CERTIFICATION AND TESTING OF ELECTRONIC VOTING SYSTEMS

HEARING

BEFORE THE

SUBCOMMITTEE ON INFORMATION POLICY, CENSUS, AND NATIONAL ARCHIVES

OF THE

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

HOUSE OF REPRESENTATIVES

ONE HUNDRED TENTH CONGRESS

FIRST SESSION

MAY 7, 2007

Serial No. 110–13

Printed for the use of the Committee on Oversight and Government Reform

Available via the World Wide Web: http://www.gpoaccess.gov/congress/index.html
http://www.oversight.house.gov

U.S. GOVERNMENT PRINTING OFFICE

36–750 PDF WASHINGTON : 2007

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) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

COMMITTEE ON OVERSISGHT AND GOVERNMENT REFORM

HENRY A. WAXMAN, California, *Chairman*

TOM LANTOS, California
EDOLPHUS TOWNS, New York
PAUL E. KANJORSKI, Pennsylvania
CAROLYN B. MALONEY, New York
ELIJAH E. CUMMINGS, Maryland
DENNIS J. KUCINICH, Ohio
DANNY K. DAVIS, Illinois
JOHN F. TIERNEY, Massachusetts
WM. LACY CLAY, Missouri
DIANE E. WATSON, California
STEPHEN F. LYNCH, Massachusetts
BRIAN HIGGINS, New York
JOHN A. YARMUTH, Kentucky
BRUCE L. BRALEY, Iowa
ELEANOR HOLMES NORTON, District of Columbia
BETTY McCOLLUM, Minnesota
JIM COOPER, Tennessee
CHRIS VAN HOLLEN, Maryland
PAUL W. HODES, New Hampshire
CHRISTOPHER S. MURPHY, Connecticut
JOHN P. SARBANES, Maryland
PETER WELCH, Vermont

TOM DAVIS, Virginia
DAN BURTON, Indiana
CHRISTOPHER SHAYS, Connecticut
JOHN M. McHUGH, New York
JOHN L. MICA, Florida
MARK E. SOUDER, Indiana
TODD RUSSELL PLATTS, Pennsylvania
CHRIS CANNON, Utah
JOHN J. DUNCAN, Jr., Tennessee
MICHAEL R. TURNER, Ohio
DARRELL E. ISSA, California
KENNY MARCHANT, Texas
LYNN A. WESTMORELAND, Georgia
PATRICK T. McHENRY, North Carolina
VIRGINIA FOXX, North Carolina
BRIAN P. BILBRAY, California
BILL SALI, Idaho

PHIL SCHILIRO, *Chief of Staff*
PHIL BARNETT, *Staff Director*
EARLEY GREEN, *Chief Clerk*
DAVID MARIN, *Minority Staff Director*

SUBCOMMITTEE ON INFORMATION POLICY, CENSUS, AND NATIONAL ARCHIVES

WM. LACY CLAY, Missouri, *Chairman*

PAUL E. KANJORSKI, Pennsylvania
CAROLYN B. MALONEY, New York
JOHN A. YARMUTH, Kentucky
PAUL W. HODES, New Hampshire

