, and to suggest that there are conflicts of interest implies that the vendors have influence over the voting system testing process solely because they pay for testing. This is not the case.
- Reform federal testing process to provide more transparency and openness.—With the EAC assuming responsibility for the voting system certification process, more information about voting system testing will be available. Examples of information that will be available from the EAC include testing reports and technical data packages.
- *Require broader disclosure of voting system source code.*—In the EAC's upcoming certification program, voting system vendors will be required to submit a final software version to an escrow agent and allow election officials to compare the delivered software against the software version on file with the escrow agent. Maryland has previously used MST's National Software Reference Library to compare the version of the software being used in the State against the version qualified by the National Association of State Election Directors. This comparison has been performed both before and after statewide elections and reassures election officials that no unauthorized software is being used.
- *Incorporate closed feedback loops into the regulatory process.*—It is my understanding that the EAC has developed a process to collect and investigate claims that voting systems are not performing appropriately and are not in compliance with voting system standards, and I support this effort. It is important that the EAC serve as both a resource to election officials for investigating potential voting system malfunctions and noncompliance with stand-

ards and, if necessary, initiating a decertification system if the allegations are substantiated.

- *Strengthen the evaluation of usability and accessibility.*—I believe that the enhanced usability and accessibility standards in the VVSG are an important first step. I understand that the 2007 standards will include additional usability and accessibility factors.
- *Increase representation of technical experts in computer security on the TGDC.*—Four of the fifteen—or 25 percent—of the TGDC's current members are technical experts. (Election officials currently hold four seats on the TGDC, the same number as technical experts.) Increasing the number of technical experts at the expense of other subject matter experts would not reflect the realities of voting systems and elections administration and would alter the balance that currently exists on the TGDC. While technical experts play an important role in improving election administration, they are but one voice in the debate.
- *Ensure that standards are grounded in the best scientific and engineering understanding.*—While I agree with this recommendation, the science of voting systems must be balanced against the realities of elections.

ANSWERS TO POST-HEARING QUESTIONS

Responses by David Wagner,[1] Professor of Computer Science, University of California-Berkeley

Questions submitted by Chairman Vernon J. Ehlers and Chairman Sherwood L. Boehlert

Q1. How do you think the sections of the 2005 Voluntary Voting Systems Guidelines (VVSG) that deal with security should be improved?

A1. I recommend sweeping changes to how the 2005 Voluntary Voting Systems Guidelines (VVSG) deal with security, to bring them up to date with fundamental changes over the past decade in how voting systems are built. The 2007 VVSG are in the process of being drafted, and I propose several suggestions for consideration.

- *Require that systems provide voter-verified paper records.* The single most effective step that the VVSG could take to improve security would be to stop certifying new voting systems that do not provide a voter-verified paper record. The VVSG could also be revised to require that the use procedures provided by the vendor specify how to perform a routine manual audit of these paper records.

  Given the current state-of-the-art, there is no known way to provide a comparable level of security without voter-verified paper records. In the long run, as technology advances, it may be possible to develop alternative voting technologies that provide an equal or greater level of security without using paper. Consequently, it may be appropriate to structure the VVSG to permit other systems that demonstrably provide an equal or greater level of security as voter-verified paper records with manual audits. However, any such provision would need to be accompanied by a new process for determining which systems meet this criteria. The current evaluation and testing process is not capable of making these determinations with any credibility; major reforms of the current processes would be required before such a provision would be safe to add. Adding such a provision without accompanying reform of the process used to evaluate which systems qualify for the exception would eliminate much of the benefit of a requirement for voter-verified paper records. In addition, it should be expected that evaluating the security of systems that do not use voter-verified paper records will be considerably more expensive and difficult than evaluating systems that use voter-verified paper records, due to the fact that paperless systems do not record a permanent copy of the voter's intent that the voter can verify.
- *Begin enforcing existing requirements.* At present, many of the security requirements in the 2005 VVSG are not enforced or tested by the federal qualification process. While the existing requirements of the VVSG are, for the most part, a fairly reasonable start at specifying security requirements for a voting system, the lack of enforcement renders these well-intentioned requirements ineffective.

  The VVSG do not specify any specific testing procedure for many of the security requirements, and perhaps as a consequence, the federal testing labs apparently do not perform an independent analysis of whether these requirements are met. Instead, the testing labs seem to concentrate their efforts on requirements for which there is a concrete testing procedure defined in the VVSG. We now know of multiple examples where the federal testing labs have approved voting systems that contain violations of the VVSG [1].
- *Create faster ways to investigate and act on experience from the field.* At present, the EAC has no way to respond quickly to new discoveries about the security of deployed voting systems. Currently, the only mechanism the EAC has to affect the machines that voters vote on is to revise the VVSG. However, these revisions take an extremely long time to take effect. For instance, the next revision of the VVSG is not scheduled until 2007. Moreover, the 2007 VVSG are not expected to take effect until 2009. Furthermore, when the 2007 VVSG do go into effect in 2009, they will only affect newly developed or modi-

[1] This work was supported by the National Science Foundation under Grant No. CNS–052431 (ACCURATE). Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author and do not necessarily reflect the views of the National Science Foundation. I do not speak for UC–Berkeley, the National Science Foundation, or any other organization. Affiliations are provided for identification purposes only.

fied systems submitted for certification after that date. Any systems that had been already certified or already deployed at that time would be grandfathered. Consequently, any new provisions in the 2007 VVSG will only affect systems purchased after 2009, and possibly only systems that were both developed and purchased after 2009. Because jurisdictions purchase new systems only rarely—perhaps once a decade or so, at best—any revisions to the VVSG that the EAC wished to make today might not have any impact on the machines that a majority of Americans vote on until 2015 or so.

Moreover, the EAC has no formalized, systematic way to gather data from the field about the performance of voting systems or to track incidents and failures across the country.

In comparison, the aviation industry has more effective mechanisms for investigating and responding to new discoveries about threats to aviation safety. Whenever a plane crash or other serious in-flight anomaly occurs, federal investigators immediately investigate the cause of the failure. If serious problems are found, federal regulators have the authority to require that corrective action be taken immediately, if necessary. The consequence is that federal authorities have the ability to respond to serious problems that affect aviation safety in a matter of months. The EAC lacks any corresponding capability to investigate or respond to voting system failures.

It would help to create ways to investigate voting system failures, to require reporting of election incidents, to gather data from the field and quantitatively measure the rate of failures, to update voting standards more frequently in response to this data, and to require timely adherence to the standards [2].

Also, it would help to establish a process to decertify voting systems that are certified and then are subsequently discovered to have security flaws or to violate the standards. It would help if the EAC were to exercise its authority to decertify systems when they are found to have security vulnerabilities.

- *Require some additional safeguards recommended by security experts.* Many security experts have recommended several additional safeguards: banning wireless communications in voting systems; banning some forms of interpreted code; banning code stored on removable storage media. These would not on their own fix all the security problems we are currently experiencing, but they would help address some known gaps in the standards.

Q1a. Do you think that the way in which security for voting systems is tested needs to change? If so, how, and if not, why not?

A1a. Yes. The current process is not working: systems with serious security vulnerabilities are getting approved. I suggest several reforms.

- *Convene a panel of security experts to conduct independent security evaluations of every system submitted for certification.* Each time a voting system is submitted to the federal qualification process, the EAC could convene a panel of leading security experts from both academia and industry to perform an independent security analysis of the system. Independent security evaluations are standard practice in the field of computer security; the election industry has lagged behind the rest of the field in this respect.

Over the past few years, external experts have been much more effective at finding security flaws and assessing the security of today's e-voting systems than the federal testing labs. Consequently, it makes sense to enlist those who have demonstrated skill at finding security vulnerabilities in voting systems, so that we know about the flaws and can take appropriate action before the systems are deployed in the field. For instance, in 2003 four academics found more security flaws in one voting system in 48 hours of examination of the voting software than the federal testing labs had in the years that the system was deployed. In 2005, a Finnish security researcher found two significant security vulnerabilities after approximately one week of study of a voting system, upon the request of a county election official in Florida. In 2006, the same Finnish researcher found another serious security vulnerability after another week of study of the same voting system, at the request of a county election official in Utah. Independent security evaluations could help reduce the chances of approving and deploying a flawed system.

Given that many have lost faith in the ability of federal testing labs to evaluate the security of voting systems, independent security evaluations would provide an independent check on the federal testing labs. Because the effectiveness of an independent security evaluation is highly dependent upon

the skills of the participants, it is important that panelists be chosen from among the best minds in computer security. To this end, I would recommend that the EAC consult with the ACCURATE project to identify potential panelists. The panel should have full access to all technical information about the voting system, including all source code. The panel should also have full access to a working unit of the voting system, and the authority and ability to physically inspect and run tests on that unit. The panel should be asked to write a report of their findings, and the report should be made public in its entirety. If necessary, the vendor's proprietary interests can be protected, while preserving transparency and the independence of the evaluators, through an appropriate non-disclosure agreement.

- *Require vendors to disclose the source code of all voting system software by a specified future date.* The use of secret software has contributed to a loss of transparency and eliminated opportunities for public oversight of important parts of the machinery of our elections [3]. This secretiveness has contributed to a loss of confidence in the voting systems. The best way to remedy this would be to require that vendors make all source code, and other technical information about the design and construction of their voting machines, publicly available for all interested parties to examine [4]. Vendors would still enjoy the protection of patent and copyright law but would be required to forfeit trade secrecy in their software to field systems in federal elections.

  Some transition strategy may needed to phase in this requirement. One possibility is to specify a date several years in the future after which source code to voting systems would be required to be disclosed and provide advance notice to vendors of that date. In the short-term, source code might be required to be disclosed to any accredited security expert who is willing to sign appropriate non-disclosure agreements.
- *Eliminate the COTS loophole.* The standards currently contain an exception that exempts commercial off-the-shelf software (COTS) from some of the testing. Because COTS software has been implicated in some recent security vulnerabilities, I believe there is a good argument for eliminating this exception.
- *Eliminate conflicts of interest; ensure that evaluators are truly independent. At present, the federal testing labs work for the vendors: they are paid and selected by the voting vendors. We need some other mechanism that better ensures the independence of the testing labs.*

  One possibility would be for the testing labs to be paid by the Federal Government, with vendors required to reimburse the government for all costs incurred. For instance, in California the state has set up an escrow account for each vendor. The vendor is required to deposit sufficient funds to cover all the costs of certification testing into this account; when the state hires consultants or other experts, they are paid out of this escrow account. The Federal Government could use a similar system. This would make it clear that labs work for the Federal Government and have a fiduciary responsibility to the citizenry, not to the vendor.

  It may be possible to devise creative new approaches that rely on market forces to make testing more effective. For instance, if federal labs had to pay damages when a voting system they approved turned out to be insecure, they would have an incentive to make their testing processes as effective as possible. One possibility might be to require federal labs to carry insurance and give all citizens standing to sue the labs for approving insecure voting systems, setting the damages for endangering democracy at a high dollar amount. Federal approval of a voting system might mean far more if testing labs needed to keep their insurance premiums down in order to remain profitable. It is not clear whether such an approach can be made workable, but new incentive structures may be worth exploring.
- *Make all reports from the testing labs public.* Today, the results from the federal testing labs are not made available to the public. The labs consider them proprietary and the property of the vendor. If a system fails to gain the testing lab's approval, this fact is not disclosed to anyone other than the vendor who paid for the testing.

  I recommend that the results of all testing at the federal level be disclosed to the public. All reports produced by the testing labs should be published in full, whether the systems pass or fail.
- *Enforce all security requirements in the standards.* As mentioned earlier, many security requirements are never tested and consequently are not en-

forced. Security evaluation of voting systems should change so that all security requirements are assessed. We should expect and require testing labs to fail any voting system if they cannot demonstrate that it meets all security requirements.

Q2. Is computer security testing different from other types of conformance testing, and if so, how? Has this type of testing ever been performed on voting equipment and if so, what were the results? Should this type of testing be performed routinely on voting equipment?

A2. Yes, security evaluation is different from other types of conformance testing. Conformance testing—commonly also known under the name "functionality testing" or "black-box testing"—is concerned with ensuring that the system will respond in certain ways under ordinary operating conditions. This makes conformance testing fairly straightforward: the best simulates ordinary operating conditions and then checks that the system responds as desired under these conditions. For instance, if we want to test that a voting system correctly counts write-in votes under normal operating conditions, then we can run a mock election, cast several write-in votes, and confirm that they are counted correctly. As this example illustrates, conformance testing is often fairly straightforward.

In contrast, security evaluation is concerned with ensuring that the system will not misbehave when it is intentionally misused. Thus, ordinary conformance testing is concerned with how the system behaves under normal conditions, while security evaluation is concerned with how it behaves under abnormal conditions. Unfortunately, it is very difficult to predict how an attacker might try to misuse the system. If we could predict how the attacker were going to misuse the system, then we could simulate such misuse and observe whether the system is able to respond appropriately. However, usually we do not know how an attacker might try to misuse the system, and there are too many ways that an attacker might try to misuse the system to exhaustively enumerate them all. Consequently, there is no way to simulate how the system reacts to these kinds of unanticipated attacks. This makes security evaluation more difficult than ordinary standard conformance testing.

For these reasons, standard conformance testing practices are not effective at evaluating whether a system is secure or not. Security practitioners are familiar with this phenomenon [5]. As a result, when experienced practitioners need to evaluate the security of some software, they normally use discipline-specific methods chosen to be effective for security purposes, instead of just relying on testing. These methods always include some form of adversarial analysis, which may include elements of threat assessment, source code review, architectural review, penetration analysis, and red teaming. Security practitioners also understand that, to be most effective, adversarial analysis should be performed by security experts who are neutral and independent. This process of adversarial analysis, when performed by independent security experts, is sometimes known under the name "independent security evaluation." Use of these adversarial analysis methods is routine practice in industries where security is mission-critical.

Yes, these security evaluation practices have been applied, on a limited basis, to several voting systems. In each case, serious security flaws were found.

- In 2003, researchers from Johns Hopkins and Rice Universities undertook an adversarial analysis and source code review of voting software used in Diebold touchscreen voting machines [6]. They found numerous security vulnerabilities.
- In 2004, a security consulting company (RABA Technologies) performed an independent security evaluation of Diebold voting systems and found several security vulnerabilities [7].
- In 2005, Finnish researcher Harri Hursti applied source code analysis and testing to discover and confirm two security vulnerabilities in an optical scan machine manufactured by Diebold [8].
- In 2006, I and several other security experts analyzed source code provided by Diebold as part of our independent security evaluation of Diebold systems [9]. We confirmed that Hursti's vulnerabilities were present in both Diebold optical scan and touchscreen machines. We also found 16 other security defects that had not been previously known.
- In 2006, Hursti was asked to examine a Diebold touchscreen machine, and he discovered another serious security vulnerability using adversarial analysis [10].

In each case, the use of practices specific to the field of computer security was central to the effectiveness of these security evaluations. As far as I can tell, none

of these security vulnerabilities had been previously discovered by the federal testing labs, perhaps because the labs were focused on standard conformance testing and failed to use methods more appropriate to security evaluation [11].

Yes, these security-specific evaluation methods should be applied routinely to voting systems. They are the best tools we have for weeding out insecure voting systems, for proactively finding and fixing security vulnerabilities in voting systems before they are deployed, and for increasing confidence in the security of these systems.

It is worth mentioning that the term "testing" has a more specific meaning in the computer science jargon than its everyday meaning. Someone who is not a computer specialist might use the word "testing" to describe any method for evaluating the quality of software or for finding software defects. In contrast, computer scientists use the term "testing" more narrowly to refer to one specific method for evaluating software quality: among computer scientists, the unqualified term "test" is often viewed as a synonym for "black-box testing," "functionality testing," or "conformance testing." Computer scientists would say that "testing" is just one method of assessing the quality of software, but that there are others, as well. When it comes to security, those other methods are usually more effective than "testing." Because of the potential for confusion, I will avoid use of the unqualified word "testing;" I will use terms like "functionality testing" to refer to one specific method of evaluating software quality, and terms like "evaluation" to refer to the broad goal of evaluating software quality and finding software defects.

Q3. In your written testimony, you stated that functionality testing is not as good as discipline-specific testing. Please explain the difference between functionality and discipline-specific testing, and why you believe discipline-specific testing should be used for voting equipment.

A3. "Functionality testing" is a synonym for "black-box testing" or "conformance testing." Thus, my response to Question 2 is relevant to this question as well.

As I mentioned, security practitioners have developed discipline-specific methods—methods that are suited to the discipline of computer security—for evaluating the security of computer systems. These include source code analysis, independent security analysis, architecture and design reviews, and red teaming. Functionality testing verifies that a machine does what it is supposed to do, when it isn't under attack; in contrast, these security evaluation methods verify that a machine does not do what it isn't supposed to do, even when it is under attack. These discipline-specific methods should be used on voting equipment in addition to functionality testing, because they are the best known way to assess the security of such systems.

The discipline of usability has also developed its own discipline-specific methods for evaluating the usability and accessibility of computer systems, including user testing with actual voters and poll workers as well as heuristic evaluation by usability and accessibility experts. These methods specifically cater to human factors concerns and are designed to evaluate how the software influences interactions between humans and computers. These methods are focused less on functional requirements (e.g., can the system display candidate names in a bold font?) and more on assessing performance via quantitative metrics of usability. These discipline-specific methods should be used for voting equipment, because they are the best known way to assess the usability and accessibility of such systems.

Q4. Mr. Groh and Ms. Lamone expressed concerns about the use of the voter-verifiable paper audit trail. These concerns included the additional costs to jurisdictions of implementing these systems, and the accessibility of such technologies to the disabled community. Ms. Lamone also cited a Maryland study that indicated that the paper trail, in addition to other verification technologies, was not ready for prime time. Do you agree with these concerns? If so, why, and if not, why not?

A4. In short: I agree with the concerns about cost; I do not agree with the concerns about accessibility; I do not agree with Ms. Lamone's characterization of the Maryland study. I provide my reasoning below.

- I do share Mr. Groh and Ms. Lamone's concerns about the costs of implementing systems that support voter-verified paper records. Approximately 15 states have purchased paperless voting systems that do not provide voter-verified paper records [12]. Some of these paperless voting systems can be retrofitted to produce a voter-verified paper trail, but in some cases these systems cannot be easily upgraded or retrofitted with a paper trail. Even when it is possible, retrofitting is not cheap. Replacement is even more expensive, as it involves throwing away equipment and replacing it with more modern

equipment. It is certainly understandable why states who have made a significant investment into a particular voting system would be reluctant to scrap these systems and incur significant costs in replacing them. It is unfortunate that some states bought paperless voting systems without realizing the security, reliability, and transparency consequences of that action.

The costs would vary widely from state to state. Currently, 27 states require by law that all voting systems produce voter-verified paper records, and another eight states have deployed voting systems with voter-verified paper records even though state law does not require it. In total, 35 states (70 percent of states) have voting systems that already produce a paper audit trail and would not need to be upgraded or replaced. Those 35 states would not incur any cost. The remaining 15 states (30 percent) do not consistently use systems with a paper audit trail statewide. In those states, some or all of the voting equipment in the polling places would need to be upgraded, retrofitted, or replaced. On the other hand, equipment used for scanning absentee (mail-in) ballots, which account for 30–40 percent of the vote in many states, would not need to be changed.

Even within this class of 15 states, costs would vary by state. At one extreme, some states use paperless DREs throughout the state, and all of those DREs in every county would need to be upgraded, retrofitted, or replaced. As best as I can tell, there appear to be five states (DE, GA, LA, MD, SC) in this category. Of those five states, two (GA, MD) use DREs that would need to be completely replaced, because there is no good way to upgrade or retrofit them with a paper trail; two (LA, SC) use DREs for which an approved printer add-on is already on the market; and I do not know whether retrofitting is possible in the remaining state (DE). Obviously, replacing all DREs is the most expensive possible case. At the other extreme, in some states the voting equipment is not uniform throughout the state and costs would be less in some counties than in others. For instance, approximately 52 of 67 Florida's counties use optical scan voting machines plus one accessible voting system (DRE or ballot marking device) per polling place; upgrades for those counties would be less expensive, because the optical scan machines would not need to be upgraded, retrofitted, or replaced.

Costs will also vary according to the system that is in use. Many modern DREs (e.g., the Diebold TSx, ES&S iVotronic, Sequoia Edge, and Hart-Intercivic eSlate) can be upgraded to produce a paper trail: approved printer units are available on the market. Upgrading these DREs to add a printer might cost approximately $500–$2000 per DRE, depending on the vendor. Some older DREs (e.g., the Diebold TS) cannot easily be upgraded or retrofitted with a paper trail, and would have to be replaced with all new equipment. Buying new DREs normally costs about $3000–$5000 per DRE. However, in some cases it may be cheaper to replace the paperless DREs with a hybrid system using optically scanned paper ballots. These hybrid systems require purchasing one optical scan machine plus one accessible voting machine (DRE with VVPAT or ballot marking device) per precinct, and this equipment typically costs in the ballpark of $10,000–$12,000 per precinct. Because an all-DRE solution usually requires several DREs per precinct, hybrid systems using optical scanners may come out cheaper. The cost advantages of hybrid systems are more pronounced in states that require DREs to display a full-face ballot, because full-faced DREs are significantly more expensive than standard DREs [13]. I would encourage jurisdictions to consider all available options.

In summary, I do not know what the total costs might be, but I share Mr. Groh and Ms. Lamone's concerns that the costs of implementing a voter-verified paper trail will be significant in some states.

- I do not agree with their concerns about the accessibility of these voting systems to the disabled community. The disabled community has praised the development of touchscreen voting systems as providing major improvements in accessibility, and rightly so: the accessibility benefits are significant and real. However, voter-verified paper records are in no way incompatible with these benefits. Today, every major vendor who offers a touchscreen voting machine also offers a version of that touchscreen machine that produces a voter-verified paper record. Those VVPAT-enabled versions provide the same accessibility support—audio interfaces, high-contrast displays, sip-and-puff devices, booths designed for wheelchair voters, and so on—as their paperless brethren do. Adding a printer makes the machine no less accessible.

I believe security and accessibility do not need to be in conflict; I believe we can have both. This is fortunate, because I believe both security and accessibility are important goals.

I understand that one concern is that visually impaired voters will not be able to independently verify what is printed on the voter-verified paper record. This concern is valid, but I do not consider it a persuasive argument against voter-verified paper records. If a blind voter does not trust the voting machine to work correctly, then it is true that they have no way to independently verify that their vote has been recorded correctly. In other words, blind voters must rely upon the voting software to work correctly, and they are vulnerable to software failures; they have no independent means of checking that the software is working correctly. This situation is truly unfortunate. However, this is the case for all currently available voting technologies, whether they print a paper record or not. If the machine prints nothing, then the blind voter still cannot independently verify that their vote has been recorded correctly on electronic storage. To put it another way, with paperless voting machines, neither sighted voters nor blind voters have any chance to independently verify their vote; with voter-verified paper records, sighted voters can independently verify their vote, but blind voters cannot. Voter-verified paper records do not make the independent verification problem any worse for blind voters; they just fail to make things better.

The policy question is whether it is valuable to improve security and reliability for most voters, even if there are some voters who are not helped by these measures (but are not harmed by them, either) and remain without any means of independent verification.

- I do not agree with Ms. Lamone's characterization of the Maryland study. At present, Maryland uses a paperless touchscreen voting machine, called the Diebold TS. The Maryland study was commissioned to study whether there exists any technology currently on the market that could be used to upgrade or retrofit the Diebold TS with a way for voters to independently verify that their vote was recorded, and to evaluate whether any of these are ready for use in real elections. The Maryland study was specifically limited to studying methods of upgrading or retrofitting the Diebold TS; replacement was out of scope for the study. The conclusion of the study was that there was no good way of upgrading the Diebold TS that would be ready for use in the near future. I have read the study carefully and I agree with that conclusion. I agree with Ms. Lamone that the study was "very thorough" and "provided some very valuable information."

  However, I disagree with Ms. Lamone's characterization of the study as finding that "the paper trail" was not "ready for prime time." In fact, the Maryland study's findings were more narrow than that. The Maryland study was asked not to consider any technology that would require replacing Maryland's Diebold TS machines; they were asked to consider only technology for upgrading those machines, and they did so. It is indeed justified to conclude from the study that none of the systems for upgrading the Diebold TS are "ready for prime time." However, the study says nothing about the viability of other, more modern voting systems that do provide a voter-verified paper trail. The correct conclusion to draw from the Maryland study is that if Maryland wants to adopt voter-verified paper records, they will need to replace their existing Diebold TS machines; retrofitting is not a viable option. The study says nothing about whether existing, deployed systems that provide a paper trail are ready for prime time. I believe there are existing paper-trail systems that are already ready for prime time.

  Maryland is in an admittedly difficult position. Maryland was one of the first states to adopt touchscreen voting systems, and while the Diebold TS machines they bought were thought by some to be adequate at the time, at present the Diebold TS machines are no longer the most current technology. The Diebold TS was not designed to provide a paper trail. Its successor, the Diebold TSx, does provide a voter-verified paper audit trail. The other major voting system vendors also sell voting machines that do provide a paper trail. Not all states are in the same position that Maryland is in: many states already use systems with a voter-verified paper trail; and some states have voting systems that do not currently provide a voter-verified paper trail, but that can be upgraded or retrofitted to provide a paper trail.

Q5. The 2005 VVSG contains an appendix on independent dual verification systems that could perform the same functions as a voter-verifiable paper audit trail. Is

this technology being used in voting systems today or is more research needed to make it operational? What are the advantages and disadvantages of this technology? To what extent are there other technologies that could perform the same function as a voter-verifiable paper audit trail?

A5. No, this technology is not being used today in any deployed voting system that I am aware of. More research would be needed to determine whether the approach can be made operational. The future of this approach is uncertain at this point.

The advantages and disadvantages of any particular system will depend on how that system is designed and implemented. It is difficult to comment on advantages and disadvantages in the absence of a fully implemented system. I can only speculate.

One potential disadvantage is that evaluating whether these systems meet the security requirements is likely to be significantly more expensive for paperless independent dual verification systems than for systems producing a voter-verified paper record, both because the certification process would need to be overhauled, and because assessing whether paperless independent dual verification systems are secure is inherently more difficult than assessing whether systems with a paper trail meet their security goals. Another potential disadvantage of paperless independent dual verification systems is that it may be harder for voters who do not have a degree in computer science to know whether they should trust those systems. One motivation for seeking paperless systems is that eliminating the need to handle or store paper could make election administration more efficient. Also, ideally such a system might provide visually impaired voters with a way to independently verify their vote, which would be a significant advantage. Unfortunately, no such method is known at present.

At present, it is an open question whether it will be possible to develop a paperless voting system that can perform the same function as a voter-verified paper trail. There does not appear to be any firm consensus among computer scientists on whether such an alternative is even possible, given the current state of technology; on what directions are most promising to explore; or on how far off this goal may be. I believe that more research is warranted, but that we should not expect deployable replacements for paper anytime soon.

Q6. Have you conducted any studies of the problems/deficiencies of paper-based systems?

A6. Yes. I have conducted studies that revealed some problems and deficiencies in certain paper-based systems. I have not attempted to undertake any study to exhaustively categorize all possible problems or deficiencies that can arise with paper-based systems. Of course, the history of paper-based elections in this country dates back at least two hundred years, and it is well-known that they can be susceptible to certain kinds of problems (e.g., problems in the handling, transportation, or storage of paper ballots) if elections are not well-administered.

Q6a. Is your support for a voter-verified paper record principally motivated by confidence in paper-based systems or a lack of confidence in direct recording electronic systems? If the former, what is the source of this confidence? If the latter, on what basis do you conclude that paper-based systems are necessarily superior?

A6a. My support for voter-verified paper records is motivated both by confidence in paper-based elections (if they are administered well) and by my lack of confidence in paperless DRE machines.

My confidence in systems that produce voter-verified paper records and include routine manual audits is based on my study of these systems and on analysis of their security properties. My confidence in these systems is based on the ability of voters to verify for themselves that their vote was recorded as they intended, and on the ability of observers to verify that votes were counted correctly and to exercise effective oversight of the process.

My lack of confidence in paperless DRE machines is based on my study of these systems, on analysis of these systems in the open literature [14], and on the documented security flaws and failures of these systems. For instance, the Brennan Center report found that with paperless DRE machines, a single malicious individual with insider access may be able to switch votes, perhaps undetected, and potentially swing an election. The analysis in the Brennan Center report also found that systems that produce voter-verified paper records and include routine manual audits are significantly more secure against these threats than paperless DRE machines.

Q7. Do you foresee any problems that might arise in jurisdictions utilizing a voting system that attaches printers to Direct Record Electronic voting machines? What do you think they might be?

A7. Yes. There are several issues such jurisdictions may want to be aware of.

First, the introduction of printers raises questions of printer jams and the reliability of these devices. California's solution to this problem has been to adopt volume testing, where approximately 10,000 ballots are cast on 50–100 machines in a mock election. Volume testing seems to be effective in weeding out unreliable machines and improving the reliability of voting machines—including their susceptibility to printer jams. The first such volume test found serious printer jam problems in one voting system; fortunately, the vendor was able to correct those problems, and subsequently their system passed the volume testing with no serious problems. California has now certified several DRE voting machines that come with an printer, and these systems appear to provide a satisfactory degree of reliability.

Second, a voter-verified paper record is only effective in proportion to the number of voters who actually verify the paper record as they cast their ballot [15]. Consequently, jurisdictions may wish to consider undertaking voter education to inform voters of the importance of checking the accuracy of the voter-verified paper record.

Third, there is no point in printing a voter-verified paper record if those paper records will never be used or examined by election officials for their intended purpose, i.e., to check vote counts. For this reason, it is important that the jurisdiction create procedures specifying the conditions under which those paper records will be inspected, and what will be done in case of a discrepancy between the paper record and the electronic record. My own recommendation is that jurisdictions adopt routine manual audits; that discrepancies trigger an investigation; that any unexplained discrepancies discovered trigger a manual recount; and that in the event of a discrepancy between the electronic record and paper record, the paper record verified by the voter should have a (rebuttable) presumption of accuracy unless there is some specific reason to believe that the paper records are inaccurate or incomplete.

Fourth, in any election system that uses paper, the handling, transportation, and storage of the paper records is crucial. It is important that jurisdictions establish procedures to establish a good chain of custody for paper ballots and paper trails. For instance, analysis performed by the Brennan Center shows that, if the chain of custody is done poorly, jurisdictions may still be vulnerable to fraud, no matter what voting technology they use.

Finally, and most importantly, the success of an election is determined by more than just technology: it depends crucially on the people who run the election and the processes and procedures they use. Effective and competent election administration is crucial—and printers do not eliminate this important requirement.

Questions submitted by Democratic Members

Q1. Dr. Wagner, to what extent do voting system security vulnerabilities outlined in the Brennan Center Study reflect weaknesses in the 2002 standards and current certification process? To what extent have those weaknesses been addressed in the 2005 version of the voting systems guidelines and proposed certification process?

A1. The threats outlined in the Brennan Center study reflect significant gaps in the 2002 standards and in the current certification process. The Brennan Center study identified potential threats to voting systems that are not addressed by the 2002 standards or by the current certification process.

Those gaps have not been addressed in the 2005 standards or the certification process it proposes. The Brennan Center study suggested six concrete recommendations to improve the security of elections. None of those are required or recommended by the 2005 standards. In some cases, the 2005 standards takes stances that are directly at odds with the recommendations of the Brennan Center study. For instance, the Brennan Center study recommended banning all wireless communications, yet the 2005 standards explicitly allow wireless communications under certain conditions. One lesson from the Brennan Center study is that the best defense against these threats is the use of voter-verified paper records with routine manual audits; however, the 2005 standards do not require voter-verified paper records or manual audits. If voter-verified paper records are not in place, the Brennan Center recommended that parallel testing be used as a stop-gap; however, the 2005 standards do not require parallel testing, and very few states currently undertake the effort (and expense) of parallel testing.

Q2. Dr. Wagner, what additional measures need to be taken at the federal level to reduce the incidence of voting system vulnerabilities and problems across the U.S.?

A2. Please see to my answers to Question 1, starting on page 1, for detailed suggestions.

The most significant step that could be taken is to mandate that all voting systems provide voter-verified paper records, and that jurisdictions perform routine manual audits of these records. Also, it would help to conduct more rigorous testing of voting machines, performed by truly independent authorities, using testing methods based on the best scientific and engineering understanding from each applicable discipline and performed by experts from each relevant field; to invite outside security experts to perform independent security evaluations of all voting systems before certification; to increase transparency surrounding the federal testing and qualification process; to begin enforcing the existing security requirements already in the standards; to strengthen the security requirements and testing processes so they reflect the latest understanding of voting systems; and to disclose the source code of all voting systems.

Q3. Dr. Wagner, why do you believe that electronic voting machines cannot be trusted?

A3. If the electronic voting machines are accompanied by a voter-verified paper trail and routine manual audits, and if they are used properly, I believe that they can be trusted. Under these circumstances, they may offer some significant advantages.

However, I do not believe that paperless electronic voting machines can be trusted. The evidence that would be required to trust them is nowhere to be found.

It is beyond the state-of-the-art to verify that the software and hardware used in voting systems will work correctly on election day. For instance, how do we know that a programmer at the vendor has not introduced malicious logic into the voting system? The short answer is that we don't. Malicious logic that has been introduced into a voting system could, for instance, switch five percent of the votes away from one candidate and to the benefit of some other candidate; in a close race, this might make the difference between winning and losing, and such an attack might be very hard to detect. At present, we have no good ways to gain any confidence that our voting systems are free of malicious code; that is beyond the state-of-the-art [16]. Consequently, it seems there is little alternative but to assume that, for all we know, our voting systems could potentially be tampered with to introduce malicious code that will be triggered in some future election.

A second significant concern arises due to the possibility of defects unintentionally introduced into voting systems. Modern electronic voting systems are a highly complex assembly of software and hardware, and there are many things that can go wrong. It is not possible, given the current state of technology, to verify that voting systems are free of defects, flaws, and bugs, or to verify that they will record and count votes correctly on election day; given the complexity of modern voting systems, this is beyond the state-of-the-art.

Consequently, at the moment there seems to be little or no rational basis for confidence in paperless electronic voting machines [17]. In the end, it's not up to voters to take it on faith that the equipment is performing correctly; it's up to vendors and election officials to prove it.

Q4. Dr. Wagner, why is it that most security experts and computer scientists believe it is necessary to regularly audit voter-verified paper trails?

A4. Routine audits are crucial if we are to trust electronic voting [18, 19]. With both DREs and optically scanned paper ballots, it is important to routinely spot-check the paper records against their electronic counterparts. As I explained in my response to Question 3, there is no basis for confidence in the electronic records produced by electronic voting systems—we cannot know, a priori, whether they are correct or not. Given the stakes, we have to be prepared for the worst: that the electronic records may be inaccurate or corrupted. The purpose of a manual audit of the voter-verified paper records is to confirm whether or not the electronic records match the paper records verified by the voter.

The paper records verified by the voter are the only records that we can rely upon to be accurate: they are the only hard copy record of voter intent, and they are the only records that the voter has the chance to inspect for herself. It would be perfectly adequate, from a security point of view, to simply discard the electronic records and to manually count all of the voter-verified paper records (without the assistance of computers). Such a 100 percent manual count would produce results that could not be corrupted by computer intrusions, malicious logic, or software de-

fects. However, manual counting of paper records is labor-intensive and costly. Given the number of contests on a typical American ballot today, routine 100 percent manual counts are probably not economically viable.

To address these concerns, voting experts have devised an alternative that preserves the cost-efficiency of electronic vote counting with the trustworthiness of 100 percent manual counts [20]. This alternative is based around machines that produce voter-verified paper records along with routine manual audits. During the audit, the paper records from some percentage (perhaps one percent or five percent) of the precincts are manually counted; then the paper tallies are compared to electronic tallies. If they match exactly in all cases, then this provides evidence that the electronic vote-counting software produced the same vote totals that a 100 percent manual count would have produced, which provides a rational basis for confidence in the election outcome. On the other hand, any mismatches discovered during the audit indicate that something has gone wrong. This provides an opportunity to identify the problem and remedy it, if possible, or to perform a 100 percent manual recount if the problem cannot be identified.