MICHAEL R. TURNER, Ohio
CHRIS CANNON, Utah
BILL SALI, Idaho

TONY HAYWOOD, *Staff Director*

CONTENTS

	Page
Hearing held on May 7, 2007	1
Statement of:	
Davidson, Donetta L., chairman, U.S. Election Assistance Commission; and Mark W. Skall, chief, Software Diagnostics and Conformance Testing Division, National Institute on Standards and Technology	17
Davidson, Donetta L.	17
Skall, Mark W.	34
Kellner, Douglas A., co-chair, New York State Board of Education; Dr. David Wagner, associate professor, Computer Science Division, University of California, Berkeley; Lawrence Norden, Brennan Center for Justice, New York University School of Law; John Washburn, VOTETRUSTUSA Voting Technology Task Force; and Mac J. Slingerlend, president and CEO, CIBER, Inc., accompanied by John Pope, vice president for contracts	54
Kellner, Douglas A.	54
Norden, Lawrence	78
Slingerlend, Mac J.	105
Wagner, Dr. David	64
Washburn, John	93
Letters, statements, etc., submitted for the record by:	
Clay, Hon. Wm. Lacy, a Representative in Congress from the State of Missouri, prepared statement of	3
Davidson, Donetta L., chairman, U.S. Election Assistance Commission, prepared statement of	19
Kellner, Douglas A., co-chair, New York State Board of Education, prepared statement of	57
Maloney, Hon. Carolyn B., a Representative in Congress from the State of New York:	
Information concerning CIBER	110
Prepared statement of	15
Norden, Lawrence, Brennan Center for Justice, New York University School of Law, prepared statement of	80
Skall, Mark W., chief, Software Diagnostics and Conformance Testing Division, National Institute on Standards and Technology, prepared statement of	36
Slingerlend, Mac J., president and CEO, CIBER, Inc., information concerning CIBER	118
Wagner, Dr. David, associate professor, Computer Science Division, University of California, Berkeley, prepared statement of	66
Washburn, John, VOTETRUSTUSA Voting Technology Task Force, prepared statement of	96

CERTIFICATION AND TESTING OF ELECTRONIC VOTING SYSTEMS

MONDAY, MAY 7, 2007

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON INFORMATION POLICY, CENSUS, AND NATIONAL ARCHIVES,
COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM,
New York, NY.

The subcommittee met, pursuant to notice, at 9:30 a.m., in City Council Chambers, New York City Hall, 131 Duane Street, New York, NY, Hon. Wm. Lacy Clay (chairman of the subcommittee) presiding.

Present: Representatives Clay and Maloney.

Staff present: Tony Haywood, staff director/counsel; Adam C. Bordes, professional staff member; and Nidia Salazar, staff assistant.

Mr. CLAY. The Subcommittee on Information Policy, Census, and National Archives of the House Committee on Oversight and Government Reform will now come to order.

Today's hearing will examine issues relating to the certification and testing of electronic voting systems under the Help America Vote Act of 2002.

Without objection, the Chair and other Members present will have 5 minutes to make opening statements, and without objection, Members and witnesses may have 5 legislative days to submit a written statement, or extraneous material for the record.

Let me say, first of all, that it is a pleasure to be here in the Big Apple to discuss a topic of tremendous importance to New Yorkers and the Nation as a whole; the need for effective and transparent certifications and testing of electronic voting systems. I want to thank my distinguished friend and colleague, Congresswoman Carolyn Maloney, for inviting us to New York and I want to thank City Council Speaker Christine Quinn for making the City Council Chambers available to us. This is a wonderful venue for a hearing.

And this is the subcommittee's second hearing on electronic voting systems. During an April 18th hearing in Washington, the subcommittee heard testimony concerning widespread vulnerabilities in modern electronic voting systems. Those weaknesses are a major concern for Congress, State, and local entities, that administer the electoral process, and all Americans who value their stake in our democracy. Passed on response to reports of serious voting irregularities during the November 2000 Presidential election, HAVA established the first set of uniform minimum standards and requirements for the administration of Federal elections.

The law authorized $3.86 billion in funding. The bulk of this funding was provided to enable States to replace punch card or mechanical voting equipment, improve their election administration capabilities, meet new election requirements and improve access for disabled voters.

Beginning in fiscal year 2003, many States used HAVA funds to procure new electronic voting systems. In 2005, the EAC approved new voting system standards, the 2005 voluntary voter system guideline for States to use as a reference, when procuring new machines under HAVA.

Unfortunately, numerous States have reported problems with new voting systems, as well as difficulty ensuring that their systems comply with the evolving HAVA standards.

Voting system problems include software vulnerabilities that impair security or reliability, and the inability to confirm voter intent in the case of systems that lack an independent audit component, such as a verifiable paper trail.