Consequently, routine manual audits are the best way to ensure that the electronic vote-counting systems are working correctly; to discover and recover from major failures of the electronic vote-counting software; to prevent and deter large-scale vote fraud; to provide transparency; and to give election observers evidence that the election was performed correctly. If done right, these audits provide us with a powerful defense against errors and election fraud: the paper records are a cross-check on the electronic records, and the electronic records are a cross-check on the paper. It is for these reasons that I recommend routine audits be used across the board, for both DREs and optically scanned paper ballots.

Q5. Dr. Wagner, why is inspection of machine software and hardware not sufficient for trusting a voting system?

A5. As explained in my response to Question 3, it is beyond the state-of-the-art to verify through inspection that the machine software and hardware will work correctly on election day. Given the current state of technology, it is not feasible to verify that the machine software and hardware is free of malicious logic, nor is it feasible to verify that the machine software and hardware is free of defects, flaws, and bugs.

Modern voting software and hardware is too complex to inspect completely. The software in a typical voting machine might contain hundreds of thousands of lines of source code. If all of this source code were to be printed on paper, it would fill thousands of sheets of paper. Each line of source code would have to be inspected manually by software experts, and these experts would have to understand how those lines of source code might interact with each other. This task is too complex to perform with 100 percent confidence; it is simply too easy to miss problems.

The U.S. Tax Code might provide a useful analogy [21]. The tax code also contains thousands of pages of material, and probably no one person understands it in its entirety. The tax code is infamous for containing loopholes that aren't obvious on first inspection; so, too, can source code contain malicious code or defects that aren't obvious on first inspection. At the same time, tax code is written to be interpreted by human judges, who might apply some degree of common sense from time to time; in comparison, software is executed by computers, who are unfailingly literal-minded, so while small ambiguities in the tax code might be minor, small ambiguities in software can be catastrophic. The analogy to the tax code is decidedly imperfect, but it might help provide some intuition about why inspection of voting software and hardware is not sufficient to trust a voting system, given the current state of technology.

A second difficulty is that, given current practice, it is difficult to be sure that the software and hardware that is running on the machine on election day is the same as what has been inspected. The existing technology does not provide any way to verify what software is running on the voting machine. Moreover, some machines have known security vulnerabilities that could allow an attacker to modify the software installed on the machine, so that the software executed on election day differs from the software that was inspected and certified. Also, there have been documented cases where uncertified versions of software were inappropriately installed and used in elections [22,23,24,25].

At the same time, despite these limitations, inspection does have benefits. While it is not sufficient on its own to provide a basis for trust in voting systems, inspection—if done right—is still a good idea that can help reduce the number of voting system failures. Unfortunately, today's voting systems are not currently subject to any meaningful form of inspection by independent parties. The source code is kept secret by vendors, and access is tightly restricted. The federal testing lab—one of

the few parties who are routinely given access to voting source code—do not perform meaningful inspections of source code. (The limited inspection that federal testing labs perform is more analogous to running a spell-checker on a student essay than to checking whether the writing in the essay is grammatical, coherent, meaningful, or persuasive.) In the few cases where independent experts have had the chance to inspect voting source code, they have often found serious flaws in these products which the testing labs overlooked [26]. Consequently, I believe that broader inspections of voting system software and hardware would help improve the reliability and security of elections, even though they are not on their own sufficient and would need to be supplemented with voter-verified paper records and routine manual audits.

Notes

1. David Wagner, Written testimony before U.S. House of Representatives at joint hearing of the Committee on Science and Committee on House Administration, July 19, 2006.
2. "Public Comment on the 2005 Voluntary Voting System Guidelines," ACCURATE Center, submitted to the United States Election Assistance Commission, September 2005.
3. Douglas W. Jones, "Voting System Transparency and Security: The need for standard models," written testimony before the EAC Technical Guidelines Development Committee, September 20, 2004. *http://www.cs.uiowa.edu/~jones/voting/nist2004.shtml*
4. Peter G. Neumann, Written testimony before the California Senate Elections Committee, February 8, 2006. *http://www.csl.sri.com/neumann/calsen06.pdf*
5. Aviel D. Rubin, Written testimony before the Election Assistance Commission, May 5, 2005. *http://avirubin.com/eac.pdf*
6. Tadayoshi Kohno, Adam Stubblefield, Aviel D. Rubin, and Dan S. Wallach, "Analysis of an Electronic Voting System," May, 2004.
7. RABA Innovative Solution Cell, "Trusted Agent Report: Diebold AccuVote-TS System," January 20, 2004.
8. Harri Hursti, Black Box Voting, "Critical Security Issues with Diebold Optical Scan," July 4, 2005.
9. "Security Analysis of the Diebold AccuBasic Interpreter," Report of the California Secretary of State's Voting Systems Technology Assessment Advisory Board, February 14, 2006.
10. Harri Hursti, Black Box Voting, "Critical Security Issues with Diebold TSx," May 11, 2006.
11. Douglas W. Jones, "Connecting Work on Threat Analysis to the Real World," June 8, 2006.
12. "The Machinery of Democracy: Protecting Elections in an Electronic World," Brennan Center Task Force on Voting System Security, June 27, 2006.
13. New Yorkers for Verified Voting, "Analysis of Acquisition Costs of DRE and Precinct Based Optical Scan Voting Equipment for New York State," April 13, 2005. *http://www.nyvv.org/doc/AcquisitionCostDREvOptScanNYS.pdf*
14. Barbara Simons, "Electronic voting systems: the good, the bad, and the stupid," *ACM Queue* 2(7), October 2004.
15. Justin Moore, "How Effective is an Occasionally-Used Paper Ballot?" *http://www.cs.duke.edu/?justin/voting/paper_effectiveness.pdf*
16. Jonathan Bannet, David W. Price, Algis Rudys, Justin Singer, Dan S. Wallach, "Hack-a-Vote: Demonstrating Security Issues with Electronic Voting Systems," *IEEE Security & Privacy Magazine* 2(1), January/February 2004, pp. 32–37.
17. David L. Dill, Bruce Schneier, Barbara Simons, "Viewpoint: Voting and technology: who gets to count your vote?" *CACM* 46(8), August 2003.
18. Douglas W. Jones, "Auditing Elections," *Communications of the Association for Computing Machinery* 47(10), October 2004, pp. 46–50.
19. Aviel D. Rubin, Written testimony before the Election Assistance Commission, June 30, 2005. *http://avirubin.com/vote/eac2.pdf*
20. Roy G. Saltman, "Final Project Report: Effective Use of Computing Technology in Vote-Tallying," NBSIR 75–687, prepared for the Clearinghouse on Election Administration, May 1975.
21. This analogy is taken from Barbara Simons, Jim Horning, "Risks of technology-oblivious policy," *CACM* 48(9), Sept. 2005.

22. "Staff Report on the Investigation of Diebold Election Systems, Inc.," Presented before the California Voting Systems and Procedures Panel, April 20, 2004. *http://www.openvotingconsortium.org/files/shelly_diebold_report*april20*_final.pdf*
23. "Phase II County Voting System Review," R&G Associates, April 19, 2004. *http://web.archive.org/web/20041108230726/http://www.ss.ca.gov/elections/ks_dre_papers/rg_phase_II_revised_report.pdf*
24. "E-Voting Undermined by Sloppiness," Kim Zetter, Wired News, December 17, 2003. *http://www.wired.com/news/evote/0,2645,61637,00.html*
25. "Diebold: Voting machine maker dinged in CA: Auditor says software wasn't approved," Elise Ackerman, *Mercury News,* December 17, 2003.
26. Douglas W. Jones, "Misassessment of Security in Computer-Based Election Systems," *Cryptobytes* 7(2), Fall 2004, pp. 9–13.

ANSWERS TO POST-HEARING QUESTIONS

Responses by John S. Groh, Chairman, Election Technology Council, Information Technology Association of America

Questions submitted by Chairman Vernon J. Ehlers and Chairman Sherwood L. Boehlert

Q1. In his testimony, Dr. Wagner recommended that the Technical Guidelines Development Committee (TGDC) and the Election Assistance Commission (EAC) take the following actions to improve security and reliability of voting systems. For each recommendation listed below, please answer these questions: Do you agree with the recommendation? If so, to what extent and how are voting systems manufacturers implementing the recommendation? If not, why not?

Q1a. Mandate voter-verified paper records and mandatory manual audits.

A1a. Mandated voter-verified paper records: Although today's voting equipment is reliable, accurate, and secure, the ETC and its members recognize that some jurisdictions and/or states prefer the option of a voter-verifiable paper audit trail (VVPAT). In response, most vendors developed VVPAT technical options to meet that customer need. At this time, some states (over half) have developed legislation requiring VVPAT, but the cost of providing that equipment is the burden of the state or jurisdiction. Before a federal agency mandates the use of VVPATs, the ETC recommends that current VVPAT usage be monitored to learn from real-world experience with the technology. Also, it should be anticipated that additional federal funding will be needed to accommodate that mandate.

Mandatory manual audits: The ability to audit an election as prescribed by HAVA and other laws, rules, and regulations is an important requirement of all voting system available today. However, whether or not those audits are manual or automatic is a state or local decision. The ETC and its members regularly work with jurisdictions and/or states to implement and comply with specific election processes and procedures. In considering federally mandated manual audits, it is important to keep in mind that manual audits can provide a verification of election results, but due to human error, a manual audit can also create additional issues that would have to be anticipated and addressed during implementation. Further, there are costs involved in performing manual audits. If a federal agency mandates a manual audit, then additional federal funding will be needed to accommodate that mandate.

Q1b. Expand standards from focusing primarily on functionality testing to incorporate technical evaluations of the security, reliability, and usability of voting machines.

A1b. The EAC 2005 voting systems guidelines expand upon the FEC 2002 standards, particularly in the areas of security, reliability and usability. However, tests and measures for these requirements have not yet been fully defined to where the tests are objective and repeatable.

The ETC and its members, as stakeholders, have contributed to development of the 2005 guidelines and have offered public comment on their implementation. In general, our belief is that technical *and* functional evaluations are both important aspects of the testing process. In fact, technical evaluations against the federal requirements have always been a part of federal certification. *(Please see the attached overview of the current federal certification process.)* Therefore, standards, and accompanying testing, should not focus only on technical or functional aspects of voting equipment, but rather continue to include both in balance.

In addition, federal standards should not be too prescriptive or restrictive. Over regulation by the Federal Government could lead to higher costs, could stifle innovation by slowing reaction to necessary change or technological advances to meet emerging needs, and could intrude on state and local authority or practices.

In considering additional federal action in this area, it is important to keep in mind that the intent of the federal requirements for voting systems has been to establish a "minimum" standard for evaluating voting systems. Each state has the authority to mandate a higher level and quite a few do require higher State level certification standard. However, between states there are sometimes conflicting requirements and there are also issues which are under the authority of the state and not the Federal Government. In the past, the federal standard has tried to not conflict with individual state requirements and to not create requirements which are under a state's authority to mandate. These elements need to be taken into consideration whenever improving the federal standard.

Q1c. Eliminate conflicts of interest in the federal testing process by establishing a new funding process whereby Independent Testing Authorities (ITA) are not paid by the vendors whose systems they are testing.

A1c. There is no influence that the vendors have over the work that the ITAs perform. The ITAs are testing to a standard as they would test any system to a standard. The ITAs are accountable to the EAC for the testing to that standard, regardless of whether the ITAs are paid by the vendors or by some other funding mechanism.

This situation is similar when a car owner takes car into an auto service shop for required state emission testing to meet federal or state standards. The car owner pays for the testing; however, he or she has no influence over whether your vehicle passes the test or not. The service shop is accountable to the state or local jurisdiction for testing to the required standard.

While there may be other issues to consider in evaluating the merits of providing federal funding for this function, conflict of interest need not be one of them.

Q1d. Reform the federal testing process to make all ITA reports publicly available and documentation and technical package data available to independent technical experts.

A1d. The EAC is reforming the format of the ITA reports so that they may be released to the public without compromising intellectual property. The ETC vendor members endorse the public release of the testing process and the testing results. The ITA reports that exist today could be released to the public if they didn't contain the intellectual property that is inherently embedded into them. The ETC is hopeful that the EAC's reformatting of the ITA reports will allow the testing information to be publicly available.

However, the Technical Data Packages (TDPs) contain intellectual property of commercial value to the vendor and therefore are held as confidential and cannot be released to the public. The TDP could be made available to designated independent technical experts but only with acceptable and binding non-disclosure agreements signed between the independent expert and the vendor. Vendors have invested millions of dollars in research and development to produce their product lines and to compromise that investment without compensating the vendor would not be economically viable.

Q1e. Require broader disclosure of voting system source code, at a minimum to independent technical experts under appropriate non-disclosure agreements.

A1e. See response above for question (d).

Q1f. Institute a process for collecting, investigating, and acting on data from the field on performance of voting equipment, including a mechanism for interim updates to the standards to reflect newly discovered threats to voting systems.

A1f. Although we would need additional detail about the form, function, and approach, the ETC agrees with the general concept. Currently, there is a lot of misinformation about the performance of voting equipment. As a result, voter confidence is unnecessarily compromised. It could be beneficial to the public to task an agency which understands the environment and "totality of circumstances" in which voting equipment is used as an entity to investigate issues and report objectively on their factual findings. That effort could provide a level of transparency for the public and a level of fairness and truth in reporting to the election industry and the general public.

Q1g. Increase the representation of technical experts in computer security on the TGDC.

A1g. If the tests and measures defined are objective and repeatable, increasing the representation of computer security experts will not add any value; it would not matter who tested the equipment, as the results would be similar. With subjective tests and measures, having more technical experts will just provide more differing opinions without agreement. Passing the security tests would then be a matter of who tested it and not whether it met a standard. The goal should be to define more objective tests and measures for security requirements, and on this point computer security experts could play a role. An effort was made but never concluded during the IEEE P1583 project to gain agreement on an objective and repeatable set of tests and measures to evaluate voting system security. Computer security experts could focus their efforts on completing the process.

Q2. How do you think the sections of the 2005 Voluntary Voting Systems Guidelines (VVSG) that deal with security should be improved? Do you think that the way

in which security for voting systems is tested needs to change, and if so, how, and if not, why not?

A2. Although the 2005 VVSG have enhanced the security requirements for voting systems, the testing of those requirements has not been well enough defined. The tests currently proposed are very subjective, if they exist at all. Studies need to be performed to develop tests and measures that are objective and repeatable, otherwise, success in testing will be a matter of who tests the equipment and not the standard to which it is tested. If tests and measures are objective and repeatable, it should not matter who tests a voting system as the test results should be the same or similar between testers.

Q3. In your testimony you described an idea for phased implementation of the 2005 VVSG. Please explain in more detail how a phased implementation would work? Are there parts of the 2005 VVSG that could be implemented now?

A3. Voting systems certified to the 2002 federal standards should be grandfathered-in under the 2005 standard until additional federal funding is provided to states and local jurisdictions to support purchasing on newly upgraded equipment. Additionally the timeframe for transition to a new voting system certified under the 2005 VVSG could be allowed over an eight year period, or two voting cycles.

Q4. The 2005 VVSG contains an appendix on independent dual verification systems that could perform the same functions as a voter-verifiable paper audit trail. Is this technology being used in voting systems today or is more research needed to make it operational? What are the advantages and disadvantages of this technology? To what extent are there other technologies that could perform the same function as a voter-verifiable paper audit trail?

A4. Independent dual verification (or IDV) is a good concept, but there are technological as well as economic and usability factors that must be considered before implementing such a solution. This includes:

- Complexity for the voter and poll worker.
- Added costs for the jurisdiction in having two independent systems for each voting station (including material, storage, transportation)

Currently, some claim that other technologies could perform the same function as a VVPAT, however it is important to point out that, when compared to paper, those technologies are more complex for voters and poll workers to understand and trust, and those technologies are more costly then paper-based verification systems. Any requirement must be valued and measured against the real-world application and use. The goal should be to make the voting process easier for all voters and to encourage them to come out and vote not to add additional complexities that may have the opposite affect.

Questions submitted by Democratic Members

Q1. Mr. Groh, do vendors currently provide election officials with documentation that explains the security features of their systems that they sell and the procedures required for an election to be secure. If not, is this something they should provide to election officials?

A1. Yes, vendors do provide election officials with documentation that explains the security features of their systems. Vendors also provide best practices on using the equipment securely, however it is up to the State and the Local Election jurisdiction to establish and perform those processes as they establish as a best practices.

Q2. Mr. Groh, do you have any concerns about how to interpret the 2005 standards/guidelines? Are you satisfied with mechanisms for addressing questions and issues arising from the guidelines during the two-year transition period?

A2. Yes, the ETC members do have concerns on the interpretation of the 2005 VVSG. *First,* there is some ambiguity in the standards that will require interpretation, and certain clarifying answers will be profound. *Second,* some requirements conflict with one another and will have to be resolved. *Third,* some requirements are not yet technologically feasible and/or will likely to impact overall cost of the newly enhanced equipment. *Finally,* currently there are requirements that do not have well defined tests if they have any tests defined at all. Some of the tests are very subjective in their measurement and could depend on who performs the test as to whether a voting system will pass or fail. The pre-established tests for each

requirement should be objective and repeatable so that it does not matter which ITA performs the test.

The mechanisms for addressing questions and issues are still being defined by the EAC. Those mechanisms will likely not be implemented until the EAC adopts a *Full Certification Process* in December 2006. Currently, the EAC has only adopted an Interim Certification Process which only allows modifications to existing certified voting systems to be tested and does not allow a vendor to submit a new product or accessory for federal certification under the 2005 VVSG.

Prior to the date when those mechanisms are implemented for 2005 VVSG certification, the ETC is working with NIST (the authors of the 2005 VVSG) to better understand the intent of the new requirements so that voting systems can be developed to comply. However, as there will likely be a learning curve in applying the new standard to evaluations of voting systems, and a learning curve in applying the new interpretation mechanisms, there will likely be delay in the certification of voting systems to the VVSG 2005 standard.

The ETC members have been in contact with the EAC, formally asking for more clarity on the new certification process and procedures they are rolling out. We have received feedback, but there are still open questions we are working with the EAC to reach full clarification.

Regarding opportunities to address questions and issues about pertaining to implementation of the 2005 guidelines, the ETC and its members are still awaiting clarification of the actual mechanisms for doing so. We do, as described above, have concerns and would welcome the opportunity to engage in direct discussion and deliberation about the challenges we and election administrators could face. At this point, our input has been limited to working with NIST (the authors of the 2005 VVSG) to better understand the intent of the new requirements so that voting systems can be developed to comply.

Q3. Mr. Groh, does ITAA or its Election Technology Council specify or endorse any testing or product quality standards or processes for its members that supplement the Election Assistance Commission's voting system standards? If so, what are they?

A3. The Election Technology Council does not specify or endorse testing or product quality standards or processes. Rather, we contribute to the guideline and standards development process by providing our expertise as developers and Subject Matter Experts (SMEs) of voting technology. The current federal standards process is thorough and rigorous, but also on-going and regularly updated to reflect emerging needs or technical opportunities. This process has worked well to incent continually updated and enhanced voting system options.

At the same time, the federal standards provide a minimum benchmark. States and jurisdictions are able to expand and mandate higher standards than the EAC's standard. In fact, many states do have laws and rules which require testing and product quality above the EAC standard.

Q4. Mr. Groh, reports of problems in Indiana, West Virginia, Michigan and Texas elections—among others—indicate that voting systems are being delivered to jurisdictions for the 2006 election with reliability and accuracy problems that could affect election results. What steps are your organization and its membership taking to respond to actual and potential voting system problems that have surfaced during recent primaries?

A4. The ETC is a trade association and cannot comment on the specific issues of individual member companies. A vendor member company would have to provide information to specific reported issues with their systems and the state or local election jurisdiction they serve. However, in general, it is important to keep in mind that implementation of the *Help America Vote Act* has created the greatest transformation in the way elections are run since the *Voting Rights Act* of the 1960s. This is a time of tremendous change and that change has presented challenges to not only election vendors, but election officials and voters, as well. In each case, it is important to keep in mind the human element in carrying out elections, and that vendors and election officials have a shared responsibility in the process. Though reliability of the voting equipment is critically important, so too are processes, procedures, and training.

Q5. Mr. Groh, you warn that election officials must exercise caution against taking shortcuts in important areas such as training, testing and preparation. Could you provide some examples of what you are talking about and are there cases where this is taking place?

A5. The observation was a general one related to the importance of thorough training, testing, and election preparation. With the compressed timeline against nationwide implementation of the Help America Vote Act, it is important to emphasize that these areas must not be compromised and, in fact, must be enhanced given the greater complexities around newer voting technology. Specific examples would include training on ADA sensitivity; voter outreach; poll worker training; and total system pre-election testing of equipment.

Q6. Mr. Groh, you mention that increasing complexity required of voting systems by the standards/guidelines is creating a need for more using training and that the vast majority of problems experienced with voting systems are attributable to insufficient training and preparedness in the polling place. Would you describe the training and operation manuals your membership provides to local election officials?

A6. The Election Technology Council does not develop or provide training and operation manuals to local election jurisdictions. Each vendor company develops training and operation documentation relevant to their own specific voting systems. In addition, most have developed materials specifically geared toward educating voters about the use of new voting systems for use by the local election jurisdictions. From the ETC perspective, it is important to point out that even with the detail of the manuals provided to local jurisdictions, to be effective, these materials must be read, they must be used, and, they must be localized to include jurisdiction-specific processes, procedures, policies, and documentation.

In addition, the Election Assistance Commission (EAC) has developed material providing best practices-based guidance to elections officials and is in the process of developing and releasing by end of September 2006 a newly revised edition of *"Best Practices Guidelines"* which will compliment the *"Quick Start Guide"* they released in June 2006.

Q7. Mr. Groh, Dr. Wagner made a number of short-term recommendations based on the Brennan Center report that he believes could improve the security and reliability of voting equipment that will be used this November. These recommendations include routine audits of voter-verified paper records, performing parallel testing of voting machines, adopting procedures for investigating and responding to evidence of fraud or error, and banning voting machines with wireless capabilities. Would you please comment on these suggestions?

A7. First, it is important to state that the ETC members takes strong exception to much of Dr. Wagner's testimony. In our response to other questions from the committee, we provide comment on some of the general concepts contained in Dr. Wagner's recommendations. Overall, in response to his testimony, it is important to point out that The ETC endorses recommendations to enhance the security and integrity of elections by using the voting systems security features which were designed to be used in concert with security procedures and personnel.

For more perspective on the Brennan Center Task Force report on voting system security, please read the Election Technology Council response. It is available for review and download at:
http://www.electiontech.org/downloads/ETC-BRENNANCENTER%20RESPONSE-FINAL.pdf

Q8. Mr. Groh, Dr. Wagner's testimony outlines problems that we frequently see reported in news articles about problems with voting equipment. In addition to his comments on the current status of voting equipment, he makes a number of longer-term recommendations, many which focus on conformance criteria and testing of voting machines. Would you please comment on these recommendations?

A8. Please see response to question 7 above and responses to other questions from the Committee.

Appendix 2:

Additional Material for the Record

STATEMENT OF THE U.S. PUBLIC POLICY COMMITTEE OF THE ASSOCIATION FOR COMPUTING MACHINERY

The U.S. Public Policy Committee for the Association for Computing Machinery (USACM), commends Congress for reviewing issues related to voting machines, testing practices and standards. Ensuring that voting is accurate, error-free, secure and accessible to all registered voters is of great importance. However, as experts in computing, we have grave reservations about the safeguards in place with many of the computerized voting technologies being used. New federal standards and a certification process hold promise for addressing some of these problems, but more must be done ensure the integrity of our elections. We recommend that Congress and the Election Assistance Commission (EAC):

- Create a formal feedback process that will ensure that lessons learned from independent testing and Election Day incidents are translated into best practices and future standards.
- Make the testing process more transparent by making the testing scope, methodologies and results available to the public.
- Ensure that the guidance for usability and security standards provides performance-based requirements and is clear so as to minimize the variance of human interface designs from jurisdiction to jurisdiction.
- Create a mechanism for interim updates to the standards to reflect emerging threats, such as newly discovered security defects or attacks.
- Require voter-verified paper trails and audits to mitigate the risk associated with software and hardware flaws.

Testing, Certification and Reporting

Thirty-nine states require federal certification of their voting systems, which is currently handled by independent testing authorities (ITA). They test the systems against the 2002 Voting System Standards (VSS). Ideally this testing would discover any flaws in the system and allow for corrections before subsequent elections. However, in May 2006, a new report[1] was issued outlining several security vulnerabilities in one brand of certified electronic voting machines. Many computer scientists were stunned by the fundamental nature of these defects, and noted that the reported defects were the most egregious security vulnerabilities known to date. This was not, however, the first time serious security vulnerabilities were revealed.[2,3,4]

There are several gaps in our testing and certification system that need to be addressed even if we have more robust standards for voting systems. First, there is no corrective mechanism to ensure that flaws found during testing are fixed before subsequent elections. Second, the guidelines are being construed quite narrowly; if a flaw is found that is not explicitly prohibited by the guidelines, a system is still certified. It is unclear how such flaws can be successfully addressed under the current certification process. Finally, there is a clear need to create a formal system for reporting problems in the field and improving the standards based on these reports. This step will allow election officials throughout the country to be informed of potential problems and that experiences can inform the federal standards.

Under the *Help America Vote Act* (HAVA) the EAC is responsible for certifying voting systems through accredited laboratories. The National Institute of Standards and Technology (NIST) is taking over the accreditation process of ITAs from the National Association of State Election Officials. Federal involvement may make the testing and certification process more independent, but not necessarily more transparent.

---

[1] Harri Hursti, May 11, 2004, "Diebold TSx Evaluation Black Box Voting," Black Box Voting, *http://www.blackboxvoting.org/BBVtsxstudy.pdf*

[2] Tadayoshi Ohno, Adam Stubblefield, Aviel Rubin, Dan Wallach, May 2004, "Analysis of an Electronic Voting System, IEEE Symposium on Security and Privacy 2004." IEEE Computer Society Press, *http://avirubin.com/vote.pdf*

[3] RABA Technologies LLC, January 20, 2004. "Trusted Agent Report Diebold AccuVote-TS Voting System," *http://www.raba.com/press/TA_Report_AccuVote.pdf*

[4] David Wagner, David Jefferson, Matt Bishop, February 14, 2006, "Security Analysis of the Diebold AccuBasic Interpreter," California Voting Systems Technology Assessment Advisory Board, *http://www.ss.ca.gov/elections/voting_systems/security_analysis_of_the_diebold_accubasic_interpreter.pdf*

[1] Lawrence Norden et al., *The Machinery of Democracy: Protecting Elections in an Electronic World* (Brennan Center for Justice ed., 2006), available at *http://www.brennancenter.org/programs/downloads/SecurityFull7-3Reduced.pdf.*

[2] For a complete list of the Task Force Members, see *The Machinery of Democracy* at i.

Currently, voting machine vendors are the clients of the ITAs. Typically, they are the only recipients of the testing results, which are considered to be proprietary. This is not unusual. Certification testing of other products that the public relies on, such as aviation software and medical devices, is also proprietary. A key difference is that if an aviation system fails, the failure is reported to the FAA and investigated. If a medical device fails, the FDA investigates. Where the investigation demonstrates flaws in the management, manufacture, design, or testing of the aviation system or medical device, these flaws become public record and the operating rules and or equipment standards are adjusted accordingly. Investigation reports are public records.

Our country is far from having any such formal system for voting. We should have a system to ensure that lessons learned from multiple jurisdictions are feedback to vendors, states and federal officials, and then incorporated into standards and best practices. Often the real-world conditions of an election reveal errors that have not been detected by testing. The only organized incident reporting system for voting equipment that has been employed recently is a limited, all-volunteer project sponsored by several non-profit groups.

Further, Congress should seek to make the certification process and testing results more transparent, and, like incident reporting, have a formalized system for incorporating the results into federal standards. The public should know the results of voting system tests and the certification tests of ITAs. California and New York State are taking steps to make their processes more transparent. Federal incentives also could strengthen the independence and transparency of the testing process. Incident reporting and transparent testing results would make it much more likely that vendors and elections officials would implement the lessons learned both from their own practices and from other jurisdictions.

Voting Guidelines

The new 2005 Voluntary Voting System Guidelines (VVSG) improve on the 2002 VSS, but they are not sufficient for ensuring that electronic voting systems are secure, reliable, usable and verifiable. It is unclear whether the level of guidance in the 2005 VVSG is adequate to guarantee that all eligible voters will be able to understand and use the new voting systems. In the area of human factors, the 2005 standards still leave too much to the discretion of local jurisdictions and are based on functional requirements instead of performance-based requirements. This is also a general problem with the security standards. While the EAC recognizes the problem, it is not in a position to act quickly.

The guidelines process is far from timely. The 2005 VVSG will take effect in December 2007—two years after the standards were approved. In that timeframe it is difficult to refine the guidelines to handle problems not already covered. NIST is helping develop the next VVSG, but that will likely not be implemented before elections in 2010. Viruses and other security attacks operate in minutes and days, not months or years. A new method of developing and implementing interim guidelines quickly is necessary to respond to new problems.

Paper Trails and Audits

Even with improved standards and a process more responsive to emerging threats, the best designed and tested systems will continue to have flaws. We've seen numerous examples of security threats in software for commercial systems and critical infrastructures. Flaws, unfortunately, are inherent in any complex software system. There are formal mathematical proofs that testing is incapable of finding all accidental software flaws, and finding purposely concealed flaws is even more difficult. It is also possible to have unanticipated hardware or operational failures as well as accidents that can corrupt or lose vote totals held in memory of some voting machines.

To mitigate these risks we recommend paper trails and audits. Voting systems should enable each voter to inspect a physical record to verify that his or her vote has been accurately cast, and to serve as an independent check on the result produced and stored by the system. Making those records permanent—not based solely in computer memory—allows for an accurate recount. We are encouraged by the actions of 36 states that have either established voter-verified paper trails as law or purchased equipment capable of providing voter-verified paper trails.

Thank you for taking the time to consider this important issue. Ensuring that computer based systems are secure, reliable, usable, and ultimately trustworthy will require ongoing involvement of technical experts, usability professionals, voting rights advocates, and dedicated election officials in the U.S. and other countries. We stand ready to provide technical guidance to Congress on this and other issues.

Please contact ACM's Office of Public Policy should you have any questions at (202) 659–9712.

About ACM

ACM, the Association for Computing Machinery, is an educational and scientific society uniting the world's computing educators, researchers and professionals to inspire dialogue, share resources and address the field's challenges. ACM strengthens the profession's collective voice through strong leadership, promotion of the highest standards, and recognition of technical excellence. ACM supports the professional growth of its members by providing opportunities for life-long learning, career development, and professional networking.

ABOUT USACM

The ACM U.S. Public Policy Committee (USACM) serves as the focal point for ACM's interaction with U.S. Government organizations, the computing community, and the U.S. public in all matters of U.S. public policy related to information technology. Supported by ACM's Washington, D.C., Office of Public Policy, USACM responds to requests for information and technical expertise from U.S. Government agencies and departments, seeks to influence relevant U.S. Government policies on behalf of the computing community and the public, and provides information to ACM on relevant U.S. Government activities.

STATEMENT OF LAWRENCE NORDEN
CHAIR, TASK FORCE ON VOTING SYSTEM SECURITY
BRENNAN CENTER FOR JUSTICE
NEW YORK UNIVERSITY SCHOOL OF LAW

The Brennan Center thanks the Committees on House Administration and Science for holding this joint hearing. We especially thank Chairman Ehlers for his leadership in taking steps to ensure that our elections are as fair and secure as possible.

The Voluntary Voting System Guidelines ("VVSG") considered at the joint hearing today can, and should, be a cornerstone in the shared federal and state effort to ensure elections that are secure, accurate and accessible. However, in their current form, the VVSG fail to achieve that goal. After summarizing the recently completed work of the Brennan Center Task Force on Voting System Security (the "Brennan Center Security Task Force"), I will review the very serious gaps in the security, usability and accessibility of current systems that have gone unaddressed in the VVSG. Until these looming problems are confronted and remedied, the machinery of American elections will remain a legitimate concern for all of us who care about the health of our democracy.

I. Report of the Brennan Center Task Force: The Machinery of Democracy: Protecting Elections in an Electronic World

Over the past year-and-a-half, the Brennan Center has worked with leading technologists, election experts, security professionals, and usability and accessibility experts to review the current state of voting systems in the United States. Three weeks ago, we released the first study from this collaboration, *The Machinery of Democracy: Protecting Elections in an Electronic World* (the "Brennan Center Security Report")[1] In the coming weeks, we will be releasing comprehensive reports on the usability and accessibility of voting systems.

The Brennan Center Security Report was a summary of the Nation's first systematic analysis of security vulnerabilities in the three most commonly purchased electronic voting systems. This threat analysis was conducted by the Brennan Center Task Force[2] and revealed that all three voting systems have significant security and reliability vulnerabilities; the most troubling vulnerabilities of each system cannot be substantially remedied; and few jurisdictions have implemented any of the key security measures that could make the least difficult attacks against voting systems substantially more secure.[3]

The Task Force surveyed hundreds of election officials around the country; categorized over 120 security threats; and evaluated countermeasures for repelling attacks. The report of the Task Force concluded:

- **All of the most commonly purchased electronic voting systems have significant security and reliability vulnerabilities.** All three systems are equally vulnerable to an attack involving the insertion of corrupt software or other software attack programs designed to take over a voting machine.
- **Automatic audits, done randomly and transparently, are necessary if paper records are to enhance security.** The report called into doubt basic assumptions of many election officials by finding that using voter-verified paper records without requiring automatic audits—as is done in twenty-four states—is of "questionable security value."
- **Wireless components on voting machines are particularly vulnerable to attack.** The report finds that machines with wireless components could be attacked by "virtually any member of the public with some knowledge of software and a simple device with wireless capabilities, such as a PDA."
- **The vast majority of states have not implemented election procedures or countermeasures to detect a software attack** even though the most troubling vulnerabilities of each system can be substantially remedied.

Among the countermeasures advocated by the Task Force are routine audits comparing voter-verified paper trails to the electronic record; and bans on wireless components in voting machines. Currently only New York and Minnesota ban wireless components on all machines; California bans wireless components only on DRE machines. The Task Force also advocated the use of "parallel testing": random, Election

[3] *Id.* at 3.
[4] *Id.* at 8.
[5] Although there is no firm consensus on precise benchmarks to measure the usability of vot-

Day testing of machines under real world conditions. Parallel testing holds its greatest value for detecting software attacks in jurisdictions with paperless electronic machines, since, with those systems, meaningful audits of voter-verified paper records are not an option.

II. Scientific Threat Analyses Should be the Basis for Guidelines on Security and Reliability

The threat analysis performed by the Brennan Center Task Force on Voting Security involved (a) identifying and categorizing potential threats to voting systems, (b) prioritizing these threats based on level of difficulty, and (c) determining how much more difficult each of the catalogued attacks would become after various sets of security measures were implemented.[4]

To our knowledge, neither the Election Assistance Commission (the "EAC"), nor state election officials have undertaken similar comprehensive analyses before adopting voting system security and reliability guidelines. *The Brennan Center Security Report shows that unless the EAC and the States commission such studies and use them to establish security guidelines for each VVSG-certified system, voting system security measures are likely to continue to fail to address important security and reliability concerns.*

The Brennan Center Security Report and threat analysis demonstrate that merely assuming machines are programmed and configured correctly, without some independent form of verification such as a voter-verified paper record, is a significant security and reliability risk. Ultimately, if we are to have confidence in the accuracy of our voting systems, all voting machines must have some form of independent dual verification, in which the verification is audited against the official record.

III. Usability Testing Is the Key to Ensuring that Voter Intention Is Accurately Recorded

The performance of a voting system is measured in significant part by its success in allowing a voter to cast a valid ballot that accurately reflect her intended selections without undue delays or burdens. This system quality is known as "usability."[5] Following several high profile controversies in the last few elections—including, most notoriously, the 2000 controversy over the "butterfly ballot" in Palm Beach County, Florida—voting system usability is a subject of utmost concern to voters and election officials.

The current VVSG requires that the "voting process shall provide a high level of usability for voters."[6] It includes many valuable guidelines for vendors and election officials. Unfortunately, it does not require the kind of usability testing by users and experts that is necessary to ensure that voter intentions are recorded as accurately as possible. To date, only a few studies have compared different ballots directly or definitively determined what makes one form of ballot more usable than another—i.e., less prone to producing errors, more efficient, and more confidence-inspiring.[7] Without such information, it is impossible to create systems and procedures that will reduce voter error.