A change in requirements have left some States out of compliance with HAVA standards because their systems were designed and procured before current standards took effect.

In addition, there have been serious problems relating to the EAC's accreditation and oversight labs that test and certify voting systems for compliance with HAVA.

In January, for example, the New York State Board of Elections suspended CIBER, Inc., a lab that has reportedly tested 70 percent of the Nation's voting systems, due to ineffective internal controls and CIBER certification practices, and lack of transparency in their testing process.

CIBER also has failed to win accreditation by the EAC. New York has decided to postpone the procurement of new voting systems until there is a more dependent and transparent certification program to identify system vulnerabilities and ensure HAVA compliance before systems are marketed to States.

We rely upon our voting systems to record each and every vote accurately. Uniform testing standards and vigorous oversight of the certification process for voting systems are necessary to ensure that these systems operate reliability and securely, and without this we risk eroding the public confidence that is necessary for active voter participation and a healthy democracy.

We have invited today's witnesses here to shed light on the factors that have impeded the ernest efforts of States like New York, to improve accuracy, reliability and security in their voting systems, while complying with HAVA requirements.

I want to thank all of our witnesses for appearing before the subcommittee today, particularly those who traveled long distances and adjusted their busy schedule to be with us. I welcome all of you and look forward to an informative and frank discussion of these important issues, and now I would turn to my colleague and dear friend, Mrs. Carolyn Maloney. Thank you.

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

Attention for —

Opening Statement of Rep. Wm. Lacy Clay (D-MO), Chairman
Subcommittee on Information Policy, Census, and National Archives
House Committee on Oversight and Government Reform
Field Hearing on "Certification and Testing of Electronic Voting Systems"
City Hall, New York, NY

May 7, 2007

GOOD MORNING. TODAY WE WILL EXAMINE CHALLENGES RELATED TO THE CERTIFICATION AND TESTING OF ELECTRONIC VOTING SYSTEMS UNDER THE HELP AMERICA VOTE ACT OF 2002, OR HAVA ~~(HAH-VUH).~~

IT IS A PLEASURE BEING HERE IN THE BIG APPLE TO DISCUSS A TOPIC THAT IS OF TREMENDOUS IMPORTANCE TO NEW YORKERS AND THE NATION AS A WHOLE.

I WANT TO THANK OUR GRACIOUS HOST, CONGRESSWOMAN CAROLYN MALONEY AND ALSO THANK MAYOR BLOOMBERG FOR WELCOMING US INTO CITY HALL; SUCH A

WONDERFUL VENUE FOR OUR HEARING.

THIS IS THE SUBCOMMITTEE'S SECOND HEARING ON ELECTRONIC VOTING SYSTEMS.

DURING OUR FIRST HEARING, HELD IN WASHINGTON ON APRIL 18TH, THE SUBCOMMITTEE HEARD TESTIMONY CONCERNING WIDESPREAD VULNERABILITIES IN OUR MODERN ELECTRONIC VOTING SYSTEMS.

THOSE WEAKNESSES ARE A MAJOR CONCERN FOR CONGRESS, STATE AND LOCAL ENTITIES THAT ADMINISTER THE ELECTORAL PROCESS, AND ALL AMERICANS WHO VALUE THE INTEGRITY OF OUR DEMOCRATIC PROCESS.

OUR VOTING SYSTEMS MUST BE RELIED UPON TO RECORD EACH AND EVERY VOTE ACCURATELY. FLAWS IN THE SECURITY OF THESE SYSTEMS UNDERMINE THE PUBLIC CONFIDENCE THAT IS NECESSARY TO ENCOURAGE ACTIVE VOTER PARTICIPATION.

OUR DEMOCRACY IS WEAKENED WHEN PEOPLE DO NOT TRUST THAT THEIR VOTE BE COUNTED OR WILL NOT BE COUNTED CORRECTLY.