As it contemplates future drafts of the VVSG, the Brennan Center strongly urges the EAC to commission further study of usability issues, such as "incidental undervoting, over-voting, or any other inaccuracies that are products of the human/system interaction."[8] Moreover, regardless of the voting system used, election officials should conduct usability testing in their local communities on proposed ballots *before* finalizing their design.

---

[4] *Id.* at 8.

[5] Although there is no firm consensus on precise benchmarks to measure the usability of voting systems, academics and industry researchers have developed design guidelines in other areas, most importantly in web-browser design, that can increase usability. See Sanjay J. Koyanl et al., U.S. Dept. of Health and Human Resources, *Research-Based Web Design and Usability Guidelines* (Sept. 2003), available at *http://usability.gov/pdfs/guidelines_—book.pdf*

[6] Election Assistance Commission, *Voluntary Voting System Guidelines,* Volume I Version 1.0 at § 3.1 (2005), available at *http://www.eac.gov/VVSG%20Volume_I.pdf,* [hereinafter EAC VVSG].

[7] See Jonathan Goler, Ted Selker, and Lorin Wilde, *Augmenting Voting Interfaces to Improve Accessibility and Performance* (2006), available at *http://vote.caltech.edu/reports/chi-abstract-golerselker.pdf;* Ted Selker, Matt Hockenberry, Jonathan Goler, and Shawn Sullivan, *Orienting Graphical User Interfaces Reduces Errors: the Low Error Voting Machine,* available at *http://vote.caltech.edu/media/documents/wps/vtp_wp23.pdf*

[8] Accurate, *Public Comment on the 2005 Voluntary Voting System Guidelines* at 26 (Sept. 30, 2005), available at *http://accurate-voting.org/accurate/docs/2005_wsg_comment.pdf.*

IV. Assessments of System Accessibility Must Include Full Range of Disabilities and Entirety of Voting Process

Traditionally, many voters with disabilities have been unable to cast their ballots without assistance from personal aides or poll workers. Those voters do not possess the range of visual, motor, and cognitive facilities typically required to operate common voting systems.

The *Help America Vote Act of 2002* ("HAVA") took a step forward in addressing this longstanding inequity. According to HAVA, new voting systems must allow voters with disabilities to complete and cast their ballots "in a manner that provides the same opportunity for access and participation (including privacy and independence) as for other voters."[9] For voting systems to become truly accessible to all voters, members of disabled populations should be included in empirical research to ensure that vendors have satisfied VVSG requirements.[10] In particular, assessments of such systems should:

- *Examine each step a voter must perform, starting with ballot marking and ending with ballot submission.* Systems that may provide enhanced accessibility features at one stage of the voting process may be inaccessible to the same voters at another stage in that process.
- *Take into account a full range of disabilities and ensure that accessible features are fully usable by people with disabilities.* When selecting participants for system tests, officials should include people with sensory disabilities (e.g., vision and hearing impairments), people with physical disabilities (e.g., spinal cord injuries and coordination difficulties), and people with cognitive disabilities (e.g., learning disabilities and developmental disabilities). Given the rising number of older voters, officials should take pains to include older voters in their participant sample. Ensuring that the entire process is as easy to use as possible for voters with disabilities is the only way of creating real accessibility.
- *Use full ballots that reflect the complexity of a real election.* A simplified ballot with only a few races or candidates may produce misleading results.

V. Conclusion

The VVSG is a piece of a larger effort occurring on many fronts to improve the machinery of our elections. Given the leadership responsibilities of the EAC, the VVSG must set a high standard. The guidelines should be informed by the scientific testing methods used successfully to assess the risks of other widely-deployed technologies; and by the real-world experiences of the voting populations likely to be thwarted by voting systems that fall short on accessibility and usability.

Refinements to the VVSG that I've recommended would, if adopted, move us several steps closer to the goal of fair, accessible and secure elections.

---

[9] *Help America Vote Act* 42 U.S.C. § 15481(a)(3)(A) (2002).

[10] See also *Accurate Public Comment* at 29.

Comments on the 2005 VVSG

Presented to the July 19 Joint Committee Hearing on the 2005 VVSG

Roy Lipscomb
Directory of Technology
Illinois Ballot Integrity Project
http://ballot-integrity.org
contact@ballot-integrity.org
773/262-5927

Submitted August 18, 2006

Text:

2.3.3.1 Common Requirements

"c. Record the selection and non-selection of individual vote choices for each contest and ballot measure."

Recommendation 1:

Add:

"Ideally, this will include an explicit checkbox for "None of the Above" (or a similar phrase) in all contests."

Discussion 1:

1. Unintentional undervotes will be eliminated if this option is available and if the voter is required to mark at least one checkbox in each contest.

2. Many voters wish to have such an option.

3. The word "Abstention" might be preferable, since it is suitable for appearing in multiple checkboxes, in contests where the voter can make multiple selections.

Recommendation 2:

Add:

"g. Impress upon the voter the critical importance of personally reviewing and confirming each copy of the ballot for complete accuracy before casting it. This can be accomplished though prominent informational and warning messages, through public service announcements, and through other appropriate means."

Discussion 2:

1. This pertains not only to VVPATs, but to paper-only ballots as well.

In a recent experiment, 16% of the paper-only ballots had errors[1]. If this is anywhere near the rate in the field, uncorrected errors by voters can skew the outcome of elections.

2. Studies show that few voters actually verify their paper record. In one study, 47% of voters entirely ignored the paper record[2]. In another study (one which I encountered several months ago, but did not save) the figure was 10%.

If these figures are representative, the reputation of VVPATs as constituting a substantially "voter-verified" data set is illusory.

3. By now, this deficiency is undoubtedly well known to potential malefactors, and can be used by them to advantage.

In certain demographics, where verifying the paper record is known to be low, a machine may be reconfigured to produce a certain percentage of incorrect paper records.

a. If none of those records are noticed, or if they are ignored, the machine totals are successfully skewed.

b. If one of them is noticed and reported, any earlier, unreported ones will most likely be retained as official and accurate, even though the machine will now be taken out of service.

Text:

2.3.3.3 DRE System Requirements

"k. For electronic image displays, prompt the voter to confirm the voter's choices before casting his or her ballot, signifying to the voter that casting the ballot is irrevocable and directing the voter to confirm the voter's intention to cast the ballot."

Recommendation:

As I argue above, this should be recommended for paper-only ballots as well.

Text:

2.3.4 Broadcasting Results

(Intentionally unquoted)

Recommendation:

Add:

"d. When all polling places in the election have closed, allow for publication of copies of all individual ballots, in a way that does not compromise the privacy of any voter, or the anonymity of any ballot."

Discussion:

If voter anonymity is fully perserved, there is no reason to preclude the publication of the individual ballots from each polling place.

(The presumption is that each polling place has a sufficient number of voters that identifying any particular voter's ballot would be essentially impossible.)

The advantage of publishing the copies of the ballots is that the general public is now enabled to review and confirm the vote count. This reduces or eliminates controversy about possible miscounts.

Text:

7.8.1 Overview

"The verification processes for the two cast vote records must be independent of each other, and at least one of the records must be verified directly by the voter."

Recommendation:

See next item, below.

Text:

7.8.2 Basic Characteristics of IV Systems

"The voter verifies the content of each cast vote record and either (a) verifies at least one of the records directly or (b) verifies both records indirectly if the records are each under the control of independent processes.

"Discussion: Direct verification involves using human senses; for example, directly reading a paper record via one's eyesight. Indirect verification involves using an intermediary to perform the verification; for example, verifying an electronic ballot image on the voting machine."

Recommendation:

Alll "indirectly verified" documents should be classed as unofficial only.

Discussion:

"Indirect verification" of votes defeats the objective of "voter verification."

The objective is to eliminate the possibility of intermediary error.

To employ an intermediary (the voting machine) during the verification retains the possibility of intermediary error.

Text:

7.9.1 Display and Print a Paper Record

(Intentionally unquoted)

Recommendation:

Add:

"d. All vote data on the paper record shall be in a form that the voter can easily and readily verify."

Discussion:

1. Any data not conforming to the above clause is not "voter-verifiable."

2. Barcoded vote-data is not "voter verifiable." Random audits of barcodes do not alter this fact.

3. An argument can be made that barcode data on a VVPAT constitues a separate record from the voter-verifiable data on the VVPAT.

4. If a barcode on a voter's paper record is used to count the votes, an argument can be made that a voter-*un*verified record was used for that counting.

Text:

7.9.3 Electronic and Paper Record Structure

"g. The paper record shall be created such that its contents are machine readable.

"Discussion: This can be done by using specific OCR fonts or barcodes."

Recommendation:

Eliminate "or barcodes" from the above clause.

Discussion:

Barcodes violate the voter-verifiability requirement of the VVPAT.

Text:

7.9.7 VVPAT Accessibility

"Discussion: For example, the accessible voting equipment might provide an automated reader that converts the paper record contents into audio output."

Recommendation:

1. This should be a requirement rather than an option.

2. The automated reader must be a device separate from and independent of the voting machine itself.

Discussion:

1. The VVPAT is intended to be the official vote record for audits and recounts. Thus, the VVPAT is the vote record that should be verified by the voter.

2. Having the voting machine (or an attachment to it) intervene between the VVPAT and the voter violates the checks and balances available to sighted voters.

Footnotes:

1. http://www.usenix.org/events/evt06/tech/full_papers/greene/greene.pdf

" A Comparison of Usability Between Voting Methods. Kristen K. Greene, Michael D. Byrne, and Sarah P. Everett; Department of Psychology, Rice University."

Excerpt: "To review: able-bodied, sighted college students and Houston residents who had previously voted in an average of 10 elections made errors on 4% of the contests ....The scientists also checked the error rate "by ballot" and found that "nearly 16% of the ballots contained at least one error."

2. http://www.lombardoconsultinggroup.com/nvvotersurvey.pdf (That file is no longer available at the original site. A copy is posted at http://e-grapevine.org/nvvotersurvey.pdf)

STATEMENT OF THE NATIONAL COMMITTEE FOR VOTING INTEGRITY (NCVI)

"Elections require an end-to-end concern for a wide variety of integrity requirements, beginning with the registration process and ballot construction, and continuing through vote tabulation and reporting."—Peter Neumann

Our thanks go to the Committees for holding this joint hearing, *"Voting Machines: Will New Standards and Guidelines Help Prevent Future Problems?"* We would like to offer a special thanks to Chairman Ehlers for his leadership on these important issues, which are challenging to our nation's public election's process.

General Comments

The Voluntary Voting System Guidelines (VVSG) is an improvement in some respects over the standards created by the Federal Election Commission process for 1990 and 2002: the increased attention to accessibility for voters with disabilities and language minorities is a step forward over previous voting technology standards. However, the document's treatment of security, transparency, and auditability reflects no improvement over previous standards. In fact some sections of the VVSG pose serious challenges to election integrity and voter privacy.

Current State of Voting System Certification

We are very troubled by the decision of the EAC to keep in place the existing voting technology certification process beyond the period designated by HAVA. On August 18, 2005, the EAC announced that the current voting technology certification process will be in place until the spring of 2007, with only one change: instead of the National Association of State Elections Directors (NASED) providing oversight of the three NASED approved laboratories the EAC will perform that function.

> "Provide for interim accreditation of National Association of State Election Directors (NASED) accredited Independent Test Authorities (ITA). The EAC will develop a process to temporarily accredit current NASED ITAs. This temporary EAC accreditation is needed to ensure that certified test laboratories are available in the near term. It has been determined that the EAC will not receive a recommended list of testing laboratories from the NIST National Voluntary Laboratory Accreditation Program (NVLAP) until the spring of 2007." [1]

Allowing the current three certification laboratories to remain until the spring of 2007, as the only accredited laboratories that can certify voting systems intended for use in public elections, will not have a temporary effect. This decision will negatively affect those laboratories that have shown an interest in being accredited to certify voting technology. It may also diminish the intended results of the promulgation of new voting technology standards, and undermine public confidence in the accreditation and certification process. We strongly object to the continuation of the NASED ITA established voting technology laboratory accreditation and certification process because it allows failed voting technology to pass certification, is in violation of HAVA Section 231(b)(1), ignores the work already begun by NIST to replace the NASED ITA process, and hinders transparency.[2]

The widely reported failures of voting systems, which have passed NASED ITA certification, cannot be ignored. The failures are too numerous to summarize in this letter, but a few of the more notable ones are worth recounting:[3]

> Sarpy County Recount (Nebraska): As many as 10,000 phantom votes were added in 32 of 80 precincts when a machine error doubled the votes during counting. Source: Channel Six Omaha NE WOWT, available at *http://www.wowt.com/news/headlines/1164496.html* (Nov. 5, 2004).
>
> Broward Vote-Counting Blunder (Florida): Vote tabulation software changes amendment results when the maximum capacity of 32,000 is reached, and the software begins to subtract votes. Source: Channel 4 WJXT Florida, available at *http://www.news4jax.com/politics/3890292/detail.html* (Nov. 4, 2004).
>
> Carteret County (North Carolina): A voting machine loses more than 4,000 votes leaving three races including the Superintendent of Public Instruction and the state Agriculture Commissioner's race in doubt. Source: WRAL.com available at *http://www.wral.com/news/3891488/detail.html* (Nov. 4, 2004).

---

[1] U.S. Election Assistance Commission, Staff Recommendation: EAC Voting System Certification & Laboratory Accreditation Programs Adopted August 23, 2005: EAC Public Meeting, Denver, CO, available at *http://www.eac.gov/VSCP_082305.htm*

[2] Lillie Coney, Testimony, U.S. Election Assistance Commission, Denver, Colorado, August 23, 2005, available at *http://www.epic.org/privacy/voting/eac-8_23.pdf*

[3] National Committee for Voting Integrity, Election News, 2004, available at *http://votingintegrity.org/archive/news/e-voting.html*

San Joaquin County (California): The Secretary of State's test of Diebold's TSx voting system recorded that almost 20 percent of the touchscreen machines crashed during the election simulation. Based on the voting systems performance California refused to certify the use of Diebold's TSx voting system in public elections. Source: *Oakland Tribune* available at *http://www.votersunite.org/article.asp?id=5818* (Aug. 3, 2005).

HAVA Section 231(b)(1) states that "not later than six months after the Commission first adopts voluntary voting system guidelines under part 3 of subtitle A, the Director of NIST shall conduct an evaluation of independent, non-federal laboratories and shall submit to the Commission a list of those laboratories the Director proposes to be accredited to carry out the testing, certification, decertification, and recertification provided for under this section."[4] Further, the law requires the EAC Commissioners to vote to approve the list of accredited laboratories, once submitted by the Director of NIST, for the certification of voting technology used in public elections. The Commission is also directed by HAVA to publish an explanation for the accreditation of any laboratory not included on the list submitted by the Director of NIST.

NIST began work two years ago to produce a list of accredited laboratories for the certification of voting systems. On June 23, 2004, NIST announced in the *Federal Register* that it was establishing an accreditation program for laboratories that perform testing of voting systems, including hardware and software components. On August 17, 2004, NIST's National Voluntary Laboratory Accreditation Program (NVLAP) hosted a public workshop to exchange information among NVLAP laboratories interested in seeking accreditation for the testing of voting systems under HAVA. NIST has also published the *National Voluntary Laboratory Accreditation Program's Voting System Testing Handbook 150–22.* The handbook outlined the technical requirements and guidance for the accreditation of laboratories under the NVLAP Voting System Testing laboratory accreditation program. Finally, on June 17, 2005, NIST published a solicitation for applications and fees from those laboratories interested in being considered in the initial group of applicant laboratories. The notice stated that accreditation would begin on or about September 15, 2005.

In light of the work already done by NIST to provide for a new list of laboratories to be certified by the EAC to conduct certification of voting technology, why is the process being delayed until 2007? The consequences for this delay may be a reduction in the number of new qualified laboratories seeking work in this area, further erosion of public trust in the election system, and more failed voting technology being deployed by states.

Transparency

Transparency is a key component of a functioning, healthy democracy. Transparency or open government is any effort by agencies to impart information to the public on the work of the government. Open government can be accomplished in a number of ways, which may include: public meetings, public rule-making notices, reasonable public comment periods, access to rule-making proceedings, official reports, and open records laws. The application of technology intended to provide a government service should not be excluded from open government objectives. In addition to the methods described, the adoption of technology should include efforts to involve the participation of those members of the public with relevant skills and training.

The guidance to states on the administration of elections should include strong support of open government procedures that allow public access to the election administration process. Historically, the election administration community, voting rights community, media, and partisan efforts looked closely at how elections were managed. Today, that list of constituencies has grown to include technologists, election reform advocates, and concerned citizens.

Transparency is not part of the current laboratory testing and certification process for voting technology. The NASED process did not and would not provide information on the testing process for any voting system.[5] Further, NASED would not answer specific questions regarding a voting technology manufacturer or a specific voting system.[6] In California, Diebold was found to have used uncertified software on

[4] Help America Vote Act Law, Public Law 107–252, available at *http://www.fec.gov/hava/law_ext.txt*

[5] House Science Committee's Subcommittee on Environment, Technology, and Standards, Hearing: *"Testing and Certification for Voting Equipment: How Can the Process be Improved?"* 108th Congress Second Session, June 24, 2004.

[6] *id.*

voting systems operated during public elections.[7] When asked by California election officials about their certification of Diebold's AccuVote-TSx voting system, Wyle Laboratories refused to discuss the status of the testing.[8] It was reported that Wyle Laboratory told the state that the information was proprietary. These conditions should not be tolerated, especially in light of the need to provide proof to the American public that the promise of HAVA will be fulfilled.

Audit

In the final version of voting system guidelines, too little focus is placed on the importance of conducting audits of election results. Post-election evaluation of the results is fundamental to election integrity. For audits to be credible, the same vendor that supplied the voting system being audited should not perform the audit. It is important to know when election systems perform as expected, and when they do not. For this reason, independent, verifiable, and transparent audits of election results should be routine.[9] California, Colorado, Connecticut, Hawaii, Illinois, Minnesota, New Mexico, New York, North Carolina, Washington, and West Virginia all have laws addressing election audits.[10] For example, California's audit law requires a one percent manual recount of voted ballots.

Audits should include a representative hand count of ballots or ballot images; examining documentation of the chain of custody of all voting technology; and the chain of custody on all unmarked, and marked ballots. States are well within their prerogative to determine how the results of audits will be treated, however, they should be strongly encouraged to incorporate audits into every aspect of election administration, and make the results public. States should be encouraged to engage the technology community in the decision-making process to help meet the unique needs of State or local governments to routinely audit their elections.

Today it is not enough that vendors assure states that paperless voting systems record and retain accurate vote information, those systems must be proven to do so. The record of systems failures that resulted in lost votes cannot be ignored. Ballots lost from electronic voting systems used in North Carolina and Florida in 2004 attest to the need for more rigorous voting technology standards.[11] There is also a need to ensure routine access to ballot images for recount and election audit purposes. In 2004 the California Primary election resulted in a legal challenge, *Soubirous vs. County of Riverside,* when a candidate lost an election contest by 45 votes. The candidate was denied access to the memory and audit logs of the Sequoia electronic voting machines purchased the Riverside County Board of Supervisors, which resulted in a court challenge.[12]

---

[7] Thomas Peele, "State allows unapproved machines for March election" *Contra Costa Times,* January 16, 2004. Ian Hoffman, "E-voting software problems worsens," *Alameda Times-Star,* May 15, 2004.

[8] Elise Ackerman, "Vote-machine labs' oversight called lax," *Costra Costa Times,* May 31, 2004.

[9] David Dill, Testimony, Election Assistance Commission, July 28, 2005.

[10] Verified Voting, Manual Audit Requirements, August 20, 2005, available at *http://verifiedvoting.org/article.php?id=5816*

[11] Voters Unite, Report, Myth Breakers: Facts About Electronic Elections, available at *http://www.votersunite.org/MB2.pdf*

"Electronic Voting Machines Lose Ballots Carteret County, North Carolina. November, 2004. Unilect Patriot DRE A memory limitation on the DRE caused 4,438 votes to be permanently lost. Unilect claimed their paperless voting machines would store 10,500 votes, but they only store 3,005. After the first 3,005 voters, the machines accepted—but did not store—the ballots of 4,438 people in the 2004 Presidential election. Jack Gerbel, President and owner of Dublin-Calif.-based UniLect, told The Associated Press that there is no way to retrieve the missing data. Since the agriculture commissioner's race was decided by a 2,287-vote margin, there was no way to determine the winner. The State Board of Elections ordered a new election, but that decision is being challenged in the court.

Palm Beach County, Florida. November 2004. Sequoia DRE Battery failure causes DREs to lose about 37 votes. Nine voting machines ran out of battery power and nearly 40 votes may have been lost.. . .The nine machines at a Boynton Beach precinct weren't plugged in properly, and their batteries wore down around 9:30 a.m., said Marty Rogol, spokesman for Palm Beach County Supervisor of Elections Theresa LePore. Poll clerk Joyce Gold said 37 votes appeared to be missing after she compared the computer records to the sign-in sheet. Elections officials won't know exactly how many votes were lost until after polls close."

[12] Soubirous vs. County of Riverside, No. E036733, 2006 Cal. App. Unpsb. Lexis 1218 (Cal. App. Feb 8, 2006) available at *http://www.verifiedvoting.org/downloads/legal/california/soubirous-v-countyofriverside/*

Security

Security can be defined as a series of tradeoffs.[13] For example, automobile manufacturers initially opposed interior airbags in cars because they were thought to be too costly. The government made the decision that their inclusion in cars would save lives and that the increased cost for the purchase of an automobile was worth the tradeoff.

The voter is the only person who should know how they voted. That person should not be able to prove to anyone how they voted, nor should a ballot be associated with that voter.[14] The votes cast by voters should be recorded and retained free from error or manipulation. The ballots and votes cast should be secured from tampering, damage, machine failure, or loss.

Voters should be able to cast votes and verify vote choices unassisted. Accuracy should be maintained and authenticated through a post-election audit process. State and local election contingency planning should detail what should be done in the event of a natural disaster or if a polling location unexpectedly becomes unavailable. Once an election has begun, contingency plans should cover what should take place to complete the election. For example, what should be done if a power outage occurs that exceed battery life of voting or ballot tabulation technology, voter turnout exceeds expectations, or unexpected shortages of Election Day poll workers occur, which threaten the conclusion of an election once begun.[15]

Reliability

Another technical threat to voting systems, which receives too little attention, is Electrostatic Disruption (ESD). This can be devastating to the operation of electrical equipment. Humidity and other conditions in which voting systems will operate can contribute to ESD. It is our view that more study should be done to better understand the threats that ESD poses to voting systems and develop means to mediate them. States should be directed to use a sliding scale for conditions, where machines will be used and ESD is a high probability.

Comments on Voluntary Voting System Guidelines

The Election Assistance Commission has demonstrated problems with version control of the final recommendations on voting system standards.[16] The problem has continued with the publication in the *Federal Register* the final guidance submitted to the EAC by the Technical Guideline Development Committee (TGDC) on their recommendations for voluntary voting system guidelines.[17] The TGDC recommendations sent to the EAC are available online.[18] The TGDC's online document representing their final recommendations to the EAC and the EAC's reprint of those recommendations in the *Federal Register* in April 2006 do not agree. Specifically the TGDC's final recommendations dated May 9, 2005 includes Sections 6.0.4.2.1.1.6 through 6.0.4.3.2.2, and the EAC document identified as the TGDC's recommendations document does not include these sections. The missing sections addressed the role of the NIST National Software Reference Library.

If this had been the only incident of version control problem it might not be noteworthy other than a correction be published in the *Federal Register,* but another earlier incident makes this appear to be a pattern of inefficient management of documents. For example in another incident the EAC voted on the final of the VVSG on December 13, 2005, the document was made public on January 12, 2006.[19] However, at some point between the public posting and mid-February the EAC final VVSG document was replaced by another version.[20]

Barring a thorough investigation of this issue—a solution may not be easy to achieve, however it is worth noting that the chief expertise of the National Institute

---

[13] Bruce Schneier, "Beyond Fear: Thinking Sensibly About Security in an Uncertain World" pg. 7.

[14] Coney, Hall, Vora, and Wagner, "Towards a Privacy Measurement Criterion for Voting Systems."

[15] Ace Project, Voting Operation: Contingency Plans, available at *http://www.aceproject.org/main/english/po/pohO1d.htm*

[16] National Committee for Voting Integrity, Letter (April 28, 2006).

[17] Election Assistance Commission, Technical Guidelines Development Committee's Final Recommendations on Voluntary Voting System Guidelines, *Federal Register* (April 12, 2006) available at *http://a257.g.akamaitech.net/7/257/2422/01jan20061800/edocket.access.gpo.gov/2006/pdf/06-3101pdf*

[18] TGDC final VVSG Document Delivered to the EAC May 6, 2006 available at *http://vote.nist.gov/VVSGVol1&2—pdf*

[19] EAC, Final VVSG Document January 13, 2006 available at *http://votingintegrity.org/pdf/vvsg_%20vol_I-1.pdf*

[20] EAC, Current Final VVSG Document, July 14, 2006 available at *http://www.eac.gov/VVSG%20Volume_I.pdf*

of Standards and Technology (NIST) is the development of standards, and a key component of this work is version control. Therefore, we strongly recommend that the following action be taken, the correct TGDC VVSG document be printed in the *Federal Register* in its entirety, and that NIST be directed to manage version control for the EAC of all document development required under the *Help America Vote Act* (HAVA).

VVSG creates new threats to voting system security by recommending the use of telecommunication systems to transmit the election information over public telecommunication networks. Public telecommunication networks, especially the Internet, are insecure.[21] It is important to note that HAVA Section 245 directs that the EAC conduct a study and report on Electronic Voting and Electoral Process in federal elections.[22] The study, when completed, would assess the safe use of the Internet and other communication technology's use in voting.

It is our strong recommendation that future guidance issued by the agency to states direct them to prepare realistic contingency plans in the event of electronic voting system failures that jeopardize the completion of the election process.[23] Future Voluntary Voting System Guidelines should encourage State and local election administrators not to limit their thinking to what can be done, but to consider what can be done safely to establish reliable, secure, accessible, transparent, accurate, and auditable public elections.

In VVSG Volume 1, Section 7 Security, recommends the incorporation of wireless technology in voting systems. We strongly recommend that wireless technology not be allowed in voting systems. Although wireless technology is commonplace in remote control systems for televisions, DVDs, VHS, computer networks, and other consumer products that does not mean it should be trusted in voting systems. States considering wireless technology as an option should be strongly encouraged to enumerate the need for it, and evaluate the potential risks. Manufacturers of voting systems should not incorporate wireless technology as a standard offering in voting systems used in public elections because it poses serious security risks. The only way to be sure that the risk is not present is not to include the wireless capability. If states insist on having wireless capability on voting systems, the next best security option is the ability to physically remove the device from voting systems before their use in public elections.

In closing, future recommendations to election administration should include a directive to test all ballot marking devices to be sure that they meet specifications of the precinct tabulating facility and central tabulating technology. The precinct tabulator and central tabulator technology should be calibrated to read reasonable marks, which should include a dark stroke crossing the voting target on its long dimension and half the width of the target should register as a vote. Finally, all ballot tabulators should be tested and/or calibrated to ignore erasures made by a new gum eraser of a thoroughly blackened pencil mark.

Guidance to states regarding the use of paperless direct recording electronic voting systems should include strong recommendations that at least one poll worker at each polling location should be trained to check the calibration of DRE voting machines and if necessary recalibrate them. Guidance to manufacturers should include criterion that these systems memory capacity is exceeded or a malfunction that threatens vote capture and retention is detected the voting system shall disallow the reinsertion of voter cards to disallow the appearance of continuing to record votes.

The United States is a society of equal rights. On Election Day, this nation must function as a society of equal rights, where a single vote is treated as important as the majority of votes cast.

Thank you,

MEMBERS

Peter G. Neumann, Chair * David Burnham * David Chaum * Cindy Cohn * Lillie Coney David L. Dill * Joe Hall * David Jefferson * Jackie Kane * Douglas W. Jones * Stanley A. Klein * Vincent J. Lipsio * Justin Moore * Jamin Raskin * Marc Rotenberg * Avi Rubin * Bruce Schneier * Paul M. Schwartz * Sam Smith

NCVI Intern, Richard Rasmussen

---

[21] David Jefferson, Aviel D. Rubin, Barbara Simons, David Wagner, Report, "A Security Analysis of the Secure Electronic Registration and Voting Experiment (SERVE)," January 2004.

[22] *Help America Vote Act of 2002* (HAVA), Public Law 107–252, October 29, 2002. SEC. 245. 42 USC 15385, available at *http://www.fec.gov/hava/law_ext.txt*

[23] Ace Project, Report on Physical Security, available at *http://www.aceproject.org/main/english/et/ete01a.htm*

STATEMENT OF VERIFIEDVOTING.ORG

There is a crisis of confidence today in electronic voting systems that are widely used across our nation. It grows each day as the public gains awareness of the inadequacies and vulnerabilities of those systems. The concern is perhaps greatest among those who have the most technical understanding of the computing systems that form the basis for the voting equipment.

The concerns that led to this crisis are not new, but no set of standards alone has been or will be sufficient to erase them.

There will be those who say the crisis is not the fault of inadequate systems but rather the fault of those who shed light on the inadequacies—a "shoot the messenger" approach to restoring the public's sense that they can be sure their votes will count. They are wrong. They might be able to bury their own heads in the sand, but asking the public to take it on faith that there's no such thing as a machine malfunction or someone who might want to tamper with an election is simply not good enough, and a simple review of historical fact belies that belief.

There will be those who say that *system* problems can be solved with a set of *procedures*. This too is a false fix, akin to directing the public to watch while we attach a big lock on the front door of the bank, while leaving the back door unlocked and the safe wide open. Good procedures are necessary, as are technical features that support system security, reliability and usability. However, sometimes one needs mechanisms to prevent specific acts that doesn't depend on humans to follow rules. A procedural fix cannot alone solve a system problem.

Guidelines, regardless of how well written, do not matter at all if they are not enforced. At present, mechanisms are not in place to halt the electoral process or address the problem if the Guidelines are violated or circumvented, nor even to scrutinize the process to ensure Guidelines are not violated nor circumvented. The Guidelines instead become mere fig leaves strategically draped over the never-ending problem of voting systems that cannot be made secure without the essential safeguard of a voter-verified paper record (VVPR) of every vote, and mandatory random checks of the paper records to ensure accuracy of the vote count.

Seventy percent of the states believe—regardless of the existence of any Guidelines—that voter-verified paper records are necessary.[1] Over half of the members of the U.S. House of Representatives have reflected that majority position by sponsoring legislation that would make VVPR mandatory in all states. While only 13 states currently require random manual audits of the voter-verified paper records,[2] many more have the tools to conduct those audits today.

Unless and until these practices (the use of voter-verified paper records and mandatory manual audits of those records) are adopted nationwide, the crisis of confidence will continue to grow. The current set of Guidelines, despite the efforts of those who worked on them, do not resolve this current crisis, for several reasons.

—First, they are inadequate: the current process for voting system certification is wholly insufficient for security, and resolutions of the Technical Guidelines Development Committee to include open-ended research on possible attacks were omitted from the guidelines.

—Second, they will never be adequate for security, if separate and apart from a voter-verifiable voting system and robust random manual audits. This is not to say the VVSG on security shouldn't exist, but rather that it must be understood they can only serve as a potential enhancement to mitigate risks, and cannot ever be strong enough alone.

—Third, the most significant thing the current VVSG could have done to help bolster the public's confidence was not done: On January 18, 2005, Professor Ron Rivest introduced a resolution (#13–05) to require voter-verified paper records at the TGDC meeting. Professor Rivest is the member of the TGDC with by far the greatest expertise in computer security. That resolution was voted down, by members of the committee who know less about computer security than the person who introduced the measure. Just as the Food and Drug Administration would not approve of a pharmaceutical based on a vote where accountants out-voted physicians, **it is important that decisions affecting technical requirements are made by people that are technical experts.**

---

[1] 28 states have enacted rules or legislation requiring voter-verified paper records: AZ, AK, AR (partial req.), CA, CT, CO, HI, ID, IL, ME, MI, MN, MO, MT, NC, NV, NH, NY, NJ, NM, OH, OR, SD, UT, VT, WI, WV, WA. Another eight states are deploying voter-verifiable equipment statewide even without a requirement: AL, MA, MS, NE, ND, OK, RI, WY. For details see *http://verifiedvoting,org*

[2] AK, AZ, CA, CT, CO, HI, IL, MN, NM, NY, NC, WA, WV—for details, see *http://www.verifiedvoting.org/article.php?id=5816*

—Finally, as the lion's share of HAVA equipment funding has been spent on systems that were not designed to those standards, the current VVSG can serve only as a theoretical or philosophical guideline for what you would want in a voting system, if one were going to buy a new one today. . .but almost no one is buying now. As safeguards for the systems we use today and for the foreseeable future, or as insurance that those systems are accessible and usable as possible—the VVSG are the horse lagging behind its voting-system cart.

Concerns and Recommendations

Analysis of the VVSG process to date makes clear the Guidelines are inadequate to address the current (justified) crisis of confidence in electronic voting systems. Recommendations for improvement follow.

1. Prevent Unrecoverable Lost Votes; Mandate VVPR. During the November 2004 election in Carteret County, North Carolina, a paperless DRE voting machine completely failed to record over 4,400 ballots cast on that machine; this failure occurred because those ballots exceeded the configured size of that machine's electronic memories. The machine failed to warn the affected voters that their ballots were not being recorded, the votes from those ballots were irretrievably lost, and several statewide races were thrown into limbo because the margin of victory in those races was less than the number of lost votes. While this was apparently the largest number of votes irretrievably lost on a single DRE, it was not the first or only documented instance of such a loss. Two years earlier, 436 ballots failed to be recorded on a different vendor's DRE used for early voting in Wake County, North Carolina. And just last year, in Pennsylvania, cast ballots were inadvertently erased at the end of the voting day due to a set-up error.

In each case, had those DRE voting machines been equipped with a voter-verifiable paper audit trail (VVPAT) (or had those jurisdictions been using an inherently voter-verified paper ballot system, such as optical scan ballots), those votes would not have been lost. Yet despite these problems, the revised VVSG do not adequately protect against these types of problems and lack any requirement for VVPAT, despite thousands of comments submitted by the public in support of adding such a requirement.

> To prevent future losses of votes due to malfunction, programming error, set-up error, or tampering, the VVSG must require voter-verified paper records. This step will also serve as an interim measure to regain some of the lost confidence in our voting system, although only in those jurisdictions that adopt the voluntary guidelines. For real impact, legislation requiring voter-verified paper records and mandatory random manual audits must be passed so that votes in all jurisdictions are protected.

2. Accelerate VVSG Update Process. The VVSG do not take effect until December 2007, and even then, not all states are obligated to follow them because the guidelines are voluntary. Hence, in terms of addressing the current crisis, they offer too little, too late. The lag between their development and their effective date almost ensures that they will be obsolete by the time they are in effect. The capabilities and state-of-the-art in computerized systems changes vastly over the 24-month adoption period, and the pace of voting standards development , while slightly accelerated over what it has been, still seems glacial when seen in the light of security concerns.

> Given the rate of change of technology, security-related and other standards in the VVSG should be reviewed annually, and the adoption window should be shorter than it is (e.g., 12 months rather than 24). When gravely serious security or performance problems with voting systems are uncovered as has happened in recent months, standards should be upgraded in response, and if need be, voting machines in the field re-tested for modification.[3] No new elections should have to be run on equipment demonstrated to be faulty or insecure.

3. Certification Process Should Not Be Cloaked in Secrecy. Despite some minor changes to the scheme for certifying voting systems (i.e., "qualification" has been renamed "certification," ITAs have been renamed "voting system testing laboratories," and the EAC, through NIST, will assume oversight and accreditation of the testing laboratories), the overall scheme still remains one in which private vot-

[3] These recommendations echo those of Dr. Michael Shamos, Distinguished Professor of Computer Science at Carnegie Mellon University, who testified in 2004 to the Environment, Technology, and Standards Subcommittee of the House Science Committee on the subject of voting system testing and certification. Cf. *http://www.house.gov/science/hearings/ets04/jun24/shamos.pdf*

ing system vendors contract with (and pay for) private testing laboratories to carry out certification testing in secret. Public confidence in the integrity of this certification scheme will not be achieved if this testing process continues to remain cloaked behind a veil of secrecy.

> "To keep vendors and [the VSTLs] accountable for their work, the EAC should require that, as a condition of certification, the report produced by the ITA be publicly released, along with the technical data package."[4]

4. Stronger Security Testing Needed. The VVSG scheduled to take effect in 2007 do not mandate the type of vigorous security examination needed to uncover security weaknesses (e.g., the several Hursti hacks,[5] plus additional vulnerabilities discovered by California's Voting Systems Technology Assessment Advisory Board [VSTAAB]) of the sort discovered due to the inquisitiveness and concern of local election officials (e.g., Ion Sancho, Supervisor of Elections, Leon County, Florida; Bruce Funk, Emery County Clerk, Utah). These vulnerabilities could be successfully exploited without leaving any trace. Any certification system that subjects voting systems to hundreds of hours of "testing" and which takes many months and hundreds of thousands of dollars to complete and yet fails to discover grave security vulnerabilities which can be successfully exploited in a manner of minutes is completely ineffective.

> "Security evaluations should be conducted by experts not chosen by the vendors, and those experts should be allowed to do open-ended research on possible attacks (such groups are sometimes called "Tiger teams"). Any new iteration of the VVSG should incorporate the TGDC Resolution #17–05 which called for such an approach."[6]

5. Proprietary Interests Should Not Outweigh Security and Performance Requirements. The current (and future) certification scheme based on the current (and future) VVSG appears to be biased in favor of maintaining the proprietary interests of voting machine vendors rather than ensuring the integrity of the voting systems being evaluated.

An example is the inclusion of wireless networking, which opens up security threats while facilitating vendor interests. The inevitable consequence of allowing wireless, even with special guidelines about its use, is that machines with wireless capability will be certified, even though they will not and cannot be secure. Worse, even if a jurisdiction wanted to ban wireless capabilities locally, it is possible under the current certification scheme that they would be unable to determine whether such capability was already "on-board" in their existing systems. First, they'd need the technical ability to check their hardware (and if a wireless component was found, to examine the software to ensure that the software will not support it). Second, warranty and maintenance agreements often consider things like "unauthorized" opening of the case of a voting system to violate or void the warranty. So, more than likely, a jurisdiction would have to ask the vendor if there was wireless capability and take their word for it or ask permission to examine the system to assess whether or not wireless functionality was shipped and armed.

> Wireless networking is unnecessary and inherently unsafe, and should be banned outright. Further, The VVSG should define procedures under which local election jurisdictions can reliably verify the absence of such wireless capability in any voting systems equipment that they purchase or lease.

6. Encourage (Secure) Usability Advances. The current practice of certifying whole voting systems has the potential to stifle the independent development of add-ons to existing voting systems that can greatly enhance usability and especially accessibility. For example, this practice has impeded deployment of accessible ballot-marking devices which are designed for, and capable of, working with any legacy optical scan voting system, because those devices must be re-submitted for testing with each such voting system, a process in which vendors have yet to cooperate. Accessibility advocates describe a wish for systems with a broad spectrum of capabili-

---

[4] Testimony of Dr. David Dill, Professor of Computer Science, Stanford University and Founder of Verified Voting, before the Election Assistance Commission, July 28, 2005 hearing, Pasadena, CA *http://www.eac.gov/docs/Dill.pdf*

[5] Finnish computer security expert Harri Hursti discovered two distinct classes of vulnerabilities in the Diebold AccuVote voting systems: a) Vulnerabilities associated with the use of interpreted AccuBasic code on the removable memory card used to store vote totals and/or ballot images (for details see *http://www.ss.ca.gov/elections/voting_systems/security_analysis_of_the_diebold_accubasic_interpreter.pdf*); and b) vulnerabilities associated with boot loader software and flash memory (*http://www.blackboxvoting.org/BBVreport.pdf*).

[6] Testimony of Dr. Dill July 28, 2005, ibid.

ties and features, yet typically no one system currently addresses all those needs. Jurisdictions lack the resources to obtain more than one system for accessibility, but even if they had the resources, inter-operability between competing systems is lacking.

There is a need to provide for inter-operability between such existing and potential modular devices made by different vendors. Yet it is important not to sacrifice the performance and security benefits that end-to-end system testing brings.

> The VVSG should look to develop a better solution for inter-operability such as testing a proposed subsystem, and having well-defined, standard interfaces between sub-systems that comprise a voting system. For example, a standardized schema for defining the layout of optical scan paper ballots should be developed to enable the interchange of ballot layouts between voting systems developed by different vendors, so that an optical scan ballot printed by vendor X could be marked by a ballot marking device manufactured by vendor Y and scanned by an optical scanner built by vendor Z. Each vendor would be responsible for providing conversion software to translate between their proprietary ballot layout definition files and the standardized schema.

7. Scrutiny and the Need to Address Defects Discovered After Deployment. At present, the revised VVSG and proposed certification process lack any clear mechanism for suspending or revoking the federal certification status of deployed voting systems found to contain serious defects, including security vulnerabilities, that put the public's votes and the integrity of our elections at risk. When such critical security defects are discovered in already-deployed voting systems, some fraction of impacted states issue some sort of warning or advisory, while other states take no action at all. Even when warnings or advisories are issued, most states typically take no further action to ensure that local jurisdictions comply or act on those notices, in part because the costs for implementing interim mitigation procedures fall on local election jurisdictions that lack the resources to effectively carry them out.

When defects in other types of products affect public safety, product recalls are initiated and product defects corrected at vendor expense. But when similarly serious defects or vulnerabilities are found in voting systems, we do not see federal certification revoked or products recalled. (Nor have we seen any requirement that vendors notify all their existing markets about the problem, with recommendations for mitigation or replacement. This means the same problem can occur election after election, in county after county, despite having been likely preventable in all but the first instance.)

> To help prevent voting machine problems, new Guidelines must provide a mechanism for scrutiny to ensure that its standards are maintained and enforced, especially when problems with the design of a voting machine are discovered after it has completed federal qualification and been deployed for use in elections.
>
> The revised VVSG should include mechanisms for suspending or revoking federal qualifications when serious defects in voting machines are discovered after initial qualification, and should require notification and mitigation by the vendor involved to all jurisdictions where the voting system is deployed.

Need for Prompt Action

Slightly over two years ago, on June 24, 2004, the Environment, Technology, and Standards Subcommittee of the House Science Committee held hearings on the subject: *"Testing and Certification of Voting Equipment: How can the process be improved."*[7] In his testimony[8] before that committee, Dr. Michael Shamos stated in part:

> *I am here today to offer my opinion that the system we have for testing and certifying voting equipment in this country is not only broken, but is virtually nonexistent. It must be re-created from scratch or we will never restore public confidence in elections.. . .*
>
> *. . .We need a coherent, up-to-date, rolling set of voting system standards combined with a transparent, easily-understood process for testing to them that is viewable by the public. We don't have that or anything resembling that right now, and the proposal I have heard are (sic) not calculated to install them.*

---

[7] *http://www.house.gov/science/hearings/ets04/index.htm*
[8] *http://www.house.gov/science/hearings/ets04/jun24/shamos.pdf*

. . .I propose that standards for the process of voting be developed on a completely open and public participatory basis to be supervised by the EAC, with input from NIST in the areas of its demonstrated expertise, such as cryptography and computer access control. Members of the public should be free to contribute ideas and criticism at any time and be assured that the standards body will evaluate and respond to them. When a problem arises that appears to require attention, the standards should be upgraded at the earliest opportunity consistent with sound practice. If this means that voting machines in the field need to be modified or re-tested, so be it. But the glacial pace of prior development of voting standards is no longer acceptable to the public.

Unfortunately, two years after the Subcommittee heard these concerns in testimony, little has changed. Instead of recreating the testing and certification system "from scratch" and making that process "transparent, easily-understood" and "viewable" by the public, the revised VVSG does little to address any of these concerns. Rather, the revised VVSG makes some tweaks to the "arcane technical standards" (Guidelines) and the accreditation of the testing labs, but otherwise leaves intact the existing opaque and secretive system which Professor Shamos describes as "grotesque." That system can continue no longer, and must be made transparent.

Beyond accepting public input to the revised VVSG, the "standards body" must show greater evidence that it has heard the overwhelming majority of that public input and must provide a meaningful response to key concerns raised by the public (e.g., concerns regarding the urgent need for VVPR and for the elimination of wireless technology from voting systems).

When gravely serious security problems with DREs are uncovered as they were during this past year, standards must be upgraded in response, voting machines in the field modified and retested, and the pace of voting standards development must accelerate to address usability, performance and especially security concerns.

It is time for Congress to act to safeguard our elections. Tweaking the voluntary Guidelines (not even yet in effect) will not address the public's urgent concerns about the integrity of our voting system. Immediate passage of a requirement for voter-verified paper records and mandatory random manual audits will.

UMBC

AN HONORS UNIVERSITY IN MARYLAND

Maryland Registered Voters' Opinions About Voting and Voting Technologies

Prepared for the Maryland State Board of Elections

February 2006

National Center for the Study of Elections
of the
Maryland Institute for Policy Analysis & Research
University of Maryland, Baltimore County

Maryland Registered Voters' Opinions about Voting and Voting Technologies

Donald F. Norris
National Center for the Study of Elections
Maryland Institute for Policy Analysis and Research
University of Maryland, Baltimore County
February 2006

Executive Summary

This survey of registered voters in Maryland found that voters have a high level of confidence in Maryland's touch screen voting system. Most voters surveyed agreed that the current voting system was easy to use (89 percent), made voting quicker (85 percent), and recorded and counted the votes accurately (82 percent). Voters also felt that, even given the controversy around them, touch screen systems are reliable (73 percent), can be trusted (64 percent), accurately record and count votes (73 percent) and that security measures prevent tampering or hacking (53 percent). Seven in ten (70 percent) respondents agreed that that Maryland has done all it could to prevent fraud or tampering.

While the majority of respondents voiced confidence in the current voting system, they expressed concerns about external threats to the system. Forty-seven percent agreed that touch screen systems could be tampered with and hacked into, while over half of respondents (55 percent) said they believed that that the systems could be corrupted by malicious software programming.

The telephone survey, requested by the State Board of Elections, asked 800 registered voters who voted in the 2004 general election in Maryland their opinions about a series of issues around voting and voting technologies in the state. The survey had a margin of error of plus or minus 3.5 percent at a 95 percent level of confidence.

The survey found that Maryland's registered voters are computer-literate, with 81 percent reporting that they use computers daily or several times a week. Of those, 85 percent use the Internet daily or several times a week. While a large majority of respondents (70 percent) said they have a high level of trust in computers, only 44 percent of Maryland voters have a high level of trust in government.

The use of alternatives to touch screen voting systems, as well as the introduction of vote verification systems, has been the subject of debate in Maryland and other states. Nevertheless, fewer than half (45 percent) of respondents said they had heard or read anything about touch screen systems within the past year, with 49 percent of those reporting they heard positive things and 48 percent reporting they heard negative things. Further, only one in five (23 percent) of registered voters said they had heard or read anything about people calling for different voting technologies to be added to or substituted for Maryland's touch screen voting system.

Voters were also unfamiliar with the concept of a paper trail (i.e., a system that produces a paper record or receipt that the voter can use to confirm his vote), one of the vote verification systems under discussion in Maryland. Of the 23 percent of voters who had heard or read about different voting technologies to be added to or substituted for Maryland's touch screen voting system, only 35 percent (about 8 percent of all voters sampled) responded that the primary thing that they had heard or read about involved a paper trail.

When the entire sample was asked what paper trail meant, nearly one in four (38 percent) said that they did not know. Only about 6 percent correctly indicated that paper trail means that a voter views a paper record of his vote behind a glass screen to verify the vote. Notwithstanding

the confusion about the meaning of a paper trail, 69 percent said that voters should be able to confirm their votes through paper records or receipts.

The results of this survey indicate that there is no crisis of confidence among voters about Maryland's touch screen voting system as it is currently implemented. At the same time, voters are concerned about security of the system, but unfamiliar with one of the vote verification methods under discussion (paper trail). Given voter concerns, SBE should work with local boards of elections and interested groups to inform and educate the public about what is being done to secure the touch screen voting system used in Maryland from hacking, malicious programming and acts that might compromise elections.

Table of Contents

Experience with Voting Technologies 2

Opinions about Touch Screen Voting Systems in General 3

Impact of Debate over Touch Screen Voting 4

Perceived Vulnerability of Maryland's Touch Screen Voting System 5

Controversy over Touch Screen Voting Systems 6

Equipment Attached to Maryland's Touch Screen Voting Systems 7

Computer and Internet Use; Trust in Computers and Government 7

Paper Trail and Security Concerns in Context 8

Conclusion 10

Data Tables 11

References 20

About the Author 21

About UMBC 21

About MIPAR 21

About NCSE 21

Appendix – Survey Instrument 22

Registered Voters' Opinions about Voting and Voting Technologies In Maryland

The Maryland State Board of Elections (SBE) engaged the National Center for the Study of Elections (NCSE) of the University of Maryland, Baltimore County (UMBC) to conduct a survey of the opinions of Maryland registered voters about a number of issues around voting and voting technologies in the state. Dr. Donald Norris, director of the NCSE and of the Maryland Institute for Policy Analysis and Research (MIPAR) and professor of public policy at UMBC directed this survey. In cooperation with the SBE staff,[1] he developed and pre-tested a survey instrument of approximately 10 minutes duration. NCSE contracted with the public opinion survey firm, Mason-Dixon Polling & Research, Inc., of Washington, D.C. to conduct the interviews. Mason-Dixon conducted the survey between January 9 and January 12, 2006. A total of 800 registered voters were interviewed statewide by telephone. All indicated that they were registered voters and had voted in the 2004 general election in Maryland.[2] Those interviewed were selected randomly from a commercially available voter registration list. Quotas were assigned to reflect voter turn-out by county.

The margin for error, according to standards customarily used by statisticians, for this survey is no more than plus or minus 3.5 percent at a 95 percent level of confidence. If a similar survey were conducted 100 times, 95 out of that 100 times, the results would be within plus or minus 3.5 percent of those produced by this survey. This means that we can have a high degree of confidence that the results are valid, reliable and can be generalized to the broader population of registered voters in the state.

To ascertain the representativeness of the sample, I compared sample demographics against data from the 2000 Maryland census and, for partisan registration, against the fall 2004 SBE registration data. As Table 1 shows, for gender and party registration, the sample is nearly identical with the source data and is very close in terms of county of origin, suggesting a high degree of representativeness.

However, when other demographic characteristics from the sample are compared with the 2000 census data, the results indicate that the sample over-represents whites, older voters, more affluent voters and more well educated voters.

The apparent over- and under-representation according to these characteristics is, however, more likely a function of the method of comparison than of the sample itself. The SBE does not (and probably should not) collect data on race, gender, education and income of

[1] The SBE staff provided input regarding issues that they thought would be salient for the survey, and they reviewed and provided comments on drafts of the survey instrument. They did not have any control over the questions (including question content or wording) contained in the instrument or the analysis of the survey data.

[2] The first question asked was whether the respondent was a registered voter and the second was whether he or she had voted in the 2004 Maryland general election. If both conditions were not met, the respondent was screened out of the survey. The interviewers also screened out voters who voted using absentee ballots or provisional ballots. The respondents, then, included only voters who had voted in election precincts in the 2004 general election and, thus, had used the state's touch screen voting systems.

registered voters. Consequently, I conducted comparisons between this sample of registered votes and data from the 2000 census for the state's population as a whole. It is well-known know from many years of voting studies that registered voters who vote in elections are more likely to be more well educated, more affluent, and older and less likely to be minorities, other things being equal, than the general population. Thus, it is highly likely that the sample of respondents in this random survey of Maryland registered voters who voted in the 2004 general election in Maryland is quite representative of the broader population of registered voters in the state.

The survey contained questions on a number of issues. I report the results according to the order in which questions occurred in the survey. Data tables found at the end of the text reproduce the survey results. The survey instrument is found in the Appendix at the end of this report.

Experience with Voting Technologies

The first set of questions sought to ascertain the experience of Maryland registered voters on various voting technologies. I asked whether they had *ever used* lever machines, optical scan voting systems, punch card voting systems and touch screen voting systems. (I provided brief descriptions of each system.) The results are shown in Table 2.

The largest number (87.0 percent) of voters said that they had used touch screen systems, followed by lever operated machines (79.6 percent), optical scan voting systems (48.6 percent) and, finally, punch card voting systems (38.1 percent). Since these were registered voters who voted in the 2004 general election in Maryland, 100 percent of the respondents should have said that they had voted on touch screen voting systems because these were the only precinct level voting machines used in Maryland in that election.

Next, I inquired if they recalled which type of system they used to vote in the 2004 general election (Table 3). Here only 80.3 percent recalled correctly that they used touch screen voting systems. The remainder responded as follows: optical scan – 7.3 percent; punch card – 3.9 percent; lever machine – 3.1 percent; and don't know/don't recall – 5.5 percent.

What is interesting about these figures is the imperfect recall of the voters questioned. When asked if they had ever used touch screen systems, 13 percent could not recall having done so. When asked what system they used in the 2004 general election, nearly one in five (19.7 percent) did not recall correctly that they used touch screens.

Notwithstanding recall (and recall of actual events among large groups of persons is hardly ever perfect), I followed up by asking these voters to rate their experience with the voting system that they used in the 2004 general election (Table 4). Nearly two-thirds (62.9 percent) said that the experience with the voting system that they used then was very positive and nearly one in three (29.0 percent) said it was positive. Fully 91.9 percent reported a positive experience versus only 6.8 percent reporting negative experiences (of which only 0.8 percent reported a very

negative experience. In all, Maryland registered voters who voted in the 2004 general election gave the state's touch screen voting system very high marks for a positive voting experience.

The next few questions, framed in the form of statements to which respondents were asked to agree or disagree, were designed to get at particular aspects of the voting experience and also ask voters opinions about aspects of the system on which they voted in the 2004 general election in Maryland (Table 5).[3]

The first statement was that the system "was easy to use." Here more than three-quarters (78.6 percent) agreed strongly and another 20 percent agreed for a total of 98.6 percent who agreed in some form with the statement that the system that they used to vote in 2004 was easy to use. The second statement was that the machine that the voter used had equipment problems. More than nine in ten voters disagreed with this statement (94.8 percent). More than eight in ten (84.9 percent) agreed strongly with the statement that the system on which they voted made voting faster while only 12.3 percent disagreed. Most voters disagreed somewhat or disagreed that they felt uncomfortable using the system (87.9 percent) while only 11.8 percent agreed.

The final statement concerned an issue of great contemporary concern in Maryland. It read: "I was confident that it [the system I used to vote in the 2004 election] recorded and counted my vote accurately." Here, 60.1 percent agreed strongly, 21.4 agreed somewhat (a total of 81.5 percent agreed) while only 9.9 percent disagreed of which only 4.5 percent disagreed strongly (8.6 percent did not know).

Opinions about Touch Screen Voting Systems in General

The following questions attempted to gauge voters' knowledge about and opinions of touch screen voting systems in general (Table 6). We asked, first, if they had heard or read anything about these systems within the past year. Less than half responded affirmatively (45.4 percent). We then asked those who responded affirmatively whether they had read or heard anything about touch screen systems in general (52.1 percent), in Maryland (11.8 percent) or both (32.5 percent).

Next we asked (again only of those who had responded affirmatively above) whether what they had read or heard about touch screen voting systems was positive or negative (Table 7). The responses were nearly evenly divided – 48.8 percent positive versus 47.7 percent negative. This was surprising because much of what has been said and written about these systems in the recent past is from a critical or negative perspective, especially in Maryland. Nevertheless, a plurality of those who have heard or read anything about touch screen voting systems within the past year have heard or read positive things on balance.

[3] In this and all instances where interviewers read statements and asked respondents to agree or disagree with the statements, the questionnaire deliberately alternated statements phrased in the positive with statements phrased in the negative so as to avoid the possibility of "leading" the respondents by providing only positive or negative cues to them.

I followed these questions with a series of statements about touch screen voting systems that I asked of all respondents (Table 8). The statements were that touch screen voting systems:

- Are easy to use -- 91.9 percent agreed; 3.2 percent who disagreed.
- Cannot be counted on to count the vote accurately – 60.5 percent disagreed; 19.0 percent agreed and 20.5 percent did not know.[4]
- Are secure from fraud and tampering – 39.9 percent agree; 29.1 percent disagree; 31.1 percent don't know.
- Cannot protect the privacy of the vote – 55.6 percent disagree; 24.7 percent agree; 19.9 percent don't know.
- Provide for an accurate recount of the vote – 55.9 percent agree; 21.9 percent disagree; 22.3 percent don't know.
- Can be corrupted by malicious software programming – 55.1 percent agree; 18.9 percent disagree; 26.0 percent don't know.
- Make voting faster – 85.5 percent agree; 10.0 percent disagree.
- Are not accessible to persons with disabilities – 54.6 percent disagree; 20.2 percent agree 25.4 percent don't know.

Next, I asked for the respondents' overall opinions about touch screen voting systems (Table 9). A clear plurality had a strongly favorable opinion and one in three had a somewhat favorable opinion (for a total of "favorable" responses of 76.3 percent or more than three-quarters of respondents). Only, one in six (16.0 percent) had unfavorable opinions, of whom only 5.1 percent were very unfavorable.

Taken together, the responses in Tables 8 and 9 suggest that Maryland registered voters have very positive attitudes about touch screen voting systems, notwithstanding their understandable concerns about whether these systems are secure from fraud and tampering and can be corrupted by malicious programming. (I will return to these issues later in this report.)

Impact of Debate over Touch Screen Voting

For perhaps the past two years, an important public policy debate has been waged about the Maryland's voting system. In this survey, I endeavored to gauge the extent to which registered voters were "tuned in" to that debate. Hence, I asked whether they "*had heard or read anything*

[4] Readers will note that for all but two of these statements, between 20 and 30 percent of voters signified that they did not know or could not give an opinion. (Interviewers did not read the "do not know" or "no opinion" choices to the respondents but did record such responses if respondents so indicated.)

about people calling for different voting technologies or equipment to be added to or used in place of Maryland's touch screen voting system." The results, shown in Table 10 show that fewer than one in five (22.9 percent) of Maryland registered voters are aware of this debate.

I then asked this group (that is, the 22.9 percent or 183 respondents who indicated that they were aware of the debate) what was the primary thing that they had heard or read (Table 11). This was an open-ended question in which interviewers captured and recorded the respondents' statements and placed them in categories. The interviewers did not suggest answers or categories of answers to the respondents. These, then, are the respondents' own recollections about what they had heard or read and they appear in order of frequency of response.

- Mention of paper or paper trail – 35.0 percent
- Concern about trustworthiness, reliability and related – 17.5 percent
- Lack of ability to provide valid vote count or recount – 9.8 percent
- Mention of concern about hackers, security or related – 7.1 percent
- General concern about malfunctioning equipment – 3.3 percent
- Mention of optical scan – 1.6 percent
- Other – 1.6 percent
- Don't know or don't recall – 24.0 percent

The issue of a paper trail or paper record has been a consistent theme in the debate abound Maryland's touch screen voting system for some time. Consequently, I sought to learn what Maryland's registered voters thought that the term paper trail meant. I asked this question of all respondents (Table 12). These were also open-ended questions. The largest fraction of respondents – nearly four in ten (38.1 percent) – said that they did not know or that it did not mean anything to them. This was followed, in order, by:

- Voter receives paper receipt which he gives to an election official – 18.9 percent
- Election officials get paper copies of all votes – 11.4 percent
- Other – 9.1 percent
- Election can be recounted – 9.0 percent
- Voter gets to take a paper receipt when finished voting – 8.0 percent
- Voter views paper record behind a glass screen – 5.5 percent

Perceived Vulnerability of Maryland's Touch Screen Voting System

I next asked about voters' knowledge and opinions around the issue of the vulnerability of the Maryland touch screen voting system to outside threats. In the debate around Maryland's voting system, some parties have claimed (incorrectly) that it is vulnerable to attack because it is connected to the Internet. Here, I asked voters if they knew if the system was connected to the Internet (Table 13). Only 3.4 percent said yes to this question while a plurality (46.3 percent) said no. Slightly more than half (50.4 percent) did not know.

Next, I inquired whether the respondents felt that the system was susceptible to attack by hackers (Table 14). One in three (32.9 percent) responded affirmatively and a quarter (24.9

percent) said no. More than four in ten (42.3 percent) said that they did not know.[5] The final question in this section inquired about the voters' confidence that the State of Maryland had done all it could to prevent tampering and fraud in elections (Table 15). Seven in ten (70.4 percent) were confident that the state had done all it could, including 22.9 percent who were very confident and 47.5 percent were somewhat confident. Only one in five (21.8 percent) were not confident, including 13.0 percent were not too confident and only 8.8 percent who were not confident at all. Taken together, these data reaffirm the conclusion presented earlier that most Maryland registered voters do not lack confidence in the current voting system, even though they have understandable concerns about external threats to it. (Again, more on this later.)

Controversy over Touch Screen Voting Systems

This section reports registered voters' responses to a series of statements about touch screen voting systems. I prefaced these statements in the context of pros and cons about the systems as presented by opponents and supporters of them. Here is that preface:

As you may know, a disagreement exists about touch screen voting systems. Opponents of touch screen voting systems say that they can't be trusted to accurately record and count votes because they lack independent verification systems to verify the votes at the time of voting and in any recount. Supporters say that touch screen voting systems are reliable and easy to use and that security measures put in place by election officials ensure that they accurately record and count votes at the time of voting and in any recount.

I'm going to read you some statements from both sides of this disagreement. Based on what you know about touch screen voting systems, please tell me whether you agree or disagree with these statements. That is do you agree strongly, agree somewhat, disagree somewhat or disagree strongly.

With one notable exception, the responses were fairly consistent with responses to several previous questions that were asked outside of the specific context of the disagreement over touch screen voting systems. As such and with one exception, these responses serve to reinforce previous findings about voters' mainly positive opinions about and attitudes Maryland's current voting system (Table 16).

Here are the statements and the responses to them. Touch screen systems:

- Are reliable – 73.2 percent agree; 16.2 percent disagree; 10.8 percent don't know.
- Cannot be trusted – 64.4 percent disagree; 24.0 percent agree; 11.6 percent don't know.

[5] In this case as well as in the cases of several other questions, relatively high fractions of "don't know" responses suggest the availability of a "teaching moment" that the SBE and other parties could employ to educate and inform voters about aspects of the state's voting system.

- Accurately record and counts votes – 72.9 percent agree; 15.5 percent disagree; 11.6 percent don't know.

- Can be tampered with and hacked into – 47.6 percent agree; 35.8 percent disagree; 16.8 percent don't know.

- Election officials' security measures prevent tampering and hacking – 52.9 percent agree; 30.2 percent disagree; 16.9 percent don't know.

- Voters should be able to confirm their votes on paper records or receipts – 69.4 percent agree; 23.0 percent disagree; 7.6 percent don't know

One noteworthy response is that 69.4 percent of registered voters believe that voters should be able to confirm their votes on paper records or receipts. I will return to this matter and place paper trail in the context of the rest of the findings of this study a bit later. Now, I move to the final sets of questions in the survey.

Equipment Attached to Maryland's Touch Screen Voting Systems

I asked three questions concerning voters' factual knowledge about equipment that might be part of Maryland's touch screen voting system (Table 17). Four in ten voters (40.3 percent) correctly stated that the system does not have external printers that provide a paper record. However, just over half (53.9 percent) were not sure and nearly six percent thought it did have external printers. Only 6.9 percent of voters correctly stated that the systems have internal printers than provide a paper record while a third (36.6 percent) said no and more than half (56.5 percent) were not sure. More than one in ten voters (11.8 percent) incorrectly stated that the system has some kind of verification system attached to it while more than one-quarter (26.4 percent) said it did not and nearly two-thirds (61.9) percent were not sure.

Computer and Internet Use; Trust in Computers and Government

I asked questions about computer and Internet use to gauge the extent to which Maryland voters are familiar with information systems and technology. The answers to these questions will be useful in further analysis of the survey responses. For example, is there a digital divide among Maryland registered voters and does it systematically affect their attitudes toward and opinions of voting systems and technology? I will present this higher level analysis in a subsequent report. For now, I report the frequency distribution of the responses.

Maryland is a high socioeconomic status (SES) state. That is, its citizens are among the most well educated and affluent of any state. Many of them also hold high status jobs. Data from previous studies of computer and Internet use show a direct correlation between education and income and computer and Internet use. Maryland is no exception (Table 18). More than eight in ten registered voters (80.9 percent) use computers daily or several times a week while 8.1 percent use computers occasionally. Only one in ten (11.0 percent) report never using

computers. Similarly, most (85.0 percent) of computer users use the Internet daily or several times a week while only one in ten (11.1 percent) use the Internet occasionally and only 3.9 percent report never using it. Maryland voters who use the Internet also buy things using credit cards on the Internet. More than half (57.3 percent) report buying things on the Internet daily or several days a week and another 20.9 percent do so occasionally. Only 21.5 percent reported never buying things on the Internet.

A person's trust, whether in technology or institutions, may affect his or her attitudes and behavior. Hence, I asked about the voters' trust in computers and in government. Not surprisingly, especially given the findings presented in Table 18, Maryland registered voters have a high level of trust in computers (Table 19). Here, nearly three-fourths (70.0 percent) have either a very high or a high level of trust computers compared to only 21.2 percent whose level of trust in computers is either low of very low.

Government does not fare as well (Table 20). Only 44.4 percent of Maryland voters have a high or very high level of trust in government compared to 46.4 percent with a low or very low level of trust.

Paper Trail and Security Concerns in Context

In this section, I place the seemingly anomalous responses from registered voters about wanting a paper trail and security concerns around touch screen voting systems into the context of the overall findings of this study.

First, positive responses to survey questions far outnumber negative ones. Here are the principal examples. Voters' experiences with the voting system that they used in the 2004 general election were highly positive (91.9 percent – Table 4). A large majority of voters (81.5 percent) were confident that the system that they used in 2004 recorded and counted their votes accurately (Table 5). Fewer than half of the respondents (45.5 percent) had heard or read anything about touch screen voting systems in the past year or two. And half of these respondents (48.8 percent) had heard or read positive things (Tables 6 and 7).

Most voters (60.5 percent) believe that touch screen systems count the vote accurately and provide for an accurate recount (55.9 percent). A plurality (39.9 percent) believe that they are secure from fraud and tampering (Table 8). And voters' overall opinion of touch screen voting systems is favorable (76.3 percent).

Few voters (22.9 percent, n = 183) have heard or read of people calling for different voting technologies or equipment to be added to or used in place of Maryland's touch screen voting system (table 10). Fewer still (35 percent of the 22.9 percent, n = 64) mentioned paper or paper trail when asked what they had heard (Table 11). Also, few voters understand what the term paper trail means (Table 12).

Most voters (70.4 percent) are confident that Maryland has done all that it could to prevent tampering, fraud or other actions that could adversely affect the outcome of elections

(Table 15). Most voters also agree that touch screen voting systems are reliable (73.2 percent), can be trusted (64.4 percent), accurately records and counts votes (72.9 percent) and that security measures instituted by election officials prevent hacking (52.9 percent). See Table 16. Finally (Table 19), voters have a high level of trust in computers (70.0 percent).

These data suggest two things. First, contrary to some of the rhetoric heard in the debate around the election system in Maryland, no crisis of confidence exists among Maryland registered voters about the State's touch screen voting system as it is currently implemented. Second, to the contrary, voters exhibit a reasonable and in some cases a high level of trust and confidence in that system.

These findings, however, must be balanced with responses from other questions that suggest that voters have understandable concerns. For example, a majority (Table 8) believes that touch screen voting systems can be corrupted by malicious software programming (55.1 percent although 26.0 percent responded that they don't know). The reality is that any computer or information system can be so corrupted. Table 8 also shows that while a plurality of voters (39.9 percent) believe that touch screen voting systems are secure from fraud and tampering, nearly a third (29.1 percent) disagreed and about the same fraction (31.1 percent) said that they did not know.

When given the preface and context that a disagreement exists about touch screen systems and then asked to respond to statements about those systems, nearly half of respondents (47.6 percent) said that they could be tampered with or hacked into (Table 16). However, 35.8 percent of voters disagreed and 16.8 percent said that they did not know. Maryland registered voters are relatively sophisticated. They are high SES persons who use computers and the Internet. As such, they will be aware that in general computer and information systems are susceptible to be tampered with or hacked into. But as shown above, a larger fraction (52.9 percent) believes that *"security measures put in place by election officials make certain that the touch screen voting systems cannot be tampered with or hacked into…"*

Finally, seven in ten respondents (69.4 percent) agreed that voters *"should be able to confirm the votes they cast on touch screen systems by looking at paper records or receipts of their votes."* This should not be surprising, given people's familiarity with receipts from self-service transactions (e.g., gas pumps, movie ticket kiosks, ATMs, etc.). Ask if anyone wants a receipt after any transaction, and the majority of persons will almost certainly say yes. No empirical data, of which I am aware, exist on the subject of receipt retention, use and management, and additional research in this area would be helpful. There is evidence from at least one election that most voters do not use the paper trail to verify their votes. In a video study of voters in Las Vegas in the 2004 general election, fewer than 40 percent actually looked at the paper trail to confirm their ballots and many of those voters merely glanced quickly, hit the confirm button and moved on (Los Angeles County, Registrar/Recorder, 2004).

The usability study of vote verification systems conducted for the SBE by Herrnson, et al. (2006) confirmed this finding in a different way. This study found that voters did not carefully and attentively confirm their ballots in the voting booth. Moreover, voters experienced recall difficulties between the act of voting on the touch screen and the act of confirmation on the vote

verification unit. Findings from both of these studies call into question whether voter verification, in any event, will be a useful add-on to any voting system.

Finally, the data in Table 20 show that Maryland registered voters do not have a higher level of trust in government (44.4 percent have a high level of trust in government versus 46.4 percent with a low level of trust). More voters have a higher level of trust in computers (70.0 percent) than in government (Table 19).

Conclusion

The findings from this survey of registered voters in Maryland show that there is no crisis of confidence in Maryland's touch screen voting system as it is currently implemented. In fact, the data show the opposite. They show that voters are satisfied with and confident in the system. At the same time, and even though voters believe that the state has done all it could to secure the system from fraud and tampering, they are concerned about matters of security around and hacking into the system.

Here, the SBE can do two things that should improve voters' confidence that the system is secure from fraud, tampering and hacking. First, as recommended in the technical study of vote verification systems conducted by UMBC researchers (of which I was a co-researcher), in future elections the SBE should expand its use of parallel testing to raise the security bar even higher. It should also undertake a full scale security analysis of current procedures and practices. Second, the SBE, perhaps together with groups like the League of Women Voters and with the local boards of elections (LBEs), can and should conduct a public information and education campaign to show voters what is being done to secure the system from tampering, hacking, malicious programming and other malicious acts and accidents that may compromise elections.

Data Tables

Table 1
Demographics: Sample Compared to the State

	Sample		State
	No.	**Percent**	**Percent**
Party Affiliation*			
Democrat	427	53.4	55.2
Republican	245	30.6	29.3
Independent	105	13.1	13.9
Other	13	1.6	1.5
Don't Know/Refused	10	1.3	0.0
Age			
18-34	143	17.9	30.2
35-49	232	29.0	33.8
50-64	261	32.6	20.8
65+	151	18.9	15.2
Refused	13	1.6	
Education**			
No High School	22	2.8	16.2
High School degree	142	17.8	26.7
Some College	208	26.0	25.7
Bachelor's	286	35.8	18.0
Graduate/Professional	133	16.6	13.4
Refused	9	1.1	
Gender			
Male	387	48.4	48.2
Female	413	51.6	51.8
Race/Ethnicity***			
White	580	72.5	64.0
Black	181	22.6	27.7
Hispanic	14	1.8	4.3
Other	8	1.0	6.1
Refused	17	2.1	
Household Income			
<$25,000	35	4.4	20.6
$25,000-$49,999	69	8.6	26.1
$50,000-$74,999	165	20.6	21.6
$75.000-$99,999	178	22.3	13.6
$100,000+	231	28.9	18.1
Refused	122	15.3	

County of Residence			
Alleghany	10	1.3	1.4
Anne Arundel	80	10.0	9.2
Baltimore City	72	9.0	12.3
Baltimore County	118	14.8	14.2
Calvert	13	1.6	1.4
Caroline	4	0.5	0.6
Carroll	27	3.4	2.8
Cecil	13	1.6	1.6
Charles	20	2.5	2.3
Dorchester	4	0.5	0.6
Frederick	34	4.3	3.7
Garrett	4	0.5	0.6
Harford	38	4.8	4.1
Howard	45	5.6	4.7
Kent	3	0.4	0.4
Montgomery	139	17.4	16.5
Prince George's	107	13.4	15.1
Queen Anne's	7	0.9	0.8
St. Mary's	13	1.6	1.6
Somerset	3	0.4	0.5
Talbot	6	0.8	0.6
Washington	19	2.4	2.5
Wicomico	13	1.6	1.6
Worchester	8	1.0	0.9

* From State Board of Election registration database for October 30, 2004. All other "state" data are from the 2000 census;
** "State" data for education are based on the number of persons over age 25;
*** "State" data for race/ethnicity will not equal total state population or 100% due to categorizations of the census.