CONGRESS PASSED HAVA IN RESPONSE TO NUMEROUS REPORTS OF VOTING IRREGULARITIES DURING THE 2000 ELECTIONS. THE LAW ESTABLISHED THE FIRST SET OF UNIFORM MINIMUM STANDARDS AND REQUIREMENTS FOR THE ADMINISTRATION OF FEDERAL ELECTIONS.

MOST IMPORTANTLY, HAVA CREATED THE ELECTION ASSISTANCE COMMISSION, OR E.A.C., WHICH WAS DESIGNED TO SERVE AS A NATIONAL CLEARINGHOUSE FOR ELECTION INFORMATION.

THE E.A.C. IS CHARGED WITH DEVELOPING STANDARDS FOR ELECTRONIC VOTING AND WITH ASSISTING STATE AND LOCAL GOVERNMENTS TO ENSURE THEIR COMPLIANCE WITH HAVA REQUIREMENTS.

THE E.A.C. APPROVED NEW VOTING SYSTEM STANDARDS, KNOWN AS THE 2005 VOLUNTARY VOTER SYSTEM GUIDELINES, FOR STATES TO USE AS A REFERENCE WHEN PROCURING NEW MACHINES UNDER HAVA.

IT ALLOCATED OVER $3 BILLION IN FUNDS FOR STATE COMPLIANCE EFFORTS AND TO IMPROVE INADEQUATE ELECTION ADMINISTRATION PRACTICES.

NEVERTHELESS, STATE AND LOCAL GOVERNMENTS CONTINUE TO REPORT SIGNIFICANT PROBLEMS WITH THEIR ELECTRONIC VOTING SYSTEMS.

SOME OF THE MORE SERIOUS ISSUES INCLUDE SOFTWARE VULNERABILITIES AND MACHINES THAT LACK AN INDEPENDENT AUDIT COMPONENT TO CONFIRM A VOTER'S INTENT, SUCH AS A VERIFIABLE PAPER TRAIL.

FURTHERMORE, THERE HAVE BEEN RECENT REVELATIONS

CONCERNING FAULTY ACCREDITATION PRACTICES AND LAX OVERSIGHT BY THE E.A.C. WITH REGARD TO LABS TASKED WITH CERTIFYING SYSTEM SOFTWARE AND HARDWARE UNDER HAVA STANDARDS.

STATE AND LOCAL OFFICIALS DESERVE CONCRETE PROOF THAT THEIR SYSTEMS ARE RELIABLE AND SECURE.

IN RESPONSE TO THE LACK OF INDEPENDEND OVERSIGHT, STATES SUCH AS NEW YORK HAVE DECIDED TO POSTPONE THE PROCUREMENT OF NEW VOTING SYSTEMS UNTIL THERE IS A MORE DEPENDABLE SYSTEM CERTIFICATION PROGRAM TO IDENTIFY VULNERABILITIES IN PRODUCTS BEFORE THEY REACH THE MARKETPLACE.

IN JANUARY THE NEW YORK STATE BOARD OF ELECTIONS SUSPENDED CIBER, INC. -- THE LAB IT HIRED TO ASSIST THE STATE WITH ITS PROCUREMENT CERTIFICATION PROCESS -- DUE TO INEFFECTIVE INTERNAL CONTROLS IN THEIR CERTIFICATION PRACTICES AND LACK OF TRANSPARENCY IN THEIR TESTING PROCESS.

TODAY'S HEARING OFFERS AN OPPORTUNITY TO UNDERSTAND, FROM A VARIETY OF IMPORTANT PERSPECTIVES, WHAT FACTORS HAVE CONTRIBUTED TO SHORTCOMINGS IN THE E.A.C.'S OVERSIGHT OF LABS AND VENDORS RESPONSIBLE FOR MEETING HAVA REQUIREMENTS.

OF COURSE, WE ALSO WANT TO LEARN WHAT STEPS THE E.A.C. AND

OTHERS ARE TAKING TO MAKE HAVA WORK AS CONGRESS INTENDED.