Table 2
Have you ever used any of the following voting systems to vote in elections in the U.S.?

	Yes		No		Not Sure		Total	
	No.	**%**	**No.**	**%**	**No.**	**%**	**No.**	**%**
Lever	637	79.6	132	16.5	31	3.9	800	100.0
Optical Scan	389	48.6	357	44.6	54	6.8	800	100.0
Punch Card	305	38.1	472	59.0	23	2.9	800	100.0
Touch Screen	696	87.0	89	11.1	15	1.9	800	100.0

Table 3
Type of voting system used in the 2004 General Election

	No.	%
Lever	25	3.1
Optical Scan	58	7.3
Punch Card	31	3.9
Touch Screen	642	80.3
Don't Know	44	5.5
Total	800	100.1

Table 4
Rate your experience with the voting system you used in the 2004 General Election

	No.	%
Very Positive	503	62.9
Somewhat Positive	232	29.0
Somewhat Negative	48	6.0
Very Negative	6	0.8
Don't Know	11	1.4
Total	800	100.1

Table 5
The voting system you used in the 2004 General Election

	Agree Strongly		Agree Somewhat		Disagree Somewhat		Disagree Strongly		Don't Know		Total	
	No.	%	No.	%	No.	%	No.	%	No.	%	No.	%
Was Easy to Use	629	78.6	160	20.0	9	1.1	0	0.0	2	0.3	800	100.0
Had Machine Equipment Problems	9	1.1	26	3.3	91	11.4	667	83.4	7	0.9	800	100.1
Allowed me to Vote Quicker	455	56.9	224	28.0	90	11.3	8	1.0	23	2.9	800	100.1
I Did not feel comfortable	63	7.9	31	3.9	147	18.4	556	69.5	3	0.4	800	100.1
I am Confident it recorded my vote accurately	481	60.1	171	21.4	43	5.4	36	4.5	69	8.6	800	100.0

Table 6
A. Heard or read anything about touch screen systems?

	No.	%
Yes	363	45.4
No	427	53.4
Not Sure	10	1.3
Total	800	100.1

B. If yes, where was it about (N=363)**?**

	No.	%
General	189	52.1
Maryland	43	11.8
Both	118	32.5
Not Sure	13	3.6
Total	363	100

Table 7
Was what you heard or read about touch screen systems (N=363)

	No.	%
Very Favorable	45	12.4
Somewhat Favorable	132	36.4
Somewhat Unfavorable	123	33.9
Very Unfavorable	50	13.8
Don't Know	13	3.6
Total	363	100.1

Table 8
Touch screen systems:

	Agree Strongly		Agree Somewhat		Disagree Somewhat		Disagree Strongly		Not Sure		Total	
	No.	**%**	**No.**	**%**	**No.**	**%**	**No.**	**%**	**No.**	**%**	**No.**	**%**
Are easy to use	535	66.9	200	25.0	21	2.6	5	0.6	39	4.9	800	100.0
Can't count vote accurately	48	6.0	104	13.0	204	25.5	280	35.0	164	20.5	800	100.0
Are secure from fraud	141	17.6	178	22.3	138	17.3	94	11.8	249	31.1	800	100.0
Can't protect privacy	94	11.8	103	12.9	218	27.3	226	28.3	159	19.9	800	100.2
Provide for an accurate recount	267	33.4	180	22.5	94	11.8	81	10.1	178	22.3	800	100.1
Can be corrupted	220	27.5	221	27.6	91	11.4	60	7.5	208	26.0	800	100.0
Make voting quicker	457	57.1	227	28.4	67	8.4	13	1.6	36	4.5	800	100.0
Are not accessible	67	8.4	94	11.8	162	20.3	274	34.3	203	25.4	800	100.2

Table 9
Overall opinion of touch screen voting systems

	No.	**%**
Very Favorable	343	42.9
Somewhat Favorable	267	33.4
Somewhat Unfavorable	87	10.9
Very Unfavorable	41	5.1
Don't Know	62	7.8
Total	800	100.1

Table 10

Heard or read anything about calls for different technology to be used with/or in place of Maryland's touch screen system?

	No.	%
Yes	183	22.9
No	617	77.1
Total	800	100.0

Table 11
Primary thing heard or read (N=183)

	No.	%
Paper trail	64	35.0
Don't Know	44	24.0
Trustworthiness	32	17.5
No valid recount	18	9.8
Security risks	13	7.1
Malfunctions	6	3.3
Other	3	1.6
Optical Scan	3	1.6
Negative mention of manufacturer	0	0.0
Total	183	99.9

Table 12
Paper trail means

	No.	%
Don't Know	305	38.1
Voter hands receipt to official	151	18.9
Official gets paper copy	91	11.4
Other	73	9.1
Can be recounted	72	9.0
Voter takes receipt	64	8.0
Voter reviews in booth	44	5.5
Total	800	100.0

Table 13
Is Maryland's touch screen system connected to the Internet when people are voting during elections?

	No.	%
Yes	27	3.4
No	370	46.3
Not Sure	403	50.4
Total	800	100.1

Table 14
Is Maryland's touch screen system susceptible to attack?

	No.	%
Yes	263	32.9
No	199	24.9
Not Sure	338	42.3
Total	800	100.1

Table 15
Confidence that Maryland has done all it could to prevent actions that could adversely affect the outcome of elections

	No.	%
Very Confident	183	22.9
Somewhat Confident	380	47.5
Not too Confident	104	13.0
Not Confident at All	70	8.8
Don't Know	63	7.9
Total	800	100.1

Table16
Touch screen systems:

	Agree Strongly		Agree Somewhat		Disagree Somewhat		Disagree Strongly		Not Sure		Total	
	No.	%	No.	%	No.	%	No.	%	No.	%	No.	%
Are reliable	259	32.4	326	40.8	59	7.4	70	8.8	86	10.8	800	100.2
Can't be trusted	81	10.1	111	13.9	298	37.3	217	27.1	93	11.6	800	100.0
Accurately count votes	248	31.0	335	41.9	77	9.6	47	5.9	93	11.6	800	100.0
Can be tampered with	142	17.8	238	29.8	195	24.4	91	11.4	134	16.8	800	100.2
Security prevents tampering	154	19.3	269	33.6	153	19.1	89	11.1	135	16.9	800	100.0
Voters should be able to confirm with paper	345	43.1	210	26.3	107	13.4	77	9.6	61	7.6	800	100.0

Table 17
Does Maryland's touch screen voting system have any of the following connected to it?

	Yes		No		Not Sure		Total	
	No.	%	No.	%	No.	%	No.	%
External printer	47	5.9	322	40.3	431	53.9	800	100.1
Internal printer	55	6.9	293	36.6	452	56.5	800	100.0
Any independent verification system	94	11.8	211	26.4	495	61.9	800	100.1

Table 18
How frequently do you:

	Daily		Several Days a Week		Occasionally		Never		Refused		Total	
	No.	**%**	**No.**	**%**	**No.**	**%**	**No.**	**%**	**No.**	**%**	**No.**	**%**
Use computer (N=800)	574	71.8	73	9.1	65	8.1	88	11.0	0	0.0	800	100.0
Use Internet (N=712)	499	70.1	106	14.9	79	11.1	28	3.9	0	0.0	712	100.0
Buy things on Internet with credit card (N= 684)	161	23.5	231	33.8	143	20.9	147	21.5	2	0.3	684	100.0

Table 19
Level of trust in computers

	No.	%
Very High	121	15.1
High	439	54.9
Low	138	17.3
Very Low	31	3.9
Not Sure	71	8.9
Total	800	100.1

Table 20
Level of trust in government

	No.	%
Very High	40	5.0
High	315	39.4
Low	295	36.9
Very Low	76	9.5
Not Sure	74	9.3
Total	800	100.1

References

Los Angeles County, CA, Registrar/Recorder. 2004. DVD of Voting in VVVPAT in Las Vegas, NV, 2004General Election. Los Angeles. Author.

Herrnson, Paul S., Benjamin B. Bederson, Charles D. Hadley, Richard G. Niemi, Michael J. Hanmer (with staff assistance). 2006. The Usability of Four Vote Verification Systems: A Study Conducted for the Maryland State Board of Elections. College Park: Center for American Citizenship and Politics, University of Maryland College Park.

About the Author

Donald F. Norris is Director of the Maryland Institute for Policy Analysis and Research (MIPAR) and Professor of Public Policy at the University of Maryland, Baltimore County (UMBC). He is a specialist in urban politics, public management, and the adoption, management and impacts of information technology (including e-electronic government) in public organizations. Dr. Norris has published four books and is under contract for two more (both about electronic government) due to be published in 2006 and 2007. He has published over 50 book chapters and articles in scholarly journals and nearly 100 monographs, reports and scholarly papers. Dr. Norris is editor-in-chief of the International Journal of Electronic Government Research. He holds a B.S. in history from the University of Memphis and an M.A. and a Ph.D. in government from the University of Virginia. He is the principal contact for this report and may be reached at norris@umbc.edu

About UMBC

Founded in 1966, the University of Maryland, Baltimore County (UMBC) is a public university located outside of Baltimore, Maryland. Fall 2005 enrollment of nearly 12,000 included 9,400 undergraduate and more than 2,000 graduate students. The University delivers an undergraduate educational experience characterized by a strong liberal arts and sciences core. Graduate programs emphasize selected areas of engineering, information technology, science, public policy, and human services. UMBC is one of 151 institutions in the Carnegie Foundation's doctoral/research-extensive classification for major research universities.

About MIPAR

Established in 1982, the Maryland Institute for Policy Analysis and Research (MIPAR) is the premier center for applied scholarly research on significant issues of public policy at UMBC. MIPAR conducts policy studies, program evaluations, surveys, and conferences on a wide range of topics. MIPAR activities, which are supported by federal agencies, private foundations, and state and local governments, link the resources of the University with policy makers in the state and region. Within the past few years MIPAR has developed a special strength in the area of information technology and government and e-government and e-democracy. MIPAR is affiliated with the UMBC Department of Public Policy, an interdisciplinary graduate program that offers master's and Ph.D. degrees, as well as advanced graduate certificates.

About NCSE

In cooperation with the Maryland State Board of Elections (SBE), MIPAR established the National Center for the Study of Elections (NCSE) in 2005. The goal of the NCSE is to utilize the intellectual resources of the University to address issues concerning elections, election technologies and election administration in Maryland and across the nation. Initially, NCSE will provide technical assistance and research support to the SBE in a variety of areas. UMBC faculty associated with NCSE, independently and in conjunction with the SBE, will pursue an active research agenda on a wide range of topics around elections, election technology and election administration, and will seek funding from a variety of sources to support this research. In this way, the work of the NCSE will have value and impact within the state of Maryland and nationally.

Appendix

Survey Instrument

Maryland Registered Voters Survey (January 2006)

Good afternoon/evening, I am __Name of interviewer__ From the University of Maryland Baltimore County and I'm calling Maryland residents to ask them a few questions about voting in Maryland elections. Could you take a few minutes to talk with me? Your answers will be totally confidential.

SCREENING QUESTIONS:

Screener #1: Are you a registered voter in Maryland?

Yes-PROCEED No/DK-**TERMINATE**

Screener #2: Can you tell me if you voted in the 2004 general election in Maryland? That is the last presidential election? *(If respondent is not sure, say: The presidential election in which George W. Bush and John Kerry ran for president)*:

Yes-PROCEED No/DK-**TERMINATE**

Screener #3: In that election, did you vote on a voting machine, fill out a provisional ballot or fill out an absentee ballot?

Voting Machine	1-PROCEED
Provisional Ballot	2-**TERMINATE**
Absentee Ballot	3-**TERMINATE**
Not Sure	4-**TERMINATE**

INTRODUCTION:

As you may know, several different voting systems are in use in the United States. Let me read them to you and tell me if you have ever used any of them. Have you ever used:

1. A Lever operated voting machine system – that is, a system where you pull levers to indicate your votes:

Yes 1 No 2 Not Sure 3

2. An Optical scan voting system – that is. A system where you mark a paper ballot and insert the ballot in a scanner that reads your vote:

Yes 1 No 2 Not Sure 3

3. A Punch card voting system – that is, where you punch holes in a card to record your vote:

Yes 1 No 2 Not Sure 3

4. A Touch screen voting system – that is, a system where you touch a computer screen to make your vote:

Yes 1 No 2 Not Sure 3

5. Thinking back to the 2004 general election – the one in which George W. Bush and John Kerry ran for president – do you remember which type of voting system you used when you voted? ***(Interviewer: Do not read the choices and accept only one.)***

Lever operated voting machine	1
Optical scan voting system	2
Punch card	3
Touch screen	4
Don't know or don't remember	5

6. Again, thinking back to the 2004 general election, how would you rate your experience with the voting system or voting machine you used? Was it:

Very positive	1
Somewhat positive	2
Somewhat negative	3
Very negative	4
Don't know ***(don't ask)***	5

Now I'm, going to read a few statements about your experience with the voting system or voting machine that you used to vote in the 2004 general election, please tell me if you agree strongly, agree somewhat, disagree somewhat or disagree strongly:

	Agree Strongly	Agree Somewhat	Disagree Somewhat	Disagree Strongly	Don't know ***(don't ask)***
7. It was easy to use	1	2	3	4	5
8. The specific voting machine that I used had equipment problems	1	2	3	4	5
9. It made voting faster	1	2	3	4	5
10. I did not feel comfortable using it	1	2	3	4	5
11. I was confident that it recorded and counted my vote accurately	1	2	3	4	5

Now I am going to ask you a few questions about a particular kind of voting machine, the touch screen voting system.

12. Have you heard or read anything within the past year or two about touch screen voting systems?

Yes	1
No	2-**SKIP TO Q15**
Not Sure	3-**SKIP TO Q15**

13. Was this about touch screen voting systems in general or in Maryland or both?

In general	1
In Maryland	2
Both	3
Don't know	4

14. On the whole, was what you heard or read about touch screen voting systems:

Very favorable	1
Somewhat favorable	2
Somewhat unfavorable	3
Very unfavorable	4
Don't know ***(don't ask)***	5

Now, I'm going to read some statements about touch screen voting systems. Please tell me if you agree strongly, agree somewhat, disagree somewhat or disagree strongly. Touch screen voting systems:

	Agree Strongly	Agree Somewhat	Disagree Somewhat	Disagree Strongly	Don't know ***(don't ask)***
15. Are easy to use	1	2	3	4	5
16. Cannot be relied on to count the vote accurately	1	2	3	4	5
17. Are secure from fraud and tampering	1	2	3	4	5
18. Cannot protect the privacy of the vote	1	2	3	4	5
19. Provide for an accurate recount of the vote	1	2	3	4	5
20. Can be corrupted by malicious software programming	1	2	3	4	5
21. Makes voting quicker	1	2	3	4	5
22. Are not accessible to persons with disabilities	1	2	3	4	5

23. In general, is your opinion of touch screen voting systems:

Very favorable	1
Somewhat favorable	2
Somewhat unfavorable	3
Very unfavorable	4
Don't know (**don't ask)**	5

24. Have you heard or read anything about people calling for different voting technologies or equipment to be added to or used in place of Maryland's touch screen voting system?

Yes	1
No	2-**SKIP TO Q31**

25. What was it the primary thing you heard or read? ***(Interviewer – record responses but don't ask choices.)***

1 "paper trail" any mention – **SKIP TO Q27**
2 "Optical Scan" any mention – **SKIP TO Q29**
3 General concern about the trustworthiness/reliability of system
4 General concerns about the technology malfunctioning (not malicious actions of a person)
5 Security risks/threats from hackers/internet/outside threats
6 Any negative mention of Diebold or the 'manufacturer'
7 System does not provide for valid vote count or valid recount
8 Other (record verbatim:_____)
9 Don't know or don't recall -**SKIP TO Q31**

26. What else have you heard or read?

1 "paper trail" any mention
2 "Optical Scan" any mention – **SKIP TO Q29**
3 General concern about the trustworthiness/reliability of system -**SKIP TO Q31**
4 General concerns about the technology malfunctioning (not malicious actions of a person) -**SKIP TO Q31**
5 Security risks/threats from hackers/internet/outside threats -**SKIP TO Q31**
6 Any negative mention of Diebold or the 'manufacturer' -**SKIP TO Q31**
7 System does not provide for valid vote count or valid recount -**SKIP TO Q31**
8 Other (record verbatim:_____) -**SKIP TO Q31**
9 Don't know or don't recall ***(don't ask)*** -SKIP TO Q31

27. **[If responded** 'paper trail' **in Q25 or Q26]** Would you favor or oppose adding a paper trail to Maryland's touch screen voting system? Is that strongly favor/oppose or somewhat favor/oppose?

Strongly favor	1
Somewhat favor	2
Somewhat oppose	3-**SKIP TO Q31**
Strongly oppose	4-**SKIP TO Q31**
Not Sure	5-**SKIP TO Q31**

28. What are the primary reasons you would favor adding a paper trail to Maryland's touch screen voting system? [Interviewer – record responses but do not read choices. Record all responses offered by respondents]

1 Addresses general concerns about the trustworthiness/reliability of system
2 Provides for **audit trail/independent verification** of vote
3 Provides for accurate **vote tally** or **recount**
4 Addresses Security risks/threats from **hackers/internet/other outside threats**
5 Addresses General concerns about the **technology malfunctioning** (not malicious actions of a person)
6 Addresses concerns about **Diebold or the 'manufacturer'**
7 Other (verbatim_____)
8 Don't know

*** SKIP TO Q31 ****

29. **[If mentions** optical scan **in Q25 or Q26]** Would you favor or oppose using the optical scan voting system in place of Maryland's touch screen voting system? Is that strongly favor/oppose or somewhat favor/oppose?

Strongly favor	1
Somewhat favor	2
Somewhat oppose	3-**SKIP TO Q31**
Strongly oppose	4-**SKIP TO Q31**
Not Sure	5-**SKIP TO Q31**

30. What are the primary reasons you would favor using the optical scan voting system in place of Maryland's touch screen voting system? [Interviewer – record responses but do not read choices. Record all responses offered by respondents.]

1 Addresses general concerns about the trustworthiness/reliability of system
2 Provides for **audit trail/independent verification** of vote
3 Provides for accurate **vote tally** or **recount**
4 Addresses Security risks/threats from **hackers/internet/other outside threats**
5 Addresses General concerns about the **technology malfunctioning** (not malicious actions of a person)
6 Addresses concerns about **Diebold or the 'manufacturer'**
7 **Just a better/more trusted/reliable system**
8 Other (verbatim_____)
9 Don't know

31. Can you tell me what, if anything, the term *paper trail* means to you when discussed in relation to touch screen voting? **(Interviewer: do not read choices.)**

1- Election officials get a paper copy of all votes
2- A voter receives a paper receipt to verify his or her vote and then gives the receipt to an election official
3- A voter views a paper record of his or her vote behind a glass screen to verify that vote
4- A voter receives a paper receipt of his or her vote to take when he or she leaves the voting booth
5- The election or the vote can be recounted
6- Other (verbatim _____)
7- Don't know or means nothing

32. To your knowledge, is Maryland's touch screen voting system connected to the Internet when people are voting in elections?

Yes 1 No 2 Not Sure 3

33. To your knowledge is Maryland's touch screen voting system susceptible to attack by hackers?

Yes 1 No 2 Not Sure 3

34. How confident are you that the State of Maryland has done all it could to prevent tampering, fraud or other actions that could adversely affect the outcome of elections. Are you:

Very confident	1
Somewhat confident	2
Not too confident	3
Not confident at all	4
Don't know ***(don't read)***	5

As you may know, a disagreement exists about touch screen voting systems.

Opponents of touch screen voting systems say that they can't be trusted to accurately record and count votes because they lack independent verification systems to verify votes at the time of voting and in any recount.

Supporters say that touch screen voting systems are reliable and easy to use and that security measures put in place by election officials ensure that they accurately record and count votes at the time of voting and in any recount.

I'm going to read you some statements from both sides of this disagreement. Based on what you know about touch screen voting systems, please tell me whether you agree or disagree with these statements. That is do you agree strongly, agree somewhat, disagree somewhat or disagree strongly. [Rotate order of Q35-40]

35. As they currently operate, touch screen voting systems are reliable.

Strong Agree 1 SW Agree 2 SW Disagree 3 Strong Disagree 4 Not Sure 5

36. As they currently operate, touch screen voting systems cannot be trusted

Strong Agree 1 SW Agree 2 SW Disagree 3 Strong Disagree 4 Not Sure 5

37. As they currently operate, touch screen voting systems accurately record and count votes in elections.

Strong Agree 1 SW Agree 2 SW Disagree 3 Strong Disagree 4 Not Sure 5

38. As they currently operate, touch screen voting systems can be tampered with hacked into by people who want to disrupt or change the outcome of elections.

Strong Agree 1 SW Agree 2 SW Disagree 3 Strong Disagree 4 Not Sure 5

39. Security measures put in place by election officials make certain that touch screen voting systems cannot be tampered with or hacked into in order to disrupt or change the outcome of elections.

Strong Agree 1 SW Agree 2 SW Disagree 3 Strong Disagree 4 Not Sure 5

40. Voters should be able to confirm the votes they cast on touch screen voting systems by looking at paper records or receipts of their votes.

Strong Agree 1 SW Agree 2 SW Disagree 3 Strong Disagree 4 Not Sure 5

To your knowledge, does Maryland's Touch screen voting system have any of the following connected to or associated with it? That is does it have an: [Rotate Order of Q41-43]

41. External printer that provides a paper record

Yes 1 No 2 Not Sure 3

42. Internal printer that provides a paper record.

Yes 1 No 2 Not Sure 3

43. Any type of independent verification system.

Yes 1 No 2 Not Sure 3

Now let me ask you some questions about your use of computers:

44. How frequently do you use computers at home, at work or elsewhere?

Daily	1
Several days a week	2
Occasionally	3
Never	4 **-SKIP TO Q47**

45. How frequently do you use the Internet:

Daily	1
Several days a week	2
Occasionally	3
Never	4 **-SKIP TO Q47**

46. How often do you buy things using your credit card on the internet? [READ LIST]

Frequently	1
Occasionally	2
Rarely	3
Never	4
Refused (DO NOT READ)	5

47. In general, what is your level of trust in computers? Is it: [READ LIST]

Very high	1
High	2
Low	3
Very low	4
Not Sure (DO NOT READ)	5

48. In general, what is your level of trust in government? Is it: [READ LIST]

Very high	1
High	2
Low	3
Very low	4
Not Sure (DO NOT READ)	5

Now let me ask you a few questions about yourself?

49. With which political party are you registered to vote in Maryland? Are you a registered as:

Democrat	1
Republican	2
Independent/Unaffiliated	3
Or Other Party, such as Green or Libertarian?	4
DK/Refused (DO NOT READ)	5

50. Can you tell me your age?

18-34	1
35-49	2
50-64	3
65+	4
Refused	5

51. Can you tell me the highest level of education you completed?

Didn't finish high school	1
High school diploma or GED	2
Some college/Technical Training	3
Batchelor's degree	4
Graduate or Professional degree	5
Refused	6

52. NOTE SEX:

Male	1
Female	2

53. Is your race or ethnicity:

White/Caucasian	1
Black/African-American	2
Hispanic/Latino	3
Asian or Other	4
Refused (DO NOT READ)	5

54. Can you tell me your total household income? That is, the total income of all the persons living in your household combined? Is it:

Less than 25,000	1
25,000 to 49,999	2
50,000 to 74,999	3
75,000 to 99,999	4
$100,000+	5
Refused (DO NOT READ)	6

55. What county do you live in?

Alleghany County	01
Anne Arundel County	02
Baltimore City	03
Baltimore County	04
Calvert County	05
Caroline County	06
Carroll County	07
Cecil County	08
Charles County	09
Dorchester County	10
Frederick County	11
Garrett County	12
Harford County	13
Howard County	14
Kent County	15
Montgomery County	16
Prince George's County	17
Queen Anne's County	18
St. Mary's County	19
Somerset County	20
Talbot County	21
Washington County	22
Wicomico County	23
Worcester County	24

A Study of Vote Verification Technologies for the Maryland State Board of Elections

Executive Summary

This Executive Summary presents the principal findings of two studies of vote verification technologies that were commissioned in 2005 by the Maryland State Board of Elections (SBE). The first, or the technical study, was conducted by researchers at the University of Maryland, Baltimore County (UMBC). The second, or the usability study, was conducted by researchers at the University of Maryland, College Park.

We note that while these studies were commissioned by the SBE, they were conducted independently of the SBE and, independently of one another. This should provide the citizens and decision-makers in the State of Maryland with a high degree of confidence that the studies are impartial and scientifically sound.

Part I: Technical Study Executive Summary

Scholars at UMBC, working through the National Center for the Study of Elections of the Maryland Institute for Policy Analysis and Research, conducted a technical review of vote verification systems for the Maryland State Board of Elections (SBE). Initially, the review was supposed to include up to seven systems from the following organizations and individuals: VoteHere (Sentinel); SCYTL (Pnyx.DRE); Prof. Ted Selker, MIT (VVAATT); Diebold's VVPAT; Democracy Systems, Inc. (VoteGuard); IP.Com; and Avante. We determined that IP.Com did not represent a true vote verification technology, and Avante and Democracy Systems, Inc., declined to participate in the study. We also examined the SBE's procedures for "parallel testing" of the Diebold AccuVote-TS (touchscreen) voting system in use in Maryland and used this as a baseline against which to evaluate the vote verification systems.

In conducting our analysis, we received demonstrations from the vendors, and we examined the vendors' hardware, software, and documentation to determine if their products did what their vendors claim that they do. That is, do they enable voters who use the touchscreen voting system in use in the State of Maryland to verify that their votes were cast as intended, recorded as cast, and reported as recorded, and do they permit post-election auditing? We examined such issues as:

- implementation
- impact on current state voting processes and procedures
- impact on voting
- functional completeness
- security against fraud, attack and failure
- privacy
- reliability
- accessibility

We also compared these systems to one another and to the state's current voting system and procedures, which includes the SBE's use of parallel testing around that system.

We note several specific concerns about these products, including the following:

1. Only one of these products, the Diebold VVPAT, provides for a pure paper solution.
2. All of these products would impose significant one-time implementation and on-going management burdens (cost, effort, security, etc.) on the SBE and the state's 24 Local Boards of Elections.
3. All would increase the complexity of the act of voting.
4. All would increase the amount of time required to vote.
5. All would at least double the amount of effort required to administer elections.
6. All would adversely affect voter privacy.
7. These products would have both potentially positive and potentially negative impacts on security and election integrity.
8. None can be considered as fully accessible to persons with disabilities and none of them fully meets the accessibility standards of Section 508 of the Rehabilitation Act.

9. Integration of these systems will require the cooperation of Diebold to develop and/or ensure the viability of a working interface between the vendors' products and the Diebold system.

Our principal findings are, first, that each of the systems we examined *may* at some point provide a degree of vote verification beyond what is available through the Diebold System as currently implemented. But this is true only *if the system were fully developed, fully integrated with the Diebold DREs and effectively implemented.*

Our second principal finding is that none of these systems is yet a fully developed, commercially ready product. None of these products had been used in an election in the U.S. (SCYTL has been used outside the U.S. and a different version of the Diebold VVPAT has been used in the U.S.).

Were the State of Maryland to decide to acquire any of these products, the vendor would have to invest additional money and effort to produce an actual product and make the product ready for use in actual elections. Indeed, nearly all of these vendors are looking for some level of external support to fully develop and commercialize their products.

In our expert opinion, it is a bad idea for governments to buy products that are not functionally complete and that either do not have positive records in the market place or that cannot be fully and effectively tested in simulated elections to ascertain their performance characteristics.

Therefore, based on the evidence from this study, we cannot recommend that the State of Maryland adopt any of the vote verification products that we examined at this time.

We would note that no election system—regardless of the technology involved—is foolproof nor is any election system completely immune or secure from fraud and attack. Indeed, there is a long and inglorious history of election fraud in the U.S. that involves nearly all methods and technologies of voting, especially paper voting systems. Moreover, it would be prohibitively costly to make any election totally secure.

Finally, regardless of what the State of Maryland does in the near term with regard to vote verification and vote verification systems, in future elections, it should expand the use of parallel testing. The state should also undertake a full-scale assessment of the security procedures and practices around its current voting system. We say this even with the knowledge that current security procedures are reasonable and prudent and that the SBE's system of parallel testing, as currently implemented, reduces considerably the possibility of fraud and attack on the system.

Part 11: Usability Study Executive Summary

The University of Maryland's Center for American Politics and Citizenship, along with the Human-Computer Interaction Lab, conducted a usability study of four vote verification systems and a voting system with no verification unit for the Maryland State Board of Elections.

The major findings from the expert review by human-computer interaction experts are:

- There was a perceived trade-off between usability and security. In all cases, the verification system appeared to reduce the usability of the voting process compared to the Diebold AccuVote-TS, which had no verification unit.
- The Diebold AccuVote-TSx with the AccuView Printer Module (paper printout, referred to as AccuView Printer) was rated most favorably. However, suggestions were made for improvement and questions were raised about the paper record's utility when used for a long ballot.
- Privacy concerns were raised about each of the four vote verification systems.

The major findings from the field test involving more than 800 Marylanders are:

- All of the systems were viewed favorably, including the Diebold AccuVote-TS with no verification unit.
- The Diebold with AccuView Printer was rated the most favorably in terms of voter satisfaction, but not substantially better than the AccuVote-TS with no verification unit or the VoteHere Sentinel.
- The MIT (audio) system was found to be distracting and it failed to generate as much confidence as other systems. It also was criticized by some users because of sanitary concerns related to the repeated use of the same headset.
- Participants needed the least amount of help when using the Diebold AccuVote-TS system (no verification unit). The Diebold with AccuView Printer

system (paper trail) came next. Voters received more help using the VoteHere (Internet or telephone), MIT (audio), and Scytl (monitor) systems.

The major findings concerned with election administration are:

- Adding any of the four verification systems greatly increased the complexity of administering an election.
- The paper spool in the Diebold AccuView Printer had to be changed frequently, and changing it was fairly complex.
- It was difficult and time consuming to set up the Scytl system.
- The Scytl, MIT, and Diebold AccuVote-TS with no verification unit were out of commission for some portions of the study (but not enough to affect the results).
- Diebold provided outstanding response to service calls. Scytl (based in Spain) provided poor service. No service calls were made to MIT or VoteHere.

Recommendations

- On the basis of usability and some administrative considerations, we cannot recommend that the State of Maryland purchase any one of the vote verification systems (or system prototypes) that were reviewed. There are some important tradeoffs between usability and other considerations, including the security of the vote.
- We recommend that the voter interface of AccuVote-TS (with no printer unit) be modified to incorporate some of the improvements made to the interface of the AccuVote-TSx with the AccuView Printer system.
- The AccuVote-TS with no verification unit became inoperative while an individual was voting under normal circumstances. This had a direct impact on the usability of the system and caused concern among voters. An explanation was provided but it was beyond the scope of this study to confirm it. We recommend this situation be addressed.

STATEMENT OF THE U.S. ELECTION ASSISTANCE COMMISSION

INTRODUCTION

EAC is a bipartisan commission consisting of four members: Paul DeGregorio, Chairman; Ray Martinez III, Vice Chairman; Donetta Davidson; and Gracia Hillman. EAC's mission is to guide, assist, and direct the effective administration of federal elections through funding, innovation, guidance, information and regulation. In doing so, EAC has focused on fulfilling its obligations under HAVA and the *National Voter Registration Act* (NVRA). EAC has employed four strategic objectives to meet these statutory requirements: Distribution and Management of HAVA Funds, Aiding in the Improvement of Voting Systems, National Clearinghouse of Election Information, and Guidance and Information to the States. Each program will be discussed more fully below. The topic at hand involves our strategic efforts to aid in the improvement of voting systems.

AIDING IN THE IMPROVEMENT OF VOTING SYSTEMS

One of the most enduring effects of HAVA will be the change in voting systems used throughout the country. All major HAVA funding programs can be used by states to replace outdated voting equipment. HAVA established minimum requirements for voting systems used in federal elections. Each voting system must:

- Permit the voter to verify the selections made prior to casting the ballot;
- Permit the voter to change a selection prior to casting the ballot;
- Notify the voter when an over-vote occurs (making more than the permissible number of selections in a single contest);
- Notify the voter of the ramifications of an over-vote;
- Produce a permanent paper record that can be used in a recount or audit of an election;
- Provide accessibility to voters with disabilities;
- Provide foreign language accessibility in jurisdictions covered by Section 203 of the *Voting Rights Act;* and
- Meet the error rate standard established in the 2002 Voting System Standards.

According to HAVA, the requirement for access for voters with disabilities can be satisfied by having one accessible voting machine in each polling place. In addition to these requirements, Congress provided an incentive for states that were using punch card or lever voting systems by providing additional funding on a per precinct basis to replace those outdated systems with a voting system that complies with the requirements set out above.

HAVA also provides for the development and maintenance of testable standards against which voting systems can be evaluated. It further requires federal certification according to these standards. EAC is responsible for and committed to improving voting systems through these vital programs.

Voluntary Voting System Guidelines

One of EAC's most important mandates is the testing, certification, decertification and recertification of voting system hardware and software. Fundamental to implementing this key function is the development of updated voting system guidelines, which prescribe the technical requirements for voting system performance and identify testing protocols to determine how well systems meet these requirements. EAC along with its federal advisory committee, the Technical Guidelines Development Committee (TGDC), and the National Institute of Standards and Technology (NIST), work together to research and develop voluntary testing standards.

On December 13, 2005, EAC adopted the first iteration of the *Voluntary Voting System Guidelines* (VVSG). The final adoption of the VVSG capped off nine months of diligent work by NIST and the TGDC. In May of 2005, the TGDC delivered its draft of the VVSG. EAC then engaged in a comprehensive comment gathering process, which included comments from the general public as well as from members of its Board of Advisors and Standards Board. Interested persons were able to submit comments on-line through an interactive web-based program, via mail or fax, and at three public hearings (New York, NY; Pasedena, CA; Denver, CO). EAC received more than 6,000 individual comments. EAC teamed up with NIST to assess and consider every one of the comments, many of which were incorporated into the final version.

The VVSG is an initial update to the 2002 Voting System Standards focusing primarily on improving the standards for accessibility, usability and security. The 2005 VVSG significantly enhances the measures that must be taken to make voting sys-

tems accessible to persons with disabilities and more usable for all voters. For example, the 2002 VSS contained 29 accessibility requirements, focusing primarily on accommodating persons with visual disabilities. The 2005 VVSG contains 120 requirements that establish testing measures to assure that voting systems accommodate all persons with disabilities, including physical and manual dexterity disabilities. In addition to ensuring accessibility requirements were increased and strengthened, the 2005 VVSG includes for the first time a usability section, which addresses the needs of all voters, empowering them to adjust voting systems to improve interaction. Those testing measures include allowing adjustment of brightness, contrast, and volume by the voter to suit his/her needs.