IF THE E.A.C. IS FAILING TO MEET THEIR OBLIGATIONS UNDER HAVA, THEN WE MUST ACT QUICKLY TO REMOVE TECHNICAL AND REGULATORY OBSTACLES THAT HAVE HINDERED EFFORTS OF DEVELOPING MORE RELIABLE AND SECURE VOTING SYSTEMS.

I AM HONORED TO HAVE MY FRIEND AND COLLEAGUE WHO IS A STRONG LEADER ON VOTING ISSUES, CONGRESSMAN RUSH HOLT OF NEW JERSEY. I THANK ALL OF OUR EXPERT WITNESSES FOR APPEARING BEFORE THE SUBCOMMITTEE TODAY.

PARTICULARLY THOSE WHO TRAVELED LONG DISTANCES TO BE HERE. I WELCOME ALL OF YOU AND LOOK FORWARD TO AN INFORMATIVE AND FRANK DISCUSSION OF THESE IMPORTANT ISSUES.

##

Mrs. MALONEY. Thank you so much, Lacy Clay, for your leadership on this and so many other important issues before Congress and for traveling all the way, to be here, in New York City on this very important issue. Truly nothing is more important to our democracy than the accuracy, the reliability, the trust that our people have in our voting systems, and the fact that they are reliable and dependable and transparent.

I do want to say that Rush Holt had hoped to be with us, but was not able to. He brings his greetings. He says we will be marking up his bill that he has worked 8 years on, Intro 811, tomorrow, in Congress, it will be moving forward with tremendous and important funding, $1 billion for new voting machines, $100 million for auditing and making sure that the voting machines work, and also calls for an independent audit, a paper trail. It's very important legislation. I support it.

I know that Lacy and I have some ideas to make it even better. But it is a compromise. I'm thrilled that it's moving forward and I thank all of our attendees today.

It shows that you care about our democracy, and most importantly, I thank all of our witnesses for coming and for the hard work that they're doing on this subject.

And I really especially appreciate all the hard work done by Mr. Clay and his staff on an issue that is very important to me, and I would say to every American, the accuracy and security of the Nation's voting systems.

In recent years, considerable concern has been expressed about the security and reliability of the electronic voting systems. Reports from governmental agencies, testimony before Congress, and academic studies, have indicated serious vulnerabilities that call for immediate attention.

I must add that it is one of the issues that people literally walk up to me on the street, at events, at meetings. They come up and express their concern over voting machines. This is a critical issue to my constituents and I would say to every American across this country.

Penetration testing done by independent computer security experts has demonstrated that election results can be altered in a manner that cannot be detected by normal election security procedures. Independent reviews commissioned by State election officials have revealed serious security vulnerabilities in the software, architecture of voting systems now in use.

Typically, when concerns about the security and reliability of voting systems are raised, supporters argue that these systems have been tested to Federal standards. However, at a recent hearing of this subcommittee, the Government Accountability Office reported, "The test performed by independent testing authorities, and State and local election officials, do not adequately assess electronic voting systems security and reliability. These concerns are intensified by a lack of transparency in the testing system."

The GAO, which is an independent bipartisan governmental agency, noted weak and insufficient system testing, source code reviews and penetration testing. They pointed out that most of the systems that exhibited the weak security controls had been nationally certified after testing by an independent testing authority.

Now that is scary. They're saying you cannot trust them and they've been certified. Last summer, the EAC undertook a review of the laboratories that had been testing under the NASED program. The assessment review of one of these labs, CIBER concluded, "CIBER has not shown the resources to provide a reliable product." The report also noted, "CIBER reports provide limited or no descriptions of the testing performed, so a reader or reviewer can tell if all the testing was completed."

This is very serious. This is one of the things that we want to accomplish this hearing, is how we can rectify this.

Here, in New York, an independent review—and I want to applaud the elections board of New York, they went out and got an independent review, many States did not, but New York State is so concerned about this issue; they got an independent reviewer of CIBER's test plans and these revealed that they did not document the methodologies, procedures, and processes necessary to ensure that all testing is done in a structured and repeatable way.