The 2005 VVSG also incorporated standards for reviewing voting systems equipped with voter-verifiable paper audit trails (VVPAT)[1] in recognition of the many states that now require this technology. In accordance with HAVA and to assure that persons with disabilities had the same access to review their ballots as non-disabled voters, the 2005 VVSG required VVPATs to be accessible when the paper record would be used as the official ballot or as definitive evidence in a recount. In addition, the VVSG addressed new technologies that emerged on the market since the 2002 VSS, such as wireless technology. Standards were established to require the wireless mechanism to be disabled during voting and to provide a clear, visual indicator showing when the wireless capability is activated. VVSG also establishes testing methods for assessing whether a voting system meets the guidelines. A complete listing of the changes and enhancements included in the 2005 VVSG can be found on the EAC web site, *http://www.eac.gov/Summary%20of%20Changes%20to%20VVSG.pdf.*

The 2005 VVSG, like the 1990 and 2002 VSS, is a voluntary set of voting system testing standards. States choose to make these standards mandatory for equipment purchased in those states by requiring national certification according to those standards in their statutes and/or rules and regulations. Currently, approximately 40 states require certification to either the 2005 VVSG or the 1990 or 2002 VSS. When EAC adopted the 2005 VVSG, it did so with an effective date of December 13, 2007. This two-year period was designed to allow states the time needed to make changes to their laws, rules and regulations to require certification to the new standards, as is standard practice when introducing new industry guidelines. New York has already legislatively mandated certification to the 2005 VVSG, and EAC expects over the next several years that the vast majority of the states will make changes to their legislation requiring certification to the 2005 VVSG. Prior to December 13, 2007, voting systems, components, upgrades and modifications can be tested against either the 2002 VSS or the 2005 VVSG, depending on the requirements of the states and manufacturers' requests. After December 13, 2007, EAC will no longer test systems to the 2002 VSS; systems and upgrades will only be tested to the 2005 VVSG.

Significant work remains to be done to fully develop a comprehensive set of standards and testing methods for assessing voting systems and to ensure that they keep pace with technological advances. In FY 2007, EAC along with TGDC and NIST, will revise sections of the VVSG dealing with software, functional requirements, independent verification, and security and will develop a comprehensive set of test suites or methods that can be used by testing laboratories to review any piece of voting equipment on the market. Much like the roll out of the 2005 VVSG, these future iterations will be adopted with an effective date provision and a procedure for when new voting systems, components, upgrades and modifications will be required to be tested against the new iteration of the VVSG.

Accreditation of Voting System Testing Laboratories

HAVA Section 231 requires EAC and NIST to develop a national program for accrediting voting system testing laboratories. NIST's National Voluntary Laboratory Accreditation Program (NVLAP) will initially screen and evaluate testing laboratories and will perform periodic reevaluation to verify that the labs continue to meet the accreditation criteria. When NVLAP has determined that a lab is competent to test systems, the NIST director will recommend to EAC that a lab be accredited. EAC will then make the determination to accredit the lab. EAC will issue an accreditation certificate to the approved labs, maintain a register of accredited labs and post this information on its web site to fully inform the public about this important process.

[1] VVPAT is an independent verification method that allows the voter to review his/her selections prior to casting his/her ballot through the use of a paper print out. VVPAT is merely one form of independent verification. EAC is currently working with NIST to develop standards for additional methods such as witness systems, cryptographic systems, and split process systems.

In June 2005, NVLAP advertised for the first class of testing laboratories to be reviewed under the NVLAP program and accredited by EAC. Three applications were received in the initial phase, with two additional applications following in late 2005. Pre-assessments of these laboratories began in April 2006 and formal review is proceeding. NVLAP will conduct full evaluations of at least two initial applicants this fall and, depending on the outcome of the evaluations, will make initial recommendations to the EAC before the end of the year. All qualified candidates from among the pool of five applicants will be sent to the EAC by spring 2007.

In late 2005, EAC invited laboratories that were accredited through the National Association of State Election Directors (NASED) program as Independent Testing Authorities (ITAs) to apply for interim accreditation to avoid a disruption or delay in the testing process. All three ITAs have applied for interim accreditation. Interim accreditation reviews by EAC contractors are under way and are expected to be completed by September 2006. ITAs will be accredited on an interim basis until the first class of laboratories is accredited through the NVLAP process. After that time, all testing labs must be accredited through the NVLAP evaluation process.

The National Voting System Certification Program

In 2006, EAC is assuming the duty as prescribed by HAVA to certify voting systems according to national testing standards. Previously, NASED qualified voting systems to both the 1990 and 2002 Voting System Standards. Historically, voting system qualification has been a labor intensive process to ensure the integrity and reliability of voting system hardware, software and related components. In six months, NASED received 38 separate voting system test reports for review and qualification. All requests were received, processed and monitored while the testing laboratory assessed compliance. Once a test report was produced, technical reviewers analyzed the reports prior to certification.

EAC's certification process will constitute the Federal Government's first efforts to standardize the voting system industry. EAC's program will encompass an expanded review of voting systems, and it will utilize testing laboratories accredited by EAC and experts hired by EAC to assure that the tested systems adequately met the standards.

The EAC will implement the Testing and Certification Program required by Section 231(a)(1) of HAVA in two distinct phases (pre-election phase and full program). Both phases will be rolled out in 2006. The first phase of the program will begin on July 24, 2006 and terminate upon the EAC's implementation of the program's second phase. The second phase (full program) will begin on December 7, 2006.

The pre-election phase of the program focuses on providing manufacturers a means to obtain federal certification for modifications required by State and local election officials administering the 2006 General Election. This pre-election phase will ensure a smooth and seamless transition from the NASED program (which has qualified voting systems at the national level for more than a decade) to the more rigorous and detailed EAC program. This will be done by delaying implementation of some the procedural requirements found in the full program until after the critical pre-election period. This will allow the EAC to diligently review voting system modifications while, at the same time, ensuring a smooth transition and avoiding the unacceptable delays often associated with rolling out a new program.

The full program will begin in December by requiring every voting system manufacturer that desires to have a product certified to register and disclose information about the company and its owners, board members and decision-makers. Manufacturers will be subject to a conflict of interest analysis including reviewing whether any owners or board members are barred from doing business in the United States. EAC will test complete voting systems including new components and how they integrate with the entire voting system. This process will be achieved by having technical experts review the reports provided by accredited testing laboratories to assure that the tests performed and the results are consistent with a system that conforms to the VVSG. These experts will recommend conforming systems for certification. Another new feature of the EAC certification program will be the quality assurance program. Through site visits to manufacturing facilities and field inspections, EAC will confirm that the systems that are being manufactured, sold to and used by election jurisdictions throughout the country are the same as those certified by EAC. Last, EAC will introduce a decertification process that will allow involved persons to file complaints of non-conformance, provide for the investigation of those complaints, and if warranted decertify systems because of a failure to conform to the VVSG.

Election Management Guidelines

To complement the VVSG, the EAC is creating a set of election management guidelines. These guidelines are being developed by a group of experienced state and local election officials who provide subject matter expertise. The project will focus on developing procedures related to the use of voting equipment and procedures for all other aspects of the election administration process. The election management guidelines will be available to all election officials if they wish to incorporate these procedures at the State and local levels. These guidelines cover the following topics:

- Storage of equipment
- Equipment set up
- Acceptance testing
- Procurement
- Use
- Logic and accuracy (validation) testing
- Tabulation
- Security protocols (all phases—storage, set up, transport and Election Day)
- Training of employees/poll workers
- Education for voters

The first of these management guidelines was issued by EAC in June 2006 in the form of a *Quick Start Guide* for election officials. This guide focused on the issues and challenges faced by election officials as they accept and implement new voting systems. The guide gave tips to the election officials on how to avoid common pitfalls associated with bringing new voting systems on-line.

2006: A YEAR OF CHANGE, CHALLENGE AND PROGRESS

The federal elections in 2006 have and will mark a significant change in the administration of elections. In compliance with HAVA, states have purchased and implemented new voting systems. There is a strong shift to electronic voting, although optical scan voting is still popular. In addition, states have imposed new requirements on their voting systems, and they have implemented their own testing programs for voting systems they purchase. And, in at least 25 states, voter-verified paper audit trails (VVPAT) have been required for all electronic voting. Due to the introduction of new voting systems throughout the Nation, the voter's experience at the polls will be quite different in 2006 than it was in 2000. It is estimated that one in three voters will use different voting equipment to cast their ballots in 2006 than in 2004.

Voters with disabilities will likely experience the most dramatic changes. For the first time, every polling place must be equipped with voting machines that allow them to vote privately and independently. For many voters with disabilities, this may be the first time that they will cast ballots without the assistance of another person.

Voting systems do not represent the only changes in election administration that will be apparent in 2006. States have also developed statewide voter registration lists, which will provide the ability to verify voters' identity by comparing information with other state and federal databases. This will result in cleaner voter registration lists and fewer opportunities for fraud. Another anticipated benefit of the statewide lists will be a significantly reduced need for provisional ballots, as was the case in states that had statewide voter registration lists in 2004.

This year is one of transition, which is difficult to overcome in any business; elections are no different. The introduction of new equipment will present some challenges and hurdles to overcome. For State and local governments, there are also a host of new obligations. They must receive and test a fleet of new voting equipment. Training for staff and poll workers must be organized and conducted. And, extensive education programs must be implemented to inform the public about the new voting equipment.

Although EAC cannot be on the ground in every jurisdiction to lend a hand in these tasks, we have issued a *Quick Start Guide* to assist election officials as they implement new voting systems. We also encourage states to take proactive measures to test their voting systems and voter registration lists prior to the federal elections. Such activities have proven to be an excellent tool to identify problems and solutions prior to the stresses and unpredictability of a live election.

CONCLUSION

Over the past four years, significant changes have been made to our election administration system. New voting systems have been purchased and implemented.

Each state has adopted a single list of registered voters to better identify those persons who are eligible to vote. Provisional voting has been applied across all 50 states, the District of Columbia and four territories. However, one thing has not changed. Elections are a human function. There are people involved at every level of the election process, from creating the ballots, to training the poll workers, to casting the votes.

With these changes will come unexpected situations, even mistakes. We cannot anticipate in a process that involves so many people that it will work flawlessly the first time. What we can embrace, however, is that the process has been irrevocably changed for the better. There is a heightened awareness of the electoral process in the general public. There have been significant improvements to the election administration process. And, more people have the ability to vote now than ever before.

Voting System Independent Testing and Certification Process:

Comprehensive, Rigorous, and Objective

Prepared by:
The Election Technology Council

November 2005

About The Election Technology Council

The Election Technology Council (ETC) is a group of companies that offer products and services which support the electoral process and have decided to work together to address common issues facing their industry. These companies believe that the voting infrastructure in the United States is in pressing need of improvement, and that electronic systems introduce new levels of voting inclusiveness, accuracy, efficiency, and accessibility. Working together as a division of the Information Technology Association of America (ITAA), ETC members will help election officials, lawmakers, voters, the media and others understand and better appreciate the benefits that technology can bring to the voting process.

Founding members of the ETC are: Advanced Voting Systems, Diebold Election Systems, Election Systems & Software, Hart InterCivic, Sequoia Voting Systems, and Unilect Corporation. The Council has been joined by Danaher Guardian Voting Systems, VoteHere, and Perfect Voting System.

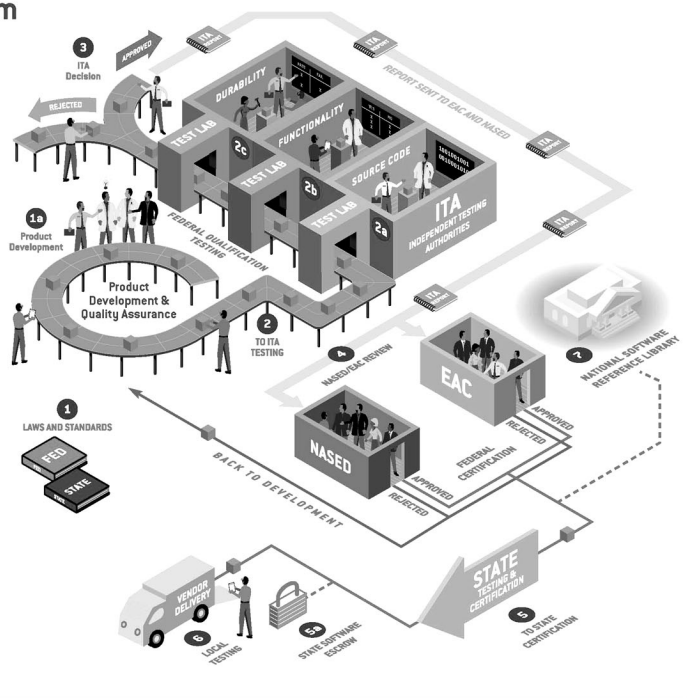
The Council affirms its complete support for voting systems testing and certification. Trust in the American system of elections is of paramount importance to our members, as it is to all parties working in the elections community. Thorough testing and review in order to provide valid certification is an important component of that trust. Hence, the Council has resolved to offer its members' experience and insights on testing and certification to those parties undertaking a review of the certification process.

VOTING SYSTEMS TESTING SUMMIT 2005

Voting System Independent Testing & Certification Process:

Comprehensive, Rigorous, and Objective

New and improved voting technology has made the election process easier, more accessible, and more secure. These enhancements benefit election administrators and voters, and encourage participation in our democracy. As technology has evolved, so, too, have procedures that ensure voting equipment deployed on Election Day is reliable, accurate, and secure. This overview depicts the comprehensive, rigorous, and objective voting system testing and certification process - at the federal, state, and local levels.



Prepared by the Election Technology Council, an association dedicated to secure and accurate voting solutions

LEGEND

1. Standards Development:
Current and evolving state and federal law, regulations, and standards define requirements that must be met before voting equipment may be used in an election. Today, the federal 2002 Voting Systems Standards provide guidance to vendors and the system-testing bodies. New standards - the Voluntary Voting System Guidelines - are currently under development.

1a. Product Development & Quality Assurance
Election systems manufacturers continually conduct new product development to enhance current voting equipment and innovate the next generation of voting technology. This development process is driven by state and federal laws/standards that establish specific voting system requirements. It is also responsive to the needs of election administrators and voters.

2. To ITA Testing:
After development, documentation, and quality assurance, to be certified to federal voting systems standards, a voting system and its component parts must go through extensive testing conducted by accredited Independent Testing Authorities (ITAs). This process begins with submission of a detailed Technical Date Packet (TDP) from the vendor.

2a. Source Code
ITAs review every line of software code to ensure compliance with standards and overall integrity. Once complete, an ITA will perform and witness the compilation of the source code into program executable files.

2b. Functionality (End-to-End System Testing)
ITAs test the functionality of the voting equipment using compiled code to ensure it operates accurately - that votes are properly captured, results are properly reported, and data is properly retained. To pass, a system must tabulate 1.5 million votes with 100% accuracy.

2b. Durability
ITAs test the operation of the voting equipment to ensure it can withstand extreme environmental conditions and intensive human handling.

3. ITA Reports
If, at any point in the testing process, an ITA identifies an issue that must be addressed, a product or component part is sent back to the vendor for additional development and resubmission through the whole ITA testing process. Only after the system or component has passed every test is it deemed qualified for federal certification. An ITA compiles the results of the entire testing process into a report which is delivered to the EAC/NASED for further review.

4. EAC/NASED Review
The NASED technical committee assesses the results of the ITA tests to ensure compliance with federal law and standards. If necessary, NASED requests clarification from the ITA and/or additional development by the vendor. Only if a system passes this review does NASED issue a number indicating formal federal certification of the specific version of the voting system.

5. State Testing & Certification
In a majority of states, federal certification is only a first step before a voting system can achieve state certification. In some cases, the state will carry out its own independent testing of the accuracy, security, and reliability of a system. State testing (which varies state-to-state) expands upon and enhances testing at the federal level. A state also will compare a product's features and functionality against state law and standards to ensure it complies.

5a. State Software Escrow
Many states require the vendor to escrow a copy of the certified system software.

6. Local Testing
After production testing and upon delivery from a vendor, local election authorities conduct acceptance testing to ensure the voting system equipment performs properly and is certified. Further still, prior to every election, local authorities test the logic and accuracy of the equipment and procedures with election-specific ballots to confirm it functions properly and is secure.

7. National Software Reference Library
After software is federally certified, election system vendors can voluntarily submit the executable code to the National Software Reference Library, which archives a validation code for future reference. This allows jurisdictions to verify the delivered system software against the archived validation code to ensure it is the certified version.

The Information Technology Association of America (ITAA) provides global public policy, business networking, and national leadership to promote the continued rapid growth of the IT industry. ITAA consists of over 350 corporate members throughout the U.S.. The Association plays the leading role in issues of IT industry concern including information security, taxes and finance policy, digital intellectual property protection, telecommunications competition, workforce and education, immigration, online privacy and consumer protection, government IT procurement, human resources and e-commerce policy. ITAA members range from the smallest IT start-ups to industry leaders in the Internet, software, IT services, ASP, digital content, systems integration, telecommunications, and enterprise solution fields. ITAA is secretariat of the World Information Technology and Services Alliance, consisting of 67 IT trade associations around the world.

For more information visit www.itaa.org.

Security Analysis of the Diebold AccuBasic Interpreter

DAVID WAGNER, DAVID JEFFERSON, AND MATT BISHOP
VOTING SYSTEMS TECHNOLOGY ASSESSMENT ADVISORY BOARD (VSTAAB)

WITH THE ASSISTANCE OF:
CHRIS KARLOF AND NAVEEN SASTRY
UNIVERSITY OF CALIFORNIA, BERKELEY

FEBRUARY 14, 2006

1. Summary

This report summarizes the results of our review of some of the source code for the Diebold AV–OS optical scan (version 1.96.6) and the Diebold AV–TSx touchscreen (version 4.6.4) voting machines. The study was prompted by two issues: (1) the fact that AccuBasic scripts associated with the AV–OS and AV–TSx had not been subjected to thorough testing and review by the Independent Testing Authorities when they reviewed the rest of the code for those systems, and (2) concern over vulnerabilities demonstrated in the AV–OS optical scan system by Finnish investigator Harri Hursti in Leon County, FL. Mr. Hursti showed that it is possible for someone with access to a removable memory card used with the AV–OS system to modify scripts (small programs written in Diebold's proprietary AccuBasic language) that are stored on the card, and also to modify the vote counts stored on the card, in such a way that the tampering would affect the outcome of the election and not be detected by the subsequent canvass procedures.

The questions we addressed are these:

- What kinds of damage can a malicious person do to undermine an election if he can arbitrarily modify the contents of a memory card?
- How can the possibility of such attacks be neutralized or ameliorated?

The scope of our investigation was basically limited to the above questions. We did not do a comprehensive code review of the whole code base, nor look at a very broad range of potential security issues. Instead, we concentrated attention to the AccuBasic scripting language, its compiler, its interpreter, and other code related to potential security vulnerabilities associated with the memory cards.

We found a number of security vulnerabilities, detailed below. Although the vulnerabilities are serious, they are all easily fixable. Moreover, until the bugs are fixed, the risks can be mitigated through appropriate use procedures. Therefore, we believe the problems as a whole are manageable.

Our findings regarding the scope of possible attacks on the AV–OS optical scan and AV–TSx touchscreen systems can be summarized as follows:

- *AccuBasic is a limited language:* The AccuBasic language itself is not a powerful programming language, but a very restricted one, narrowly tailored to one task: calculating and printing reports before and after an election. From a security point of view this is very desirable; minimal functionality generally means fewer opportunities for error or security vulnerability. In particular, *when its interpreter is properly implemented* (see below) an AccuBasic program cannot modify votes or ballot images; it can read vote counters (AV–OS) or ballot images (AV–TSx), but it cannot modify them.
- *The AccuBasic interpreter is well-structured:* The code in the AccuBasic interpreters for both machines is clean, well-structured, and internally documented. We were able to understand it with little difficulty despite the lack of external documentation.
- *Memory card attacks are a real threat:* We determined that anyone who has access to a memory card of the AV–OS, and can tamper it (i.e., modify its contents), and can have the modified cards used in a voting machine during election, can indeed modify the election results from that machine in a number of ways. The fact that the results are incorrect cannot be detected except by a recount of the original paper ballots.
- *Harri Hursti's attack does work:* Mr. Hursti's attack on the AV–OS is definitely real. He was indeed able to change the election results by doing nothing more than modifying the contents of a memory card. He needed no pass-

words, no cryptographic keys, and no access to any other part of the voting system, including the GEMS election management server.

- *Interpreter bugs lead to another, more dangerous family of vulnerabilities:* However, there is another category of more serious vulnerabilities we discovered that go well beyond what Mr. Hursti demonstrated, and yet require no more access to the voting system than he had. These vulnerabilities are consequences of bugs—16 in all—in the implementation of the AccuBasic interpreter for the AV–OS. These bugs would have no effect at all in the absence of deliberate tampering, and would not be discovered by any amount of functionality testing; but they could allow an attacker to completely control the behavior of the AV–OS. An attacker could change vote totals, modify reports, change the names of candidates, change the races being voted on, or insert his own code into the running firmware of the machine.
- *Successful attacks can only be detected by examining the paper ballots:* There would be no way to know that any of these attacks occurred; the canvass procedure would not detect any anomalies, and would just produce incorrect results. The only way to detect and correct the problem would be by recount of the original paper ballots, e.g., during the one percent manual recount.
- *The bugs are classic, and can only be found by source code review:* Finding these bugs was only possible through close study of the source code. All of them are classic security flaws, including buffer overruns, array bounds violations, double-free errors, format string vulnerabilities, and several others. There may, of course, be additional bugs, or kinds of bugs, that we did not find.
- *AV–TSx has potential cryptographic protection against memory card attacks:* A majority of the bugs in the AV–OS AccuBasic interpreter are also present in the interpreter for the AV–TSx touchscreen system. However, the AV–TSx touchscreen has an important protection that the AV–OS optical scan does not: the key contents of its removable memory card, including the AccuBasic scripts, are digitally signed. Hence, if the cryptographic keys are managed properly (see next bullet), any tampering would be quickly detected and the attack would be unsuccessful. All of the attacks we describe, and Hursti's attack as well, would be foiled, because the memory card by itself would in effect be cryptographically tamper proof.
- *But the implementation of cryptographic protection is flawed:* There is a serious flaw in the key management of the crypto code that otherwise should protect the AV–TSx from memory card attacks. Unless election officials avail themselves of the option to create new cryptographic keys, the AV–TSx uses a default key. This key is hard-coded into the source code for the AV–TSx, which is poor security practice because, among other things, it means the same key is used in every such machine in the U.S. Worse, the particular default key in question was openly published two and a half years ago in a famous research paper, and is now known by anyone who follows election security, and can be found through Google. The result is that in any jurisdiction that uses the default keys rather than creating new ones, the digital signatures provide no protection at all.
- *All the bugs are easy to fix:* In spite of the fact that the bugs we have identified are very serious, all of them are very local and very easy to fix. In each case only a couple of lines of code need to be changed. It should take only a few hours to do the whole job for both the AV–OS and AV–TSx.
- *No use of high assurance development methods:* The AccuBasic interpreter does not appear to have been written using high-assurance development methodologies. It seems to have been written according to ordinary commercial practices. In the long run, if the interpreter remains part of the code base, it and the rest of the code base should be revised according to a more rigorous methodology that would, among other things, likely have prevented the bugs we found.
- *Interpreted code is contrary to standards:* Interpreted code in general is prohibited by the 2002 FEC Voluntary Voting System Standards, and also by the successor standard, the EAC's Voluntary Voting System Guidelines due to take effect in two years. In order for the Diebold software architecture to be in compliance, it would appear that either the AccuBasic language and interpreter have to be removed, or the standard will have to be changed.
- *Bugs detailed in confidential companion report:* In a companion report we have listed in great detail all of the bugs we identified, the lines at which they occur, and the threats they pose. Because that report contains Diebold

proprietary information, and because it details exactly how to exploit the vulnerabilities we discovered, that report must be confidential.

Clearly there are serious security flaws in current state of the AV–OS and AV–TSx software. However, despite these serious vulnerabilities, we believe that the security issues are manageable by a reasonably careful combination of short- and long-term approaches. Here are our recommendations with regard to mitigation strategies.

In the short-term, especially for local elections, the security problems related to AccuBasic and the memory cards might be managed according to guidelines such as these:

- *Strong control over access to memory cards for the AV–OS:* The AV–OS optical scan is vulnerable to both the Hursti attack and attacks based on the AccuBasic interpreter bugs we found. It would be safest if it is not widely used until these bugs are fixed, and until a modification is made to ensure that the Hursti attack is eliminated. But if the AV–OS is used, strong procedural safeguards should be implemented that prevent anyone from gaining unsupervised or undocumented access to a memory card, and these procedures should be maintained for the life of all cards. Such controls might include a dual-person rule (i.e., no one can be alone with a memory card); permanent serial numbers on memory cards along with chain-of custody documentation, so there is a paper trail to record who has access to which cards; numbered, tamper evident seals protecting access to the cards whenever they are out of control of county staff; and training of all personnel, including poll workers, regarding proper treatment of cards, and how to check for problems with the seals and record a problem. Any breach of control over a card should require that its contents be zeroed (in the presence of two people) before it is used again.
- *Require generation of new crypto keys for the AV–TSx:* The AV–TSx is not vulnerable to any of these memory card attacks provided that the default cryptographic key used for signing the contents of the memory card is changed to a new, unguessable key and kept secure. If the key is changed then these threats are all eliminated, at least for the short-term. If this is not done, however, then the AV–TSx is no more secure than the AV–OS.
- *Control access to GEMS:* Access to GEMS should be tightly controlled. This is a good idea for many reasons, since a malicious person with access to GEMS can undermine the integrity of an election in many ways. In addition, in a TSx system, GEMS holds a copy of the cryptographic key used for signing the contents of the memory cards, and in both systems the GEMS server may hold master copies of the AccuBasic scripts loaded onto the memory cards.

In the longer-term, one would want to consider a number of additional measures:

- *Fix bugs:* Certainly the bugs in the source code of the interpreters for both the AV–OS and AV–TSx should be corrected with all deliberate speed, the Hursti vulnerability should be fixed, and the code re-examined by independent experts to verify that it was properly done.
- *Defensive and high assurance programming methodology:* The source code of the interpreters should be revised to introduce systematic defensive programming practices and high assurance development methods. In particular, eliminate in the firmware, insofar as possible, any trust of the contents of the memory card.
- *Protect AccuBasic code from tampering:* The AccuBasic object code could be protected from tampering and modification, either by (a) storing AccuBasic object code on non-removable storage and treating it like firmware, or by (b) protecting AccuBasic object code from modification through the use of strong cryptography (particularly public-key signatures).
- *Don't store code on memory cards:* The architecture of the AV–OS and the AV–TSx could be changed so they do not store code on removable memory cards.
- *Remove interpreters and interpreted code:* The architecture of the AV–OS and the AV–TSx could be changed so they do not contain any interpreter or use any kind of interpreted code, in order to bring the code base into compliance with standards.

2. Introduction

Scope of the study. This report summarizes the results of our review of the source code for the Diebold AV–OS optical scan (version 1.96.6) and the Diebold AV–TSx touchscreen (version 4.6.4) voting machines. This investigation, requested by the office of the California Secretary of State, was to evaluate security concerns raised by the use of AccuBasic scripts (programs) stored on removable memory cards in the two systems and offer options for their amelioration. The study was prompted by vulnerabilities demonstrated in the optical scan system by Finnish investigator Harri Hursti in Leon County, FL. Mr. Hursti showed that under certain circumstances it is possible for someone with access to a memory card to modify the scripts and modify the vote counts in a way that would not be detected by the subsequent canvass procedure, and would normally only be detectable by a recount of the paper ballots.

Our study does not constitute a comprehensive code review of the entire Diebold code base. We had access to the full code bases for the AV–OS and AV–TSx, but we did not even attempt a comprehensive review of the entire code base. Our attention was focused fairly narrowly on Diebold's proprietary AccuBasic scripting language, the compiler for that language, the interpreter for its object code, the AccuBasic scripts themselves, and the related protocols and procedures, both for the AV–OS (optical scan) and AV–TSx (touchscreen) voting systems.

In particular, we did not have the source code for the Diebold GEMS election management system, and our security evaluation does not cover GEMS at all. It is widely acknowledged that a malicious person with unsupervised access to GEMS, even without knowing the passwords, can compromise GEMS and the election it controls. This report does not address those threats, however.

Our analysis was based only on reading the source code we were given. We did not have access to a real running system (although we were able to compile and execute modified versions of the compiler and interpreter on a PC). Nor did we have any manuals or other documentation beyond that present in comments in the code itself. We had access to the source code for a period of approximately four weeks for this review.

The threat model. Different jurisdictions around the country have somewhat different procedures for conducting an election with the Diebold AV–OS and AV–TSx systems, but all include the following steps:

1. Before the election, the removable memory cards are initialized though the GEMS election management system with the appropriate election description information for the precinct the machine will be used in, and with the AccuBasic object code scripts to be used, and with other information detailed below.
2. The initialized cards are then inserted into the voting machines (optical scan or touchscreen); the compartment in which the card sits is locked and sealed with a tamper-evident seal of some kind.
3. The voting machine with its enclosed card is transported to the precinct poll site where it is stored over night (or longer) until the start of the election.
4. At the start of the election, a script on the card is used to print initial reports, including the Zero Report, which should indicate that all the vote counters are zero (in the AV–OS) and file of voted ballots is empty (in the AV–TSx).
5. All during election day, voted paper ballots are scanned and the appropriate counters on the removable memory card are incremented (AV–OS), or the voted ballots themselves are stored electronically on the memory card (AV–TSx), and electronic audit log records are appended to a file on the card.
6. At the end of election day, a script from the card is used to print final reports for the day, including vote totals.
7. Finally, one of two steps is taken, depending on the jurisdiction: either (a) the seal is broken and the memory card is removed and transported back to a central location for canvass using GEMS; or, (b) the entire voting machine is transported to the central location, where election officials break the seal, remove the memory card, and read its contents during the canvass.

The threats we are concerned about specifically involve modification of the contents of the memory card, especially the AccuBasic object code. In other words, somewhere along the line, in the procedure above, the attacker is able to get a memory card, arbitrarily modify its contents, and surreptitiously place it in a voting machine for use in an election, and do so without being immediately detected.

We assume the attacker's goal is either to change the election results undetected, or perhaps simply to disrupt the election (e.g. by causing voting machine crashes). We also assume that the attacker knows every detail of how the system works, and the procedural safeguards, and even has access to the manuals, documentation, and source code of the system. The attacker, therefore, is able to take advantage of bugs and vulnerabilities in the code. (It is standard to make these last assumptions, since it is almost impossible to keep code and related information secret from a determined attacker.)

We do not, however, assume that the attacker has any inside confederates, or has access to any passwords or cryptographic keys, or access to GEMS. We do not assume that the attacker has any access to paper ballots (AV–OS) or VVPAT (AV–TSx), nor even that he has any access to the voting system beyond the ability to insert a memory card undetected.

The process we followed. We were asked to perform a security review of the Diebold source code. As part of the review, we were provided access to the source code for the AV–OS and the AV–TSx machines. This included the source code for the AccuBasic compiler, for the AccuBasic interpreter in the AV–OS and the AccuBasic interpreter in the AV–TSx, for some AccuBasic scripts, and all other source code for the AV–OS and AV–TSx. There are two separate versions of the interpreter, one in the AV–OS and one in the AV–TSx; however, the two implementations are very similar.

We undertook a line-by-line analysis of the source code for the AV–OS AccuBasic interpreter. Three team members (Karlof, Sastry, and Wagner) read every line of source code carefully and checked for all types of security and reliability defects known to us. When we found a vulnerability in the AV–OS interpreter, we examined the corresponding portion of the AV–TSx interpreter to check whether the AV–TSx shared that same vulnerability.

After completing the line-by-line source code analysis, we applied a commercial static source code analysis tool to the AV–OS interpreter code. Code analysis tools perform an automated scan of the source code to identify potentially dangerous constructs. We obtained a copy of the Source Code Analyzer (SCA) tool, made by Fortify Software, Inc.; Fortify generously donated the tool to us for our use in this project at no cost, and we gratefully acknowledge their contribution. Two of us (Bishop and Wagner) are members of Fortify Software's Technical Advisory Board, and thus were already familiar with this tool. We manually inspected each of the warnings generated by the tool.

While our analysis uncovered several potential attacks on the system, we have not attempted to attack any working system. We performed our analysis mostly "on paper;" we did not have access to a genuine running system. We did, however, get a stubbed-out version of the code running on a PC, and were able to confirm that one of the attacks we discovered (the only one we tried) actually works.

In the end, we wrote our report in two parts. The *public* part is this document, which contains background, our findings and recommendations, and all of the explanatory information we have found to support them. The *confidential* part contains a detailed description of all of the bugs we found, the file names and line numbers where they occur, how they can be exploited, and what the consequences are. It is confidential because it contains both proprietary material and specific information about potential attacks on voting systems.

3. Background

3.1 Contents of the memory card

Both the AV–OS and AV–TSx systems use removable memory cards as key parts of their architectures. In both systems, the memory cards contain several kinds of information:

- the election description (a small database describing the races, candidates, parties, propositions, and ballot layout information for the current election);
- vote counters for every candidate and proposition on the ballot that store a count of the number of votes for that candidate (in the case of the AV–OS), or data records containing the cast ballot images (AV–TSx), along with various summary counters;
- byte-coded object programs (.abo files), which are normally created by writing scripts (programs) in the AccuBasic language and running them through the AccuBasic compiler;[1]

[1] AccuBasic object files (.abo files) are *normally* created by running AccuBasic programs through the compiler, i.e., that is the intent. But nothing prevents a programmer from directly

- the internal electronic audit log;
- an election mode field indicating whether the system containing the card is currently being used in a real election or not;
- a large number of other significant variables including strings, flags (for selecting options), various event counters, and other data describing the state of the election.

In fact, as far as we can tell, *the entire election-specific state of the voting machine* (the part that is retained *between* voting transactions) is stored on the memory card. It would take a much more comprehensive review of the software than we were able to conduct in order to verify this, but it appears to be the case.

All of this information on the memory cards is critical election information. If it is not properly managed, or if it is modified in any unauthorized way, the integrity of the entire election is possibly compromised. It is therefore vital, as everyone acknowledges, to maintain proper procedural control over the memory cards to prevent unauthorized tampering, and to treat them at all times during the election *with at least the same level of security as ballot boxes containing voted ballots.*

From one point of view, such an architecture makes good sense. In principle, it allows a memory card to be removed from a machine at almost any time (except during a short critical time window at the final completion of each vote transaction) without losing any votes or audit records, or any of the other context that has been accumulated. (Removal of a memory card during an election is procedurally forbidden under normal circumstances.) And it guarantees that when the memory card is removed at the end of the day, it contains *all* of the data needed for canvass, and for the resolution of most disputes, excepting only those that might depend on detailed forensic analysis.

Having all of the state on a removable memory card has a downside, however. It means an attacker with access to the card has potentially many other avenues of attack besides direct modification of the vote counts or the AccuBasic scripts; he can modify any other part of the election configuration or state as well. In our investigation, we did not attempt to enumerate all of these possibilities since it was clear that the only strong way to protect against all such attacks is to prevent any possibility of undetected tampering with the memory card in the first place.

When the AV–OS memory card is inserted into the AV–OS, it acts like an extension of main memory, and can be directly read and written via ordinary memory addressing, e.g., via variables and pointers. (Whether it actually is RAM, or is instead some other kind of memory-mapped storage device is not clear to us, but from a software point of view there is no difference.)

On the AV–TSx, however, the election state data is stored in a *file system* on the removable card. This means that the firmware cannot access it directly as main memory, but must use open/close/read/write calls to move data between files on the card and main memory. From a reliability and security point of view this is preferable to the architecture used on the AV–OS, since many kinds of common bugs (e.g. index or pointer bugs) can corrupt the data on a card that acts as main memory, whereas that is less likely for data packaged in a file system.

In the AV–OS, once the memory card is inserted into the voting machine, the byte-coded object programs become immediately executable by the AccuBasic interpreter in the firmware of the machine. However, on the AV–TSx the byte-coded object programs are cryptographically protected by the GEMS election management system. In effect, the GEMS server writes a sort of checksum[2] that depends on both the data and a secret cryptographic key to the memory card. When the memory card is inserted in an AV–TSx machine, the correctness of the checksum is validated and the machine refuses to enter election mode if the check fails.[3]

The cryptographic protection for the object code on the AV–TSx touchscreen machine is a significant improvement. It means that even if an attacker can get access to a memory card and modify the object code, unless he also has the cryptographic key to allow him to create a matching checksum for the modified object code, the checksum will not match when the card is inserted and the attack would be foiled. The integrity of the object code then boils down, for all practical purposes, to the secrecy of the cryptographic key (which we will discuss later).

---

writing .abo files, or modifying them, bypassing the AccuBasic language and the compiler entirely. Indeed, this is a route to several potential attacks. The AccuBasic interpreter makes no effort to verify that the AccuBasic object code has indeed been produced by the compiler.

[2] To be precise, it uses a cryptographic message authentication code (MAC).

[3] If the cryptographic message authentication code is invalid, a dialog box appears on the screen with the warning "Unable to load the election: the digital data base signature does not match the expected value," and the machine does not enter election mode.

3.2 AccuBasic

The AccuBasic programming language is a Diebold-proprietary, limited-functionality *scripting language* (a kind of programming language). The scripts (programs) written in AccuBasic are intended to be used only for creating and printing reports on the printer units attached to the AV–OS or AV–TSx.

Once a script is written in AccuBasic (the *source code* version of the script), it is run through the AccuBasic *compiler,* which translates it into a form of *object code.* The object code is represented in another Diebold-proprietary language that seems to be unnamed but is generally referred to as *byte code* or an *.abo file.* It is the object code form of the scripts that is stored on the memory card, not the source form.

Normally all .abo files are produced in this way, i.e. by running AccuBasic source through the compiler. But it is important to understand that nothing prevents a programmer from bypassing the compiler and constructing a valid .abo file directly, or by editing an .abo file produced by the compiler. (Mr. Hursti did just that, modifying the portion of the script responsible for printing the zero report.) A .abo file produced in either of these nonstandard ways might not be producible by the compiler at all from any AccuBasic source file. However, they will still be executable by the interpreter without any error, and this fact can be the basis for powerful attacks that can take advantage of bugs in the interpreter. The AccuBasic interpreter makes no attempt to validate the .abo files, i.e., to ascertain that they were in fact produced using the compiler.

The AccuBasic software for the AV–TSx is slightly different from that on the AV–OS. This is due primarily to the differences in the environment on the two systems. For example, the AV–TSx gets yes/no user input through the touchscreen, whereas the AV–OS gets it from physical buttons. Also, AV–OS memory cards contain vote counters only, whereas the AV–TSx cards store full ballot records. The memory card on the AV–OS is memory-mapped, whereas the same information is stored in a file system on the AV–TSx memory card. The AccuBasic interpreter for the AV–TSx is implemented in C++, whereas the interpreter in the AV–OS is written in C. The AV–OS interpreter contains 1,838 lines of C code (not counting blank lines, comments, or global declarations), while the AV–TSx contains 2,614 lines of C++ code (again, excluding blank lines, comments, and declarations). However, it is clear that the AccuBasic interpreter in the AV–TSx was originally just a translation from C to C++ of the one in the AV–OS, and they have subsequently diverged only slightly. The differences between the two AccuBasic interpreters are generally small enough that, except where noted, our generalizations about AccuBasic and its implementation apply equally to both versions.

AccuBasic is in one sense a general purpose language, in that it is able to do arbitrary numerical and string calculations.[4] But in another sense, *when its interpreter is properly implemented,* it is a very restricted language in that, while it can *calculate* anything, it can only control a very limited part of the functionality of the voting machine. For example, an AccuBasic script can read the vote counters (or ballot images) and the election description from the memory card, and it can read a few other internal values as well (such as the date and time); but it cannot modify any of them. And it can invoke only a few functions from the rest of the code base outside the interpreter, specifically, those needed for assembling information for, and for the printing of, reports on the machine's screen and printer. It is not possible (again, *when the AccuBasic interpreter is properly implemented*) for AccuBasic object code to:

- modify the vote counts (AV–OS) or the ballot images (AV–TSx);
- forge any votes or fail to record any votes;
- modify the election description information; or
- modify any paper ballots.

On the other hand, even when perfectly implemented, it is always possible for an erroneous or malicious AccuBasic script to:

- print false reports, or
- crash the voting machine (e.g., by going into an infinite loop).

These latter points are not flaws in the design of AccuBasic language or interpreter. Any other software, e.g., the machine's firmware, could have similar bugs. However, the fact that the scripts are on removable memory cards—and thus poten-

[4] The language uses integer and string data types, and permits assignments, sub-string extraction and assignment, conditionals, loops, a limited number of defined subroutines, subroutine calls (without arguments), and recursion. It is theoretically capable of computing any computable function.

tially exposed to tampering—makes these possibilities important. Mr. Hursti's attack on the AV–OS depended critically on his ability to modify the Zero Report script so that it falsely indicated that all counters were zero when in fact they were not. And in some jurisdictions, e.g., Florida, the reports printed by the AV–OS are the legal results of the election, so printing a false report amounts to falsifying the results of the election.

The intent of the AccuBasic language, compiler, and interpreter is that AccuBasic scripts should be usable *exclusively* for creating and printing reports on the voting machine's printer, without modifying the voting machine's behavior in any other way. With the exception of some serious bugs (described in our findings below) we found that this is indeed the case. In spite of its name, which is reminiscent of the powerful scripting language Visual Basic, we found that AccuBasic is a very limited, special purpose language; this is the right approach if one is to use an interpreted language at all.

Aside from the bugs (described below) the AccuBasic interpreters for both the AV–OS and AV–TSx are very well written and documented. We had no difficulty understanding the code and reviewing it.

4. Findings

Finding 1 *There are serious vulnerabilities in the AV–OS and AV–TSx interpreter that go beyond what was previously known. If a malicious individual gets unsupervised access to a memory card, he or she could potentially exploit these vulnerabilities to modify the electronic tallies at wild, change the running code on these systems, and compromise the integrity of the election arbitrarily. (The original paper ballots for the AV–OS, of course, cannot be affected by tampering with the memory cards.)*

The AccuBasic interpreters, in both the AV–OS and AV–TSx, have a number of serious bugs—defects in the source code—that render the machines vulnerable to various attacks. (This goes well beyond what Mr. Hursti demonstrated; his attacks did not exploit any of these vulnerabilities.) These vulnerabilities would not affect the normal behavior of the machine, and would not be discovered during testing. But they could be exploited by an attacker with unsupervised access to a memory card. Many of these vulnerabilities are present in both the AV–OS and AV–TSx; the AV–TSx code is basically a translation of the AV–OS code from C to C++, and most of the vulnerabilities were preserved in the translation.

The vulnerabilities arise because the AccuBasic interpreter "trusts" the contents of the AccuBasic object code (.abo files) stored on the memory card, and implicitly assumes that this AccuBasic object code has been produced by a legitimate Diebold AccuBasic compiler. As discussed earlier, this assumption is not necessarily justified. Anyone with unsupervised access to the AV–OS memory card could freely modify its contents, including the .abo file stored on the memory card. The same is true of the AV–TSx memory card, if the cryptographic keys are not updated from their default values (see Finding 4 below).

Types of vulnerabilities. The vulnerabilities include several instances of the classic buffer overrun vulnerability, as well as vulnerabilities with a similar effect. This kind of vulnerability would allow someone who could edit the AccuBasic object code on the memory card to completely control the behavior of the voting machine. The instant that the AccuBasic interpreter on the AV–OS or AV–TSx attempts to execute the malicious AccuBasic object code, the machine will be compromised.

Table 1 contains an overview of the 16 vulnerabilities we found in the AV–OS, and their impact. Also, Table 2 contains a similar overview of the 10 vulnerabilities we found in the AV–TSx. Note that we have excised any information that might help to exploit these vulnerabilities from those tables. We have relegated all such information to a separate Appendix, which contains additional detail: for each vulnerability, the Appendix lists the source code line number where the vulnerability appears, along with information about how the vulnerability might be exploited in the field.

These vulnerabilities were found primarily by line-by-line review of the source code, performed by three of us reading every line of the interpreter code together as a team. After we had completed a careful line-by-line security analysis, we then applied the Fortify Source Code Analyzer (SCA) tool and examined the warnings it produced. Given the care with which we performed the manual code review, we had not expected a static bug-finding tool to find any further bugs. Consistent with our expectations, the first warning we inspected from the tool referred to an exploitable security vulnerability we had already found. However, to our considerable surprise, the second warning from the tool turned out to reveal a vulnerability that we had missed as part of our manual code inspection (namely, Vulnerability V2). (The re-

mainder of warnings we examined pointed to bugs and vulnerabilities that we had already found.)

In all cases the specific bugs we found are local and easy to fix. One concern, however, is that these are just the bugs vie were able to find; there are quite possibly others we did not notice, and that automated bug-finding tools (which are always imperfect) would not notice either. Code review is difficult. It is hard to be confident that one has found all bugs (and indeed, our experience with the Fortify SCA tool highlighted this fact), and if we used another tool or if another person were to examine the code, they might find other vulnerabilities.

None of the vulnerabilities we found would have been found through standard testing, so testing is not the answer. This is a long-term problem with the use of interpreted code on removable memory cards, and with the failure to use defensive programming and other good security practices when implementing the interpreter.

These vulnerabilities have not been confirmed by verifying that they work against a full working system. (We did not have access to a running system.) We have used our best judgment to assess which bugs are likely to be exploitable, but it is possible that some bugs we classified as vulnerabilities may in fact not be exploitable. Conversely, there may be other vulnerabilities that we failed to identify because of the lack of a working system.

To double-check our analysis, we chose one vulnerability more or less at random and verified that we were able to exploit it in a simulated test environment. We were able to compile and execute a slightly modified version of the AV–OS AccuBasic interpreter, as well as the AccuBasic compiler, on a PC. We then developed an example of AccuBasic object code (an .abo file) that would exploit this vulnerability. We verified that, when using the interpreter to interpret this object code on our PC, we were able to trigger a buffer overrun and successfully exploit the vulnerability. This provides partial confirmation of our analysis, but it is certainly not an authoritative test. We did not attempt to perform an exhaustive test of all 16 vulnerabilities.

Impact. The consequence of these vulnerabilities is that any person with unsupervised access to a memory card for sufficient time to modify it, or who is in a position to switch a malicious memory card for a good one, has the opportunity to completely compromise the integrity of the electronic tallies from the machine using that card.

Many of these vulnerabilities allow the attacker to seize control of the machine. In particular, they can be used to replace some of the software and the firmware on the machine with code of the attacker's choosing. At that point, the voting system is no longer running the code from the vendor, but is instead running illegitimate code from the attacker. Once the attacker can replace the running code of the machine, the attacker has full control over all operation of the machine. Some of the consequences of this kind of compromise could include:

- The attack could manipulate the electronic tallies in any way desired. These manipulations could be performed at any point during the day. They could be performed selectively, based on knowledge about running tallies during the day. For instance, the attack code could wait until the end of the day, look at the electronic tallies accumulated so far, and choose to modify them only if they are not consistent with the attacker's desired outcome.
- The attack could print fraudulent zero reports and summary reports to prevent detection.
- The attack could modify the contents of the memory card in any way, including tampering with the electronic vote counts and electronic ballot images stored on the card.
- The attack could erase all traces of the attack to prevent anyone from detecting the attack after the fact. For instance, once the attack code has gained control, it could overwrite the malicious AccuBasic object code (.abo file) stored on the memory card with legitimate AccuBasic object code, so that no amount of subsequent forensic investigation will uncover any evidence of the compromise.
- It is even conceivable that there is a way to exploit these vulnerabilities so that changes could persist from one election to another. For instance, if the firmware or software resident on the machine can be modified or updated by running code, then the attack might be able to modify the firmware or software in a permanent way, affecting future elections as well as the current election. In other words, these vulnerabilities mean that a procedural lapse in one election could potentially affect the integrity of a subsequent election. However, we would not be able to verify or refute this possibility without experimentation with real systems.

	Type	Impact
V1	Array bounds violation	Overwrite any memory address within $\pm 2^{15}$ bytes of the global context structure with a 2-byte value that the adversary has partial control over. Might allow attacker to inject malicious code and take complete control of the machine. Might allow overwriting vote counters.
V2	Format string vulnerability	Crash the machine; read the contents of memory within a narrow range
V3	Input validation error	Choose any location on the memory card and begin executing it as .abo code; could be used to conceal malicious .abo code in unexpected locations, or to crash the machine.
V4	Array bounds violation	Memory corruption; crash the machine.
V5	Double-free() vulnerability	Overwrite any desired 4-byte memory address with any desired 4-byte value. Allows attacker to inject malicious code and take complete control of the machine.
V6	Array bounds violation	Memory corruption: overwrite any memory address up to 2^{16} bytes after the global context structure with a 2-byte value that the adversary has no control over. Might allow overwriting vote counters.
V7	Buffer overrun	Memory corruption; crash the machine
V8	Buffer overrun, integer conversion bug	Memory corruption: overwrite up to 2^{15} consecutive bytes of memory starting at global context structure. Might allow attacker to inject malicious code and take complete control of the machine. Might allow overwriting vote counters. Information disclosure: read any memory location $\pm 2^{15}$ bytes away from global context structure. Crash the machine.
V9	Buffer underrun	Memory corruption: overwrite up to 2^{15} consecutive bytes of memory extending backwards from the global context structure. Might allow attacker to inject malicious code and take complete control of the machine. Might allow overwriting vote counters. Information disclosure: read any memory location within this window. Crash the machine.
V10	Buffer overrun	Overwrite return address on the stack. Allows attacker to inject malicious code and take complete control of the machine.
V11	Array bounds violation	Information disclosure: read from potentially any memory address. Crash the machine.
V12	Array bounds violation	Write any 2-byte value to any address up to 2^{16} bytes after the global context structure. Might allow attacker to inject malicious code and take complete control of the machine. Might allow overwriting vote counters.
V13	Array bounds violation	Information disclosure: Read any 2-byte value from any address up to 2^{16} bytes after the global context structure.
V14	Pointer arithmetic error	Crash machine. Could begin interpreting random memory locations as though they were .abo code.
V15	Unchecked string operation	Machine might crash or become unresponsive
V16	Unchecked string operation	Overwrite stack memory. Might allow attacker to inject malicious code and take complete control of the machine.

Table 1: 16 security vulnerabilities we found in the AV-OS.

	Type	Impact
W1	Array bounds violation	Overwrite any memory address with a 4-byte value that the adversary has partial control over. Allows attacker to inject malicious code and take complete control of the machine.
W3	Input validation error	Choose any memory location and begin executing it as .abo code; could be used to conceal malicious .abo code in unexpected locations, or to crash the machine.
W6	Array bounds violation	Overwrite any memory location with any desired value. Allows attacker to inject malicious code and take complete control of the machine.
W7	Buffer overrun	Memory corruption; crash the machine
W8	Buffer overrun, integer conversion bug	Corrupts memory until the machine crashes.
W10	Buffer overrun	Overwrite return address on the stack. Allows attacker to inject malicious code and take complete control of the machine.
W11	Array bounds violation	Information disclosure: read from potentially any memory address. Crash the machine.
W12	Array bounds violation	Writes any 4-byte value to any address. Allows attacker to inject malicious code and take complete control of the machine.
W13	Array bounds violation	Information disclosure: read a 4-byte value from any address.
W14	Pointer arithmetic error	Crash machine. Could begin interpreting random memory locations as though they were .abo code.

Table 2: 10 security vulnerabilities we found in the AV-TSx. Note that in many cases, the same vulnerability appears in both the AV-OS and AV-TSx interpreters, so we have used parallel numbering (e.g., the bug V6 in the AV-OS interpreter also appears in a very similar form as bug W6 in the AV-TSx interpreter).

- It is conceivable that the attack might be able to propagate from machine to machine, like a computer virus. For instance, if an uninfected memory card is inserted into an infected voting machine, then the compromised voting machine could replace the AccuBasic object code on that memory card with a malicious AccuBasic script. At that point, the memory card has been infected, and if it is ever inserted into a second uninfected machine, the second machine will become infected as soon as it runs the AccuBasic script.

  It is difficult to confidently assess the magnitude of this risk without experimentation with real systems. That said, given our current understanding of how memory cards are used and our current understanding of the vulnerabilities,[5] we believe the risk of this kind of attack is low (at least in the near-term). This kind of virus would only be able to spread through "promiscuous sharing" of memory cards, which means that propagation would probably be fairly slow. If typical practice is that memory cards are wiped clean before the election, programmed, sent to the polls, and then returned for reading at the GEMS central management system, then there does not seem to be much opportunity for one infected memory card to infect many machines.
- On the AV–TSx, the attack could print fraudulent VVPAT records. Since VVPAT records are considered the authoritative record during a recount, this might enable election fraud even if the VVPAT records are manually recounted. For instance, the attack could print extra VVPAT records during a quiet time when no voter is present (however, we expect that this might be noticed by poll workers, as the TSx printer is fairly noisy). As another example, when a voter is ready to print the VVPAT record, the attack code could print two copies of the voter's VVPAT record and hope that the voter doesn't notice. The attack might print duplicate VVPAT records only for voters who have voted for one particular candidate, thereby inflating the number of VVPAT records for that favored candidate. Alternatively, it might fail to print

[5] We have assumed as part of this analysis that the GEMS central management system, and TSx machines running in accumulator mode, do not execute AccuBasic scripts as part of reading memory cards. We were not able to verify or refute this assumption; however, we have no reason to believe it is inaccurate. Of course, if this assumption is inaccurate, our analysis of the risk would be affected.

VVPAT records for voters who vote for a disfavored candidate (but of course, this could easily be detected voters who know to expect the machine to print a VVPAT record).

We believe the risk of false VVPAT records is lower than it might at first seem. See below for further discussion.

- The attack could affect the correct operation of the machine. For instance, on the AV–OS, it could turn off under- and over-vote notification. It could selectively disable over-vote notification for ballots that contain votes for a disfavored candidate, or selectively provide false over-vote notifications for ballots that contain votes for a favored candidate. On the AV–TSx, it could show the voter a wrong or incomplete list of candidates during vote selection; it could change selections between the time when they are initially selected and when they are shown on the summary screen; and it could selectively target a subset of voters, based on how they have voted or on other factors. Once the machine is running native code supplied by the attacker, its operation can be completely controlled by the attacker.

In addition, most of the bugs we found could be used to crash the machine. This might disenfranchise voters or cause long lines. These bugs could be used to selectively trigger a crash only on some machines, in some geographic areas, or based on certain conditions, such as which candidate has received more votes. For instance, it would be possible to write a malicious AccuBasic script so that, when the operator prints a summary report at the end of the day, the script examines the vote counters and either crashes or continues operating normally according to which candidate is in the lead.

Unfortunately, the ability of malicious AccuBasic scripts to crash the machine is currently embedded in the architecture of the interpreter. Any infinite loop in the AccuBasic script immediately translates into an infinite loop in the interpreter (which causes the machine to stop responding, and is indistinguishable from a crash), and any infinite recursion in the AccuBasic script translates into stack overflow in the interpreter (which could corrupt stack memory or crash the machine).

The impact on the paper ballots (AV–OS). It is important to note that even in the worst case, the paper ballots cast using an AV–OS remain trustworthy; in no case can any of these vulnerabilities be used to tamper with the paper ballots themselves.

The impact on the VVPAT records (AV–TSx). As mentioned above, on the AV–TSx it is conceivable that these vulnerabilities might enable an attacker to print false VVPAT records. We assess the magnitude of this risk here. There are two cases:

- If the bugs are not fixed, and if proper cryptographic defenses are not adopted (see Finding 3), and if a malicious individual gains unsupervised access to the memory code:

  In this case, it is hard to make any guarantees about the integrity of the VVPAT records. Attack code might be able to introduce fraudulent VVPAT records, compromising the integrity of both the electronic tallies and the paper records.

  We were unable to identify any realistic scenario where this would enable an attacker to cause fraud on a large enough scale to affect the outcome of a typical election without being detected. If the attack tries to insert many fraudulent extra VVPAT records, then the one percent recount should detect that the VVPAT records do not match the electronic tallies or that many precincts have more VVPAT records than voters who signed in (on the roster sheets), which would reveal the presence of some kind of attack and (presumably) trigger further investigation. If the attack tries to defraud many voters by failing to print a valid VVPAT record, then we suspect at least some of these voters will notice and the attack is likely to be detected. Also, mounting a large-scale attack would appear to require tampering with many memory cards or with the GEMS election management system, which restricts the class of adversaries who would have the opportunity to mount such an attack.

  Nonetheless, if such an attack is detected, it may be difficult to decide how to recover from the attack. In this scenario, both the electronic tallies and the paper records are untrustworthy, so in the worst case the only recourse may be to hold another election.

- If the bugs are fixed:

In this case, we do not see any realistic threat to the integrity of the VVPAT records.

In principle, if a malicious individual is able to introduce a malicious AccuBasic script, one might imagine a possible attack vector where the AccuBasic code prints false VVPAT records. However, in practice we do not see any viable threat here. AccuBasic scripts do have the capability to print to the AV–TSx printer, and this printer is shared for both printing reports (e.g., the zero tape, the summary report) during poll opening/closing, and for printing VVPAT records during the election. In theory, one might be able to envision a malicious AccuBasic script that, after it finishes printing the zero tape, continues running, waits some period of time, and then prints some text designed to look like a VVPAT record in hopes that this will be spooled into the security canister along with other VVPAT records. In practice, we believe that poll workers are unlikely to be fooled by this. As far as we can tell, the AV–TSx is single-threaded, so if the AccuBasic script does not relinquish control, the TSx will not show a startup screen welcoming voters to begin voting. It does not seem particularly likely that a poll worker would print and tear off a zero tape, feed the paper into the security canister, walk away before the machine has displayed a welcome screen, and fail to notice the machine printing and scrolling the tape into the security canister when there is no voter present. It is hard to imagine how this could be used for any kind of large-scale attack without being detected in at least some fraction of the polling places where the attack occurs.

Therefore, we consider this risk to be minimal, if the bugs in the AV–TSx AccuBasic interpreter are fixed.

Finding 2 *Everything we saw in the source code is consistent with Harri Hursti's attack on the AV–OS.*

Our analysis of the source code is consistent with Harri Hursti's findings that (a) the AccuBasic script on the AV–OS memory card can be replaced with a malicious script, (b) the vote counters on the AV–OS memory card can be tampered with and set to non-zero values, and (c) it is possible to use a malicious AccuBasic script to conceal this tampering by printing fraudulent zero reports or summary reports. Our source analysis confirmed that a malicious AccuBasic script is able to print to the printer (on both the AV–OS and the AV–TSx), display messages on the LCD display (on the AV–OS), and prompt for user responses (on the AV–OS). Our analysis also confirmed that the AV–OS fails to check that the vote counters are zero at the start of election day. We also confirmed that the AV–OS source code has numerous places where it manipulates vote counters as 16-bit values without first checking them for overflow, so that if more than 65,535 votes are cast, then the vote counters will wrap around and start counting up from 0 again. (It is a feature of 16-bit unsigned computer arithmetic that large positive numbers just less than 65,536 are effectively the same as small negative numbers).[6] There is little doubt in our minds that Hursti's findings about the AV–OS are accurate. Even if the bugs we found in the AccuBasic interpreter are fixed, Hursti's attacks will remain possible.

The AV–TSx also appears to be at risk for similar attacks. The AV–TSx memory card also contains an AccuBasic script and appears to be vulnerable to similar kinds of tampering, unless the cryptographic keys have been updated from their default values (see below for a discussion).

Finding 3 *The AV–TSx (but not the AV–OS) contains cryptography designed to protect the contents of the AV–TSx memory card from modification while it is in transit. This mechanism appears to be an acceptable way to protect AccuBasic scripts from tampering while the memory card is in transit, assuming election officials update the cryptographic keys on every AV–TSx machine.*

The AV–TSx uses a cryptographic message authentication code (MAC), which ensures that it is infeasible for anyone who does not know the secret cryptographic key to tamper with the data stored on the memory card. The use of the cryp-

[6] We discovered that the code does contain a check to ensure that it will not accept more than 65,535 ballots. On the surface, that might appear adequate to rule out the possibility of arithmetic overflow. However, as Hursti's attack demonstrates, the existing check is not, in fact, adequate: if the vote counter started out at some non-zero value, then it is possible for the counter to wrap around after counting only a few ballots. This is a good example of the need for defensive programming. If code had been written to check for wrap-around immediately before every arithmetic operation on any vote counter, Hursti's technique of loading the vote counter with a large number just less than 65,536 would not have worked.

tographic MAC in the AV–TSx appears to be an acceptable way to protect AccuBasic object code (.abo files) from tampering while the memory card is in transit, provided that election officials update the cryptographic keys on every AV–TSx. On the other hand, if the cryptographic keys are not updated, then the cryptographic mechanism does not protect against tampering with the contents of the memory card, for the following reasons.

The AV–TSx contains a default set of cryptographic keys. There is a procedure that election officials can use to change the keys stored on any particular AV–TSx machine. However, if this procedure is not performed on an AV–TSx machine, then that AV–TSx continues to use its default keys.

The default keys provide no security. They appear to be the same for all TSx machines in the Nation, and in fact were discovered and published two and a half years ago (see Finding 4 below). Unfortunately, if no special steps are taken, the AV–TSx silently uses these insecure keys, without providing any warning of the dangers. Therefore, election officials will need to choose a new key for the county and update the keys on every AV–TSx machine themselves. Fortunately, there is a process for updating the keys on the AV–TSx by inserting a special smartcard into the AV–TSx machine.

So long as this process is followed, the cryptographic message authentication code (MAC) should provide acceptable security against tampering.[7] Because the AccuBasic script (.abo file) is stored on the memory card, the cryptography protects the AccuBasic script from being modified. If the cryptographic keys have been set properly, this defends against attacks like Harri Hursti's against the TSx: it prevents a malicious individual from *successfully* tampering with the AccuBasic script or the ballots stored on the memory card, even if the individual has somehow gained unsupervised access to the memory card, because the cryptographic check built in to the TSx firmware will fail and the TSx will print a warning message and refuse to proceed further.

The cryptographic MAC on the TSx appears to cover almost everything stored on the memory card data file. It covers election parameters, vote counters, the AccuBasic script (.abo file), and some other configuration data. The only exceptions we are aware of is that the file version number and the election serial number do not appear to be covered by the cryptographic MAC or by any checksum. These exceptions seem to be harmless.

In effect, the cryptography acts as the electronic equivalent of a tamper-resistant seal. If the contents of the memory card is tampered with, the cryptography will reveal this fact.

We stress that, like a tamper-resistant seal, the cryptography *only* defends against tampering while the memory card is in transit. The cryptography does *not* protect against tampering with AccuBasic scripts while they are stored on the GEMS server. In the Diebold system, the cryptographic protection is applied by the GEMS server when the memory card is initialized. The GEMS server stores the cryptographic keys and uses them to compute the cryptographic MAC when initializing a memory card; later, the AV–TSx uses its own copy of the keys to check the validity of the MAC. Of course, anyone who knows the cryptographic key can change the contents of the card and re-compute the MAC appropriately. This means that anyone with access to the GEMS server will have all the information needed to make undetected changes to AV–TSx memory cards. Also, AccuBasic scripts (.abo files) are stored on the GEMS server and downloaded onto memory cards as needed. If the copy of the .abo files stored on the GEMS server were corrupted or replaced, then this could affect every AV–OS machine and every AV–TSx machine in the county. In other words, if the operator of the GEMS server is malicious, or if any untrusted individual gains access to the GEMS server, all of the machines in the county could be compromised. The AV–TSx cryptography provides no defense against this threat; instead, it must be prevented by carefully guarding access to the GEMS server.

The cryptographic algorithm used in the AV–TSx, while perhaps not ideal, appears to be adequate for its purpose. The AV–TSx uses the following MAC algorithm:

$$F_k(x) = \mathrm{AES}_k(\mathrm{MD5}(x)),$$

where $\mathrm{AES}_k(.)$ denotes AES–ECB encryption of a 128-bit value under key k. This choice of MAC algorithm is probably not what any cryptographer would select today, but it appears to be adequate. In August 2004, cryptographers discovered a way to

[7] We assume that the cryptographic keys are not stored on the memory card, but are stored on non-removable storage. We were not able to verify this assumption from the source code alone, but we have no reason to believe otherwise.

find collisions in MD5, which prompted many cryptographers to suggest using some other hash algorithm in new systems. Fortunately, these collision attacks do not appear to endanger the way that AV–TSx uses its MAC, because chosen-plaintext attacks do not appear to pose a realistic threat. In contrast, the discovery of second pre-image attacks on MD5 would probably suffice to break the AV–TSx MAC algorithm, but fortunately no practical second pre-image attacks on MD5 are known. Consequently, given our current knowledge, the AV–TSx MAC appears to be acceptable.

In the long run, it would probably make sense to migrate to a more robust MAC algorithm (e.g., AES–CMAC). Even better, a cryptographic public-key signature (e.g., RSA, DSA) would appear to be ideal for this task. With the current scheme, anyone who can gain access to and reverse-engineer an AV–TSx machine can recover the cryptographic key and attack the other memory cards in the same county; while a public-key signature would eliminate this risk. Nonetheless, for present purposes the current scheme appears to be strong enough that it is not the weakest point in the system.

Finding 4 *The AV–TSx contains default cryptographic keys that are hard-coded into the source code and that are the same for every AV–TSx machine in the Nation. One of these keys was disclosed publicly in July, 2003, yet it remains present in the source code to this day.*

We mentioned above that the AV–TSx contains a set of default keys that are used if the cryptographic keys have not been explicitly updated. We found that these default keys are hard-coded in the source code and are the same for every AV–TSx machine in the Nation.

The presence of hard-coded keys in the TS was first disclosed in a famous scientific paper by Kohno, Stubblefield, Rubin, and Wallach in July, 2003. Their paper also revealed the value of the key—namely, F2654hD4—to the public. Subsequent reports from Doug Jones revealed that this design defect dates back to November, 1997, when he discovered the same hard-coded key and reported its presence to the vendor. These authors pointed out that use of a hard-coded key that is the same for all machines is very poor practice and opens up serious risks. It would be like a bank using the same PIN code for every ATM card they issued; if this PIN code ever became known, the exposure could be tremendous. It had been our understanding that all of the vulnerabilities found in those investigations two years ago had been addressed. It is hard to imagine any justification for continuing to use this key after it had been compromised and revealed to the public. This is a serious lapse that we find hard to understand considering how widely publicized this vulnerability was.

This also illustrates the reason that cryptographers uniformly recommend against hard-coded keys. If those keys are ever compromised or leaked, the compromise can affect every machine ever manufactured, and it can be difficult to change the key on every affected machine.

The AV–TSx would be more secure if it were changed to avoid use of default keys, i.e., if election officials were *required* to generate and load a county-specific cryptographic key onto the AV–TSx before its first use, and if the AV–TSx were to refuse to enter election mode if no key has ever been loaded.

Finding 5 *The AV–OS stores the four-digit supervisor PIN on the memory card. The PIN is stored in an obfuscated format, but this obfuscation offers limited protection due to its reliance on hard-coded magic constants in the source code.*

On the AV–OS, the four-digit PIN is derived as a specific function of a field stored on the memory card and of some constant values that are hard-coded into the source code. These magic constants are the same for every AV–OS machine across the Nation, which is the rough equivalent of the hard-coded keys found in the AV–TSx. Thus, the AV–OS contains a design defect that is roughly similar to one in the AV–TSx.

Anyone with access to the AV–OS source code can learn these magic constants. Likewise, anyone who has unsupervised access to an AV–OS machine and the ability to perform reverse engineering could learn these magic constants. Once the magic constants are known, anyone who gains access to a memory card can read its contents and predict its four-digit PIN. Likewise, if they had unsupervised access to the memory card, they could set the four-digit PIN to any desired value by setting the field stored on the memory card appropriately. The use of the same magic constant values for every AV–OS machine in existence poses the risk that, if these constant values are ever disclosed, the security of the PIN protection would be undermined.

At present, we believe the security risks of this design mis-feature are probably minor and limited in extent, because even knowledge of the PIN only provides a limited degree of additional access. There are worse things that an individual could do if she gained unsupervised access to an AV–OS memory card. Nonetheless, we caution election administrators not to place too much reliance on the four-digit PIN on the AV–OS.

Finding 6 *The AccuBasic interpreter was fairly cleanly structured and was organized in a way that made the source code very easy to read.*

The source code for the AccuBasic interpreter was written in a way that made it easy for us to understand its intent and operation and analyze its security properties. The code was split into many small functions whose purpose was clear and that performed one simple operation. There were comments explaining the purpose of each function and explaining tricky parts of the code. The clarity of the interpreter source code was about as good as any commercial code we have ever reviewed.

The interpreter is structured as a recursive descent parser, so that the program's call stack mirrors the stack of the associated context-free automaton. In addition, there is a global variable holding the global interpreter context: e.g., AccuBasic registers, AccuBasic variables, and various loop indexes. This was a reasonably elegant way to structure the implementation.

There were some ways that the implementation could have been improved. The code didn't use defensive programming, which would have helped tremendously to harden it against many malicious attacks. Also, the source code didn't document the relevant program invariants and pre-/post-conditions. We were forced to work these out by hand (e.g., that certain parameters were never NULL, that the global string register would never contain a string more than 255 bytes long, and so on), and it would have helped if these had been documented in the source code. Nonetheless, on the whole the interpreter source code was structured in a way that simplified the source code review task.

Finding 7 *The AccuBasic language is not a general-purpose system; it is narrowly tailored for its purpose.*

The AccuBasic language is *not* a full, general-purpose scripting language in the same category as, say, Visual Basic, in spite of the similarity of names. Instead, it is very modest in scope, with strongly circumscribed capabilities. If you are going to use an interpreted language at all in a context where security is important, this is the right way to do: one should include only the absolute minimum functionality in the language necessary to do the job it is designed for, and AccuBasic seems to meet that goal. In particular, we note that:

- AccuBasic is computationally complete in the sense that it can *compute* anything, but its interactions with the rest of the code base are very limited. The parts of the firmware and operating system that it can invoke makes it basically useful *only* for printing reports, which is the intent.
- The AccuBasic interpreter cannot invoke most of the functions available in the firmware. It cannot read or write memory outside the its own stack. It can only invoke a handful of benign services necessary for its report-writing function, e.g., reading (but not writing) the vote totals or ballot file, accepting yes/no input from the user, writing to the printer, LCD screen, or touchscreen, appending an event to the audit log file, and reading the date and time.
- In particular, the AccuBasic interpreter has only read-only access to the vote counters or ballot file, so that AccuBasic scripts can construct reports from them, but cannot modify them.

In the short, the design of the AccuBasic language appears to us to be appropriate for its purpose.

Finding 8 *The AccuBasic interpreter cannot be invoked while the AV–OS or AV–TSx are executing the core election functionality, i.e., while they are accepting votes during the middle of election day.*

The AV–OS. We determined the AV–OS does not invoke the interpreter during the tallying of live election ballots. The AV–OS invokes the interpreter during pre-election procedures, such as printing test ballot zero reports and tallies, printing election zero reports, and printing labels for duplicate memory cards and audit reports. The AV–OS also invokes the interpreter to print post-election reports after the "ender" card is read.

The AV–TSx. We determined the AV–TSx does not invoke the interpreter while it is in "election" mode. The AV–TSx can invoke the interpreter under five circumstances:

1. Printing a zero report on machine initialization.
2. The "Print Election Results" button on the pre-election menu page for printing pre-election test results.
3. Printing election totals after a poll worker presses the "End Voting" button on the election menu page.
4. The "Print Election Results" button on the post-election menu page.
5. The "Print Results" button on the accumulator menu page.

None of these can occur during the middle of the day while the TSx is in the process of interacting with voters and accepting votes.

These observations are also positive design points. The interpreter is not only very limited in its functionality, but it is very limited in the window of time during an election that it runs, which is what one wants when security is important.

Finding 9 *The AccuBasic interpreter does not appear to have been written using high-assurance software development methodologies.*

The AccuBasic interpreter appeared to be written using commercial standards of software development. This means it is not high-assurance software, nor was it developed following high-assurance methodologies.

High-assurance methods are often used for software systems where security is of utmost importance, most notably for military applications (e.g., software used to process classified documents). At a high level, these methods are similar to those used to build safety-critical software systems, where failure of the software can lead to loss of life (e.g., software found in avionics control systems, nuclear reactors, manned space flight, train control systems, automotive braking systems, and other similar settings).

In high assurance software development, one first determines explicitly what requirements the software and/or system must meet. One then designs the system, demonstrating throughout that the design meets the requirements. The method used to demonstrate this depends upon the degree of assurance desired. One then implements the system, and again justifies that the implementation meets the design. Indeed, one should be able to point to each requirement and show exactly what code is present as a result of that requirement. Finally, the operating instructions and procedures for the system and software must also meet the requirements.