It is estimated that CIBER has tested the software in more than 70 percent of the voting machines used last November. So what the GAO and the independent review in New York is telling us is that 70 percent of those voting machines that are out there being used, really have not been tested adequately and have not been certified adequately, and may have serious flaws. Estimated, because there is no way to know for sure which lab tested which system, and apparently there's also no way of knowing, for sure, if any testing was done at all. Trusting the word of the ITA or testing labs, election officials across the country use taxpayer money to purchase equipment, believing that this equipment was in conformance with Federal standards.

Apparently, we have no way of knowing whether the equipment actually does meet Federal standards. CIBER hides behind a cloak of confidentiality, and personally, I believe that in something as important as the reliability of our voting machines, there should be no confidentiality; it should be transparent and open to the election officials, and I would say the public.

Because test methods are considered proprietary, the public and election officials cannot verify that procedures were done properly. When a system fails a test, there is no public announcement. Why in the world aren't they telling people, if certain systems are failing these tests? We have a right to know this.

Many States went out and bought these machines, thinking they were reliable. If they had known that they had failed tests, or hadn't even been certified, they would never have bought them.

Further, if the system subsequently passes, there is no way to identify what changes the manufacturer made, if any, to enable the system to pass. Considering that CIBER certified 70 percent of the machines that were used last November, we have a real dilemma. Do we keep using machines that were certified by these testing labs that did not meet the standards for accreditation, or do we have to start all over and recertify? That is a basic question before this committee today.

I am very pleased that CIBER will be here today to respond to our concerns. The National Testing and Certification Program has been vital to the sales and acceptance of voting machines in most

States. Experience is often the best test and a great deal of jurisdictions are finding problems with the machines that the testing labs seem to have missed.

Several States have moved forward quickly to buy touch screen voting machines, and they are realizing that the machines they bought do not work very well.

New Mexico, the State of New Mexico decided to switch to optical scan style voting, statewide. In 2006, including in four counties it spent nearly $4 million for touch screen machines. Last month, Maryland switched to optical scan. They even took the extraordinary step of having paper ballot votes because they didn't trust the machines.

This month, Florida followed suit, and incidentally, there will be hearings in Washington on the contested "Florida 15" because of the missing votes. New York is looking pretty smart these days. We were criticized for not going out there and buying those machines. There were court suits against us. But I think New York looks pretty smart, because New York focused on standards and refused to jump quickly into untested technology. Our elected officials may have saved taxpayers a great deal of money. We didn't buy machines that we have to change, and the New York delegation, led by Congressman Serrano, is working very hard to restore the $50 million that was taken away from New York State.

It was part of a bill that was moving forward, that has been vetoed; but we believe we will be successful in restoring that money.

We need meaningful testing to make sure equipment meets the 2005 standards. This hearing provides an opportunity to examine the current state of voting systems testing and certification in this great Nation. It can also serve as a step toward a more transparent and trustworthy process in the future. Unless we improve our certification process, we are in danger of losing the confidence of American voters.

And I want to really thank the advocates and citizens that turned out today, and many of your constant questions, e-mails, phone calls to me, are one of the reasons that I have reached out to the chairman of the appropriate committee to hold these hearings, and he has done a magnificent job and I am sure he will not stop until he is satisfied, that we have safe, reliable, transparent voting machines. So I thank everyone, especially the chairman.

[The prepared statement of Hon. Carolyn B. Maloney follows:]

14th District • New York

Congresswoman

Carolyn Maloney

Reports

2430 Rayburn Building • Washington, DC 20515 • 202-225-7944
1651 Third Avenue • Suite 311 • New York, NY 10128 • 212-860-0606

Statement of Congresswoman Carolyn B. Maloney
Field Hearing on the Certification and Testing of Electronic Voting Systems
May 7, 2007

I would like to thank Chairman Clay for holding this hearing today, and for traveling all the way to be here this morning. I appreciate all the hard work done by the gentleman and his staff on an issue that is very important to me -- the accuracy and security of the nation's voting systems.

In recent years, considerable concern has been expressed about the security and reliability of electronic voting systems. Reports from governmental agencies, testimony before Congress, and academic studies have indicated serious vulnerabilities that call for immediate attention.

Penetration testing done by independent computer security experts has demonstrated that election results can be altered in a manner that cannot be detected by normal election security procedures. Independent reviews commissioned by state election officials have revealed serious security vulnerabilities in the software architecture of voting systems now in use.

Typically, when concerns about the security and reliability of voting systems are raised, supporters argue that these systems have been tested to Federal standards. However, at a recent hearing of this subcommittee, the Government Accountability Office (GAO) reported that "the tests performed by independent testing authorities and state and local election officials do not adequately assess electronic voting systems' security and reliability. These concerns are intensified," they continued, "by a lack of transparency in the testing process." The GAO noted weak and insufficient system testing, source code reviews, and penetration testing. They pointed out that most of the systems that exhibited the weak security controls had been nationally certified after testing by an independent testing authority.

Last summer the EAC undertook a review of the laboratories that had been testing under the NASED program. The Assessment Report of one of those labs, CIBER, concluded, "CIBER has not shown the resources to provide a reliable product." The report also noted "CIBER's reports provide limited or no descriptions of the testing performed so a reader or reviewer can not tell if all the testing was completed." Here in New York an independent review of CIBER's test plans revealed that they did not document the methodologies, procedures and processes necessary to ensure that all testing is done in a structured and repeatable way.

It is estimated that CIBER has tested the software in more than 70% of the voting machines used last November. "Estimated" because there's no way to know for sure which lab tested which system. And apparently there is also no way of knowing for sure if any testing was done at all.

Trusting the word of the ITA, election officials across the country used taxpayer money to purchase equipment believing that this equipment was in conformance with Federal standards. Apparently we have no way of knowing whether the equipment actually does meet Federal standards. CIBER hides behind a cloak of confidentiality. Because test methods are considered proprietary, the public and election officials cannot verify that procedures are done properly.

When a system fails a test, there's no public announcement. Further, if the system subsequently passes, there's no way to identify what changes the manufacturer made, if any, to enable the system to pass. Considering that CIBER certified 70% of the machines in use last November, we have a real dilemma. Do we keep using machines that were certified by an ITA that did not meet the standards for accreditation or do we have to start over and recertify? I'm glad that CIBER will be here today to respond to our concerns.

The national testing and certification program has been vital to the sales and acceptance of voting systems in most states. Experience is often the best test – and a lot of jurisdictions are finding problems with the machines that the ITAs seem to have missed. Several states that moved forward quickly to buy touch screen voting machines are realizing that the machines they bought don't work very well. New Mexico decided to switch to optical scan-style voting statewide in 2006, including in four counties that spent a total of $4 million for touch-screen machines. Last month Maryland switched to optical scan. This month Florida followed suit.

New York is looking pretty smart these days – by focusing on standards and refusing to jump quickly into untested technology, our election officials may have saved taxpayers a lot of money.

We need meaningful testing to make sure equipment meets the 2005 standards. This hearing provides an opportunity to examine the current state of voting system testing and certification in this great nation. It can also serve as a step towards a more transparent and trustworthy process in the future.

Unless we improve our certification process, we are in dangering of losing the confidence of American voters.

Mr. CLAY. Thank you so much, Representative Maloney. Let me also say that I represent Missouri, which is known as the "Show Me State," and Representative Maloney has certainly laid the marker down for what the intent is of this hearing and future hearings on the transparency. So it is time that the people that produce election machines, those who monitor, those who have the authority over it, show the people of this country that it is transparent, show them that their votes will be counted accurately.

And let me say that on our first panel, we will hear from the Honorable Donetta Davidson, Chair