We saw no evidence that the AccuBasic interpreter was developed in this way. Indeed, the problems we found argue against it. We should note that we did not see *anything* beyond the code—no requirements documents, architecture documents, design documents, threat model documentation, or security analysis documents-all of which would be present were high assurance development techniques used.

Informal name	Code identifier	Summary
"uninitialized"	STAT_UNUSED	/* Empty formatted memory card. */
"downloaded"	STAT_DOWNLOADED	/* Downloaded memory card - pre-election mode. */
"election mode"	STAT_ELECTION	/* Election counting mode. */
(none)	STAT_ELECTION_DONE	/* Ender card fed, printing totals report. */
(none)	STAT_DONE	/* Post-election mode - ready for upload. */
(none)	STAT_UPLOADED	/* Upload done, ready for audit. */
(none)	STAT_AUDIT_DONE	/* Final audit report printed. */

Figure 1: The modes that the AV-OS memory card can be in. For each mode, we list the informal name we use in this report, the symbolic name found in the source code, and a brief description taken from comments in the source code.

We also expect that if one were going to use high-assurance programming practices anywhere in a voting system, the interpreter would be one of the most likely places to use it. If high-assurance practices had been used during the design and implementation of the AV–OS and AV–TSx, the vulnerabilities we found would likely have been avoided.

Finding 10 *The AV–OS is at risk from Harri Hursti's attacks no matter what state the memory cards are in when they are transported to the polls. Even if the memory*

cards are not put into election mode until the polls are opened, Hursti's attack is still possible.

The AV–OS can be in one of several modes (e.g., pre-election, election mode, post-election). This is determined by a value stored on the memory card. It has been suggested that, if election workers were to wait to put the card into election mode until polls are opened, this might provide some level of defense against Hursti's attack. We find that this scheme does not, in fact, provide any useful protection.

Because the mode is stored on the memory card, whether or not the memory card is in election mode while in transit makes essentially no security difference. An attacker who can modify the object code and vote counts on the memory card (as Mr. Hursti did) could just as easily modify the election mode indicator too. In addition, all of the vulnerabilities described earlier (due to bugs in the code) are still exploitable, no matter what mode the memory card is in.

A detailed technical analysis of the election mode issue can be found in Section 4.1.

4.1 Technical details: Election mode and the AV–OS

In the AV–OS, memory cards can be in one of seven modes, indicated by a field stored on the memory card (namely, mCardHeader.electionStatus in the source code). The states are documented in Figure 1. The mode of the memory card at the time when the machine is booted determines what functions the AV–OS will execute. The AV–OS also updates the mode of the card in response to operator input.

The memory card also contains many counters, including candidate counters (which contain, for each candidate, the number of votes cast for that candidate), race counters (which contain, for each race, the number of votes cast in that race), and card counters (which contain the total number of "cards cast" or, in other words, the number of ballots scanned). In each case, there are three values stored: the number of absentee votes, the number of election-day votes, and the total number of votes (which should be the sum of the previous two values). This reflects the fact that the machine can be set into a mode to count absentee votes or to count at the polling place. Note that there is some redundancy among these counter values: for instance, under normal operation, if Smith and Jones are the only two candidates in one race, then the race counter should equal the sum of Smith's candidate counter and Jones' candidate counter.

In Harri Hursti's demonstration, apparently the memory card was already placed into "election mode" before Hursti was given the card. It has been suggested that if the card had been in one of the two pre-election modes ("initialized" or "downloaded") when it was given to Hursti, then the Hursti attack would not work, because the process of placing the card into "election mode" would cause the vote counters to be zeroed.

Recall that Hursti's attack, in its most dangerous form, involved two components: (a) modifying the vote counters on the memory card to pre-load it with some non-zero number of votes for each of the candidates (e.g., +7 votes for Smith and -7 votes for Jones); (b) replacing the AccuBasic script with a malicious script that falsely printed a zero report showing zeros, even though the vote counters were in fact not zero. The ability to print a false zero report enabled Hursti to conceal the fact that he had stuffed the digital ballot box. This attack was demonstrated in a scenario where the card was set into "election mode" in the warehouse, before there was an opportunity to tamper with its contents. Might it perhaps be possible to defeat this attack if memory cards were left in pre-election mode at the warehouse, transported in this mode, and then poll workers were asked to set the card to "election mode" at the opening of polls? The idea is that, in the process of setting the card into "election mode," the AV–OS will zero out the vote counters on the card, thereby undoing any pre-loading of the memory card with fraudulent votes that might have occurred before that point. We were asked to characterize the behavior of election mode and investigate whether defenses of this form would provide any value in defending against Hursti's ballot stuffing attack.

Boot behavior. When starting the AV–OS machine, the operator has the option of holding the YES button or the YES and NO buttons (simultaneously) to execute special diagnostic, supervisory, and setup functions. When the machine boots, it will enter one of several modes, depending on how it is started up:

- If the operator holds the YES and NO buttons down while machine is booting, the machine enters diagnostics mode. In diagnostics mode, the operator can set the clock, dump the memory card image via a serial port, and test various physical components of the voting machine.

- If the operator holds only the YES button and the card is initialized (i.e., in any state other than "initialized," or in other words, mCardHeader.electionStatus ≠ STAT_UNUSED)), then it gives the operator the option to enter supervisor mode. To enter supervisor mode, the operator must enter the four digit PIN. In supervisor mode, the operator can modify the setup parameters, duplicate or clear the memory card, re-enter election mode after an "ender" card has been read, and reset the card to pre-election mode. In setup mode, the operator can change the phone number and configure the auto-feeder and other physical devices.
- If the card is "uninitialized" (mCardHeader.electionStatus = STAT_UNUSED), the machine enters the aforementioned setup mode. Curiously, in this case the operator can enter setup mode without entering a PIN. This means that it would be possible in this case to change the phone number it dials to transmit election results, without entering a PIN. (We are not aware of any California jurisdiction that uses the AV–OS's modem capabilities, so this is of little practical relevance in California.)

After these functions complete or if the operator chose not enter them, the machine displays

SYSTEM TEST
*** PASSED ***

and enters the main control loop. The main control loop works as follows:

- If the card state is "initialized" (STAT_UNUSED) or "downloaded" (STAT_DOWNLOADED), the machine executes pre-election functionality. Then, the machine goes back to the beginning of the loop.
- If the card state is in "election mode" (STAT_ELECTION), the machine executes the election functionality and begins accepting and counting ballots. Then, the machine goes back to the beginning of the loop.
- If the card state is in any of the four post-election states (STAT_ELECTION_DONE, STAT_DONE, STAT_UPLOADED, or STAT_AUDIT_DONE), it executes the post-election functionality. Then, the machine goes back to the beginning of the loop.

The behavior of the AV–OS. We focus on three modes, "uninitialized," "downloaded," and "election mode," and describe how the AV–OS behaves when loaded with a card in one of those three states.

If the card is "uninitialized," the AV–OS enters a mode of operation for downloading data to the memory card. If the download is successful, the operator can print an optional zero report using the AccuBasic interpreter and then the card is set to "downloaded" mode. At this point, or if a card in "downloaded" state is inserted into the AV–OS at any time, the AV–OS provides the operator with the option of performing pre-election testing. Pre-election testing includes reading blank and full marked ballots, counting test ballots, moving the ballot deflector, testing upload of results, and printing test total and audit reports.

After testing, the machine prompts the operator if he or she wants to enter election mode. If the operator answers yes, then the card is set to "election mode" (i.e., the field mCardHeader.electionStatus on the card is set to the value STAT_ELECTION) and the AV–OS proceeds to clear the election counters. The step of entering election mode zeroes out the card counters, race counters, and candidate counters. In other words, it clears the number of votes registered for each candidate, the number of votes registered in each race, and the total number of "cards cast" (i.e., the number of ballots scanned).

After the counters are zeroed, the AV–OS machine begins executing election functionality. This code first checks the card for errors. Then, it checks if any ballots have yet been counted by checking a counter stored on the memory card containing the total number of ballots that have been counted (mCardHeader.numBalCounted[CTR_TOTAL]). If no ballots have been counted, the AV–OS invokes the AccuBasic interpreter to print a zero report (without first prompting the operator) and then begins to accept and count ballots. If this counter is non-zero, then it skips the zero report step and immediately begins to accept and count ballots.

The proposed defense. The Hursti attack works by maliciously pre-loading some of the vote counters with fraudulent non-zero values. It was suggested to us that having poll workers putting the card into election mode at the polling place would defeat this attack, but it wasn't clear whether this would involve delivering memory cards in the "uninitialized" or "downloaded" state.

We believe that transporting memory cards to the polling place in the "uninitialized" state doesn't make much sense. This would mean that the cards have not been programmed and initialized yet. It seems unlikely poll workers would be expected to program and initialize the memory cards.

Therefore, we assume that this procedural defense would involve initializing memory cards at the county headquarters, so that when they arrive at the polling place they are in the "downloaded" state. This means that the memory cards will have been programmed and initialized and are ready to be put into election mode when the AV–OS machine is turned on. After the machine starts and completes the optional diagnostics mode (see above), it will prompt the operator (in order) to:

1. To count test ballots (optional);
2. To move the ballot deflector (optional);
3. To test the upload option (optional);
4. To print a totals report (optional);
5. To print an audit report (optional);
6. To prepare for the election (optional);
7. To enter supervisor mode (optional).

To enter election mode, the operator should answer yes to the 6th prompt. At that time, the AV–OS machine will clear the counters (see above) and start counting ballots.

Analysis. Unfortunately, the proposed defense against Hursti's attack is not effective. An adversary with access to the memory card could maliciously set the card into election mode, by setting the mCardHeader.electionStatus field on the card to the value STAT_ELECTION using a hex editor or by other means. When this card is inserted into the AV–OS, the AV–OS will not clear the counters, because the card is already in election mode. (The counters are only cleared when a card in the "downloaded" state is inserted into the AV–OS and explicitly put into election mode by the operator.)

On first consideration, one might expect that this attack could be detected. After all, an observant operator might notice that he or she did not have to navigate the prompts to explicitly put the machine into election mode, and thereby may be able to deduce that the card must have already been in election mode. Unfortunately, we cannot count on this defense, because things are more complex than they may initially appear.

Recall that if the memory card is in election mode and if the counter for the total number of ballots scanned (mCardHeader.numBalCounted [CTR_TOTAL]) is zero, then the AV–OS will execute an AccuBasic script to print a zero report before accepting ballots. The operator is not prompted before the AccuBasic script begins running. Of course, if we assume that an adversary has unsupervised access to the memory card while it is in transport, the adversary could have replaced the AccuBasic script on the memory card with a malicious script, and this malicious script will start running as soon as the machine is turned on. Moreover, recall that AccuBasic scripts have the power to issue prompts to the LCD display on the AV–OS. This means that an adversary could write a malicious script which simulates the prompts the operator is expecting to see, to provide the illusion that the card is not already in election mode. When the operator answers yes to the 6th prompt, the AccuBasic script can print a zero report and exit, and the machine will start counting ballots.

In this scenario, as far as the operator can see, the machine will behave exactly as it would if the card had started in "downloaded" mode and if the operator had put it into election mode, clearing the counters. Nonetheless, in reality nothing could be farther from the truth. In this scenario, the card has been tampered with to pre-load it with votes, to set it into election mode so that these vote counters won't be cleared, and the AccuBasic script on the card has been tampered with so that the operator won't notice anything unusual and the zero report will not show these pre-loaded votes.

This shows that it is possible for an adversary to tamper with the memory card in a way that cannot be detected by the operator and that bypasses the clearing of the vote counters. In other words, even if memory cards are not put into election mode until the opening of polls, the election will still be vulnerable to a variation on Harri Hursti's attack. Therefore, it is our conclusion that procedures based on putting the AV–OS into election mode at the start of the day cannot be counted upon to protect the AV–OS machine against the vulnerabilities Harri Hursti found.

4.2 Checksums

We were asked to investigate what checksums exist in the AV–OS and AV–TSx, what types they are, and what they cover. We discuss these issues next.

Background. A checksum detects *accidental* changes to data. It reduces a large amount of data down to a fixed size value. This provides a level of redundancy: if the data is changed, then the checksum almost always changes as well. Hence, the checksum may provide a way to detect the change to the data.

Note that checksums are used to detect accidental changes to data values, but they are not at all useful in detecting malicious change. An example of an accidental change is a faulty memory cell on the memory card. If it cannot properly store the value it is supposed to, the computed checksum of the data will not equal the stored checksum, and a problem will be detected. On the other hand, if an adversary changes the data as well as all copies of the checksum value, it will be impossible to notice that the data was modified.

The AV–OS uses 16-bit checksums: a checksum can take on one of 65,536 different values. The AV–OS computes numerous checksums over the data structures stored on the memory card. These checksum values are stored on the card and are also available to AccuBasic scripts to be printed in reports. A properly implemented checksum would likely detect any accidental corruption of the election setup parameters. Alternatively, a checksum printed over a memory card's vote totals at the close of polls could be compared with the same value at the county election offices to detect changes to the vote totals.

What is covered by the AV–OS checksums. The AV–OS memory card contains quite a few checksums. We list them, and what they cover, below:

1. *Election checksum:* covers the password, and flags controlling machine.
2. *Precinct checksum:* covers a few fields describing the precinct: its number, check digit, number of voters, sequence number, and precinct ID string.
3. *Precinct-card checksum:* covers fields that tie the precinct to the card structures.
4. *Race checksum:* all fields governing the race.
5. *Race counters checksum:* covers the total number of votes for each race, write ins, over-votes, under-votes, and blank votes.
6. *Candidate checksum:* covers the candidate number and party number.
7. *Candidate counters checksum:* covers all fields in the candidate structure.
8. *Card checksum:* covers all fields in the card.
9. *Card counters checksum:* covers the precinct number, card number, number of over-votes, under-votes, and blank votes for each card-counter.
10. *Voting positions checksum:* covers all fields governing where the candidate structure is.
11. *Text checksum:* covers all text fields (election title, vote center, vote date, straight party options, address, district name, race titles, and candidate names).
12. *Audit log checksum:* not used.

In summary, only some of the election setup parameters are covered by the AV–OS checksum. For example, the voting type field in the precinct (which governs whether it is early, absentee, or precinct voting) is not covered by any checksum. Additionally, the audit log is not covered by any checksum. It is difficult to determine how modifications to the fields not covered by the checksums could cause adverse effects, though it is a source of minor concern. Ideally, these checksums would cover all of the election parameters.

The AV–OS checksum algorithms. There are many ways to generate a checksum. The AV–OS code uses two separate techniques to compute a checksum. In the first, the checksum value is simply the arithmetic sum of the data being computed. As an example, if the vote counts were as follows:

Smith:	100
Jones:	32
Roberts:	7

then the checksum would be 139. If the value for any counter changes without the corresponding checksum value changing, it would be easy to notice the discrepancy and investigate what happened. However, using addition as a checksum, while simple to compute, fails to catch many classes of errors. For example, if the vote totals

for Smith and Jones were switched, the checksum would still be 139. There are other classes of changes for which addition is not ideal and will not detect changes.

The AV–OS computes checksums over textual data in a slightly different, but related, manner. The checksum depends on the value of each of the names as well as their position (first, second, or so on).

The AV–OS checksum does not detect malicious attacks. An adversary with the ability to read and write to the memory card can always engineer the checksum to match what the malicious data they place. However, relying on the checksum to guarantee that data didn't change due to a malicious individual is not possible.

Using the addition operator (+) as a checksum may catch certain classes of non-malicious changes. However, an attacker can easily produce two different memory cards which have the same checksums. This means the checksum should not be used to determine malicious tampering. The textual checksum is also vulnerable to similar attacks.

If there was a desire to use checksums to detect malicious tampering with the contents of memory cards, a different checksum algorithm would be needed. One possibility would be to compute and print a cryptographic hash of the contents of the entire memory card at the beginning and end of the day, so that election officials can verify that the contents of the memory card had not been changed during transport. A cryptographic hash function is related to a checksum but instead of 65,536 outputs, has over 2^{160} possible values; furthermore, it is specially designed to protect against reordering and malicious tampering. Examples of cryptographic hash functions include SHA–1 or SHA–256. If this route were taken, the cryptographic hash function should be applied to the entire contents of the memory card, including all election parameters and the audit log. Another possibility would be to use cryptographic digital signatures, either a public-key signature as discussed later, or a symmetric-key MAC like the one used by the TSx (see below).

The TSx "checksum." The AccuVote TSx operates differently. It reads the election parameters from a file on the memory card. There is a symmetric-key message authentication code (MAC) that protects the data from tampering. This computation depends on a secret key, and the MAC is designed so that anyone who does not know the key will not be able to tamper with the data without being detected. Thus, as long as the key is secret and unpredictable, it will detect malicious third party tampering, as well as problems with the storage media. A cryptographic MAC has all the advantages of a conventional checksum, in that it can detect accidental changes or corruption of the data, plus it can also detect malicious tampering as well. Thus, a cryptographic MAC is much better than a checksum in every way, and we expect the TSx to be extremely effective at detecting accidental data corruption.

See Finding 3 for a discussion of what data is protected by the cryptographic MAC on the TSx.

Since the TSx systems can read the AV–OS memory cards, they also include compatibility support for the data on those cards. Of course, those cards are only protected by the AV–OS checksums discussed earlier and are thus subject to the same caveats regarding tampering.

5. Mitigating the Risks

We next discuss several possible steps that could be taken to mitigate or ameliorate the risks discussed in this report. We start by discussing the full set of mitigations that might be possible in the long run; then, we discuss some short-term mitigation options.

5.1 Long-term Mitigation Strategies

Mitigation 1 *Adopt procedures that eliminate the possibility of a single person tampering with the memory card at any time during the lifetime of a memory card.*

One approach to mitigating the risk of tampering with the memory cards is to adopt various standard handling procedures that prevent someone from tampering without the risk of detection. These procedural controls would need be maintained throughout the lifetime of the memory card. They would affect procedures for writing memory cards at county offices, for opening and closing the polls, and for transport and storage of memory cards. Training of precinct judges and precinct clerks would need to be augmented to stress the critical nature of these procedural controls. Among the possibilities are these:

- Adopt the principle that no one should ever alone with memory cards, i.e., there should always be two or more persons present (or none). This parallels the common requirement that no one should be alone with ballots (blank or voted).

- Use numbered, tamper-evident seals to protect memory cards when they are stored or when they are inserted in a voting machine. Keep records, and train poll workers to monitor those seals and their numbers and report anomalies. No one person should be entrusted with that task; all poll workers should sign off that the seals were intact.
- Permanently affix serial numbers to the memory cards and adopt written chain-of-custody procedures for transfer of custody from one pair of people to another, including poll workers.
- Train all personnel, including poll workers, that memory cards are ballot boxes and must be treated with the same degree of care and security.
- Whenever the procedures outlined are breached for some reason, take the memory card(s) in question out of service and zero them (in the presence of at least two people) before using them again.

It would help if memory cards were sealed inside the AV–OS at county headquarters, and AV–OS machines delivered to the polling place with the card already inserted and protected by tamper-evident seals. At the close of polls, it would help if poll workers did not break the seal, but rather returned the entire unit (with memory card still sealed inside) to county headquarters. This would reduce the opportunity for poll workers to tamper with memory cards.

When the AV–OS is used as a central-count machine (e.g., to count absentee votes), similar processes could be used to ensure that officials never insert a memory card into the AV–OS unless they are sure no one has had unsupervised access to the memory card. Because central-count machines reside in a controlled environment with physical security protections, and only a limited number of individuals have access to them, it should be much easier to apply very strong procedural controls to these machines.

Mitigation 2 *Revise the source code of the AccuBasic interpreter to fix these vulnerabilities, introduce the use of defensive programming practices, and use security practices that will eliminate the possibility of any other vulnerabilities of the sort we discovered here.*

We can break this mitigation down into several (closely related) steps:

- Fix the AV–OS AccuBasic interpreter to eliminate the bugs we found. Every one of the bugs we found should be fixed. Any other bugs of the same sort should also be fixed.

  It is not enough merely to introduce narrow changes to patch the specific bugs we found. Those bugs were symptoms of more fundamental flaws in the programming practices used to build the interpreter. The only way to be sure that all the bugs have been eliminated is to fix the root cause. We explain next what would be involved in doing so.
- Revise the interpreter source code, line by line, to eliminate all trust in the contents of the memory card. One of the reasons that these vulnerabilities existed was because the programmer implicitly assumed that the memory card would not be tampered with, and that the AccuBasic object code (.abo file) on the memory card was produced by a legitimate AccuBasic compiler. The source code should be changed to eliminate all instances of this kind of trust. For instance, when reading an integer from the memory card, the interpreter should first check that it is within the expected range. When reading a string from the memory card, the interpreter should not blindly assume that the string is '/0'-terminated, but should check that this is true before relying on it. Thus, this would involve identifying every point in the code that reads data from the memory card (or any other untrusted source) and inserting appropriate input validation checks at that point.

  Likewise, every place where the code manipulates a vote counter, the code should check that the vote counter is (a) non-negative, and (b) arithmetic on it (e.g., incrementing a vote counter) does not wrap or overflow. If the code always checked that every vote counter were non-negative, and eliminated all possibility of arithmetic overflow or wrap-around modulo 65,536, Hursti would not have been able to pre-load a negative number of votes for one candidate on the memory card. If the code had checked that all vote counters were zero at the start of the day, Hursti would not have been able to pre-load a positive number of votes for any candidate, either.

  In addition, it would be prudent to revise the source code of the interpreter to prevent infinite loops and infinite recursion. One way to do this would be to introduce a timeout of some sort, and check for timeout every time the

AccuBasic script executes any kind of backward jump, call, or control transfer.

- Revise the interpreter, line by line, to incorporate defensive programming throughout the code. If the code had been written to follow defensive programming practices in a more disciplined way, these vulnerabilities could not have existed.

  Programming and driving a car are similar in that the programmer, like the driver, cannot control his or her environment; he or she can merely control how the software, or the car, reacts to that environment. Driving courses emphasize "defensive driving." Driving students learn to prepare for other drivers taking unexpected, and dangerous, actions. They understand that they cannot control other drivers, and that they must avoid accidents even if those accidents are not their fault.

  Similarly, programmers should develop software with the understanding that the environment is not trusted. Users may enter incorrect input; system hardware may fail; touch screens may be miscalibrated and so return nonsensical values to the program. Good programming style is to build software that either functions correctly in the face of such errors, or else reports the error and terminates gracefully. This style of defensive programming is called "robust programming."

  As an example, a buffer overflow occurs when an input is larger than the memory allocated to hold that input. The excess input can change internal values, causing the software to malfunction and return incorrect results. In some cases, this allows a malicious user to breach security. Robust programming requires that *every* input be checked; were this style followed, buffer overflows would not occur because the program would check the length of the input, determine it was too long, and reject it.

  More generally, defensive programming generally means that every module should apply these checks to data it receives from other modules, and should refrain from trusting other modules. Just as drivers are taught that they cannot control what other drivers may do, defensive programming teaches that programmers cannot control what other modules may do, and so should treat them as untrusted and ensure that other modules cannot compromise their own integrity.

  Thus, defensive programming often involves disciplined use of various idioms that ensure the safety of the code. Before copying a string into the buffer, one inserts code to check that there is sufficient room for the string. Before dereferencing a pointer, one writes code to check that the pointer is not NULL. Before adding two integers, one checks that the addition will not overflow. Code is added to perform these checks, even when they seem unnecessary, because sometimes one's assumption that the check is not necessary turns out to be inaccurate.

  Our review of the interpreter source code showed that the programmers could have applied this principle of robust programming more extensively to the code. Specifically, the code had shortcomings (detailed above) that would not occur when software is designed and written to be robust. Hence, when the bugs in the AccuBasic interpreter are fixed, it seems prudent to also revise the code to be robust in the face of erroneous, unexpected, and malicious input, and other failures such as hardware failure.

- After the source code is revised, it would make sense to commission an independent source code review to confirm whether all of the vulnerabilities have been eliminated and to assess whether the code has used structured programming practices that are adequate to have confidence that no other security vulnerabilities of this sort are likely to be present.

If the source code is not revised, anyone with unsupervised access to a memory card, or with access to the GEMS server, may be able to exploit the vulnerabilities we found to take control of voting machines and compromise the electronic tallies. Such an attack might be able to cause lasting effects that persist across elections, and it is not clear whether there would be any way to repair the resulting damage. If the source code is revised to fix the vulnerabilities we found, these attacks would not be possible.

Even if the interpreter source code is fixed, it would still be possible for an individual who can introduce a malicious AccuBasic script to cause fraudulent zero tapes and fraudulent summary reports to be printed. Depending on whether the

arithmetic overflows are fixed, such an individual might also be able to pre-load a memory card with a positive or negative number of votes for some candidates.

Mitigation 3 *Protect AccuBasic object code from tampering and modification, either by (a) storing AccuBasic object code on non-removable storage and treating it like firmware, or by (b) protecting AccuBasic object code from modification through the use of strong cryptography (particularly public-key signatures).*

All of the vulnerabilities we uncovered were due to the fact that part of the code of the voting system (namely, the AccuBasic object code) was not adequately protected from modification. Thus, one effective mitigation would be to protect the code from modification, using one of two strategies:

(a) Protect AccuBasic object code in the same way that the rest of the firmware object code is protected, by placing the AccuBasic object code on physically secured non-removable storage. Normally, firmware is protected from modification by storing it on a non-removable storage device (e.g., EEPROM) that is not easily externally accessible and that is protected from casual tampering through some kind of physical security protection. AccuBasic object code could be stored in the same way. If this were done, it would eliminate an entire attack vector, because attackers would no longer have the opportunity to replace the AccuBasic object code with a malicious AccuBasic script.

Of course, in this approach AccuBasic code would need to be protected with the same protections that are afforded to firmware code. If there is any way to update AccuBasic object code (or any other code), the update process must be strongly authenticated, and updates to the AccuBasic object code must be authenticated as securely as updates to the firmware. (By *authenticated,* we mean that there are procedural and technological controls which ensure that only authorized individuals can update the code, and only under appropriate circumstances.)

We recognize that different jurisdictions may require different AccuBasic scripts. One way to handle this would be for each jurisdiction to update the firmware with the appropriate AccuBasic script. Another possibility would be for the vendor to store all the different versions of AccuBasic object files that might ever be needed on the firmware, and for the memory card to contain an index (e.g., numbered from 1 to n, where n is the number of different AccuBasic scripts stored in the firmware) identifying which of these .abo files is to be used. Depending on the circumstances, this index might need to be protected from modification.

(b) Alternatively: Use strong cryptography to protect the AccuBasic object code while it is stored on removable media. The appropriate protection would involve signing the AccuBasic object code with a cryptographically strong public-key signature scheme (e.g., RSA, DSA, or some other appropriate public-key algorithm) and arranging for the firmware to check the validity of this signature before executing the AccuBasic code. The private key would need to be guarded zealously (e.g., using a hardware security module (HSM)). In addition, considerable thought needs to be given to key management as well as to which part of the data is signed by which principals (e.g., by the vendor, by the GEMS server, or by other authorities).

While the AV–TSx cryptography is a good first step in this direction, it falls short in several respects:

- The use of symmetric-key cryptography in the AV–TSx increases the risk of key exposure. It would be safer to use public-key (asymmetric) digital signatures for this purpose.
- The use of hard-coded symmetric keys that are the same for all AV–TSx units is highly inappropriate for this purpose, and should be avoided at all costs.
- The existence of any kind of default key is a usability pitfall, because it makes it possible for election officials to forget to change the keys, thereby leaving them unaware of their vulnerability. This is an additional problem with hard-coded symmetric keys. We recommend that default keys be avoided.
- Insufficient thought has been given to the topic of key management and which entities are in possession of the appropriate cryptographic keys.

Fixing these shortcomings would prevent unauthorized individuals from introducing malicious AccuBasic scripts.

Of course, in both approaches the AccuBasic scripts need to be considered part of the code base of the system, and should be reviewed as part of the qualification and certification process.

In the long run, the consequences of not protecting AccuBasic code from modification are that anyone who gains unsupervised access to memory cards can tamper with their contents, attack the voting systems (e.g., using Hursti-style attacks), and potentially manipulate the electronic vote tallies.

Mitigation 4 *Change the architecture of the AV–OS and the AV–TSx so they do not store code on removable memory cards.*

In the long run there are good reasons for changing the AV–OS and AV–TSx software architectures so that they do not rely on interpreted code stored on a removable memory card, or that they do not use interpreted code at all and eliminate AccuBasic. All of the potential vulnerabilities discussed here are rooted in the fact the code is stored on the removable memory cards, and these cards are handled by, and in the custody of, many people in a major election. There does not seem to be any *fundamental* reason why the AccuBasic code cannot be part of the firmware code base, rather than stored on the removable memory card. That change would not only eliminate these attacks, but some GEMS-based attacks on the code as well. Of course there would need to be enough firmware storage space in the machines to hold the AccuBasic code, but we suspect that is not an insoluble problem. This change would reduce the vendor's flexibility in providing different reporting options to different jurisdictions (i.e., different AccuBasic scripts). But if it is accepted that the AccuBasic scripts are part of the voting system "code," as they are, and that therefore they must be subject to testing and code review by federal and state examiners, then that flexibility would be lost anyway, since it cannot be expected that the examiners would be able to study hundreds of variations on the AccuBasic script packages produced for different jurisdictions.

Mitigation 5 *Change the architecture of the AV–OS and the AV–TSx so they do not contain any interpreter or use any kind of interpreted code.*

There are also good arguments for eliminating AccuBasic interpreted code entirely from voting system software. The FEC 2002 Voluntary Voting System Standards expressly forbid interpreted code in section 4.2.2. Perhaps the standard writers had in mind forbidding only powerful, interpreted *programming* languages, such as Visual Basic, and not relatively benign and limited *rendering* languages such as HTML. AccuBasic falls somewhere in the middle on the more benign side (assuming the interpreter bugs are fixed). But the text of the standard is pretty clear, and the same language from the 2002 standards has been preserved in the EAC's new successor standard, the Voluntary Voting Systems Guidelines, as section 5.2.2. To be in compliance it would seem that AccuBasic would have to be eliminated, or the standard would have to be changed.

In any case, the inclusion of interpreted languages in a voting system causes great burdens on examiners and code reviewers, who have to be highly skilled and do considerable analysis of the compiler and interpreter in order to verify that it does not present security vulnerabilities or permit malicious code to go unnoticed. It seems untenable to us that every time there is a change to the AccuBasic language or interpreter another round of detailed code review such as we have done would be required; however, an interpreter is such a delicate and powerful feature (from a security point of view) that we cannot recommend shortcuts in its examination either.

5.2 Short-term Mitigation Strategies for Local Elections

One disadvantage of several of these mitigation strategies (e.g., revising or eliminating the AccuBasic interpreter, improving the cryptography, etc.) is that changes to the source code will incur significant delays. Source code changes would need to be approved by the federal qualification process as well as the state certification process. Therefore, in the short term it seems appropriate to consider mitigation strategies that do not involve changing the source code.

For local elections (i.e., elections that do not span the entire state), we believe there are mitigation strategies that could be viable for the short term. For instance, one possibility might be the following two-prong approach:

- For the AV–TSx, update the cryptographic keys on every AV–TSx machine and rely on the cryptography to prevent tampering with memory cards. Election officials would need to first choose a secret and unguessable cryptographic key. The new cryptographic key should be chosen at random by county staff, should not be divulged to anyone, not even the vendor (because

anyone who learns the secret key gains the ability to tamper undetectably with memory cards), should not be shared across counties, and should be tightly controlled. Then, the process of updating the keys requires inserting a smartcard into every AV–TSx machine. Officials could adopt checklists or some other process to ensure that every AV–TSx machine has had its keys updated before it is sent into the field. Election officials should be warned that if they forget to change the cryptographic keys, the machine will outwardly appear to function correctly, but will be vulnerable to attack.

- For the AV–OS, deploy strict procedural safeguards to prevent anyone from gaining unsupervised access to a memory card. We would suggest dual-person controls over the entire life cycle of the memory card, chain of custody provisions, and use of numbered tamper-evident seals. It would also help to load and seal the memory card into the AV–OS unit at the warehouse in advance of the election, ship it in this state, and when the election is over, have poll workers return the entire machine (with the memory card still sealed inside) to the county collection point, where election officials would check that the seal remains undisturbed and record the number on the seal before removing the memory card. This would ensure that the memory card is protected by a tamper-evident seal for the entire time that it is outside the control of county staff and would reduce the opportunities for someone to tamper with the memory card while it is in transit. We recognize that these heightened procedural protections are likely to be somewhat burdensome, but as a short-term protection (until the source code can be fixed), they may be appropriate. See Mitigation 1 for further discussion of procedural mitigations.

While these strategies do not completely eliminate all risk, we expect they would be capable of reducing the risk to a level that is manageable for local elections in the short term.

In the longer-term, or for statewide elections, the risks of not fixing the vulnerabilities in the AccuBasic interpreter become more pronounced. Larger elections, such as a statewide election, provide a greater incentive to hack the election and heighten the stakes. Also, the longer these vulnerabilities are left unfixed, the more opportunity it gives potential attackers to learn how to exploit these vulnerabilities. For statewide elections, or looking farther into the future, it would be far preferable to fix the vulnerabilities discussed in this report.

6. Conclusions

We have detailed a number of security vulnerabilities in the AV–OS and AV–TSx implementations of the AccuBasic interpreter. In the long-term, these vulnerabilities can be easily fixed and the risks eliminated or mitigated. We have made recommendations about several ways in which that might be accomplished. In the short term, we believe the risks can be mitigated through appropriate use procedures.

7. Glossary

.abo file a file containing AccuBasic object code (byte code)

AccuBasic a Diebold-proprietary programming language used (in slightly different versions) in both the AV–OS and AV–TSx machines; AccuBasic programs allow very limited control over the behavior of the voting system

buffer a fixed-size area of memory

buffer overrun a type of program bug in which the program attempts to write more data into a buffer than the buffers size permits. The extra data is thus written beyond the end of the buffer into other memory, where it often overwrites something else of significance, i.e., either other data, or control information, or even instructions. When that happens, the program is corrupted, and any of a vast number of unpredictable things might ensue. One common hacker attack is to deliberately take advantage of a buffer overrun bug, corrupting the program in a specific way that allows the hacker to do things he otherwise would not be able to do. (Usually the goal is to take complete control of the machine.)

byte code object code of a relatively simple kind (e.g., that happens to be encoded as characters (bytes) instead of binary data)

C a very widely used programming language

C++ another widely used programming language, more modern than C, and (roughly) including C as a subset

compiler a program that translates another program from its source language (the human readable form) into an object language (a form not so easily human

readable, but much more convenient for machine execution). The AccuBasic compiler translates AccuBasic programs (source code) into AccuBasic object code (also known as byte code in this case).

file system hierarchical collection of files and directories (folders), along with their names, types, and the software to read and write them

firmware software resident inside the voting machine (i.e., not on a removable memory card) and that is (or should be) unmodifiable once the machine is in operation

hex editor an editor that can modify data directly at the binary level. (Hex refers to hexadecimal (base-16) arithmetic, which is extremely closely related to binary, but more compact.) A hex editor is a universal editor, in that it can edit absolutely any kind of digital data, although it requires some knowledge and skill to use it in any particular case.

interpreter a program whose function is to execute another program, usually one that is in the form of object code. The AccuBasic interpreter is part of the firmware of the AV–OS or AV–TSx, and executes AccuBasic object code, i.e., .abo files.

memory mapped memory mapped data is data that resides on some attached memory device, and yet is made to appear as if it is in main memory. (In the technical jargon, the data on the attached device is mapped onto a portion of the machines memory address space.)

object code a program represented in the form of discrete instructions that are easy for a computer (or an interpreter) to execute efficiently. It is more difficult for humans to read and write object code than source code, but it can be done with only modest skill. Usually object code is produced with the aid of a compiler, but it does not have to be.

scripting language a programming language designed primarily so that the programs written in it can easily manipulate character data and files (as opposed to, e.g., binary data), and can easily invoke and control other programs; AccuBasic can be described as a limited-purpose scripting language.

scripts programs written in a scripting language like AccuBasic

source code any software in the original form as written by a human programmer; this is the form in which code is easily read and written by programmers, but cannot be directly executed by a computer or an interpreter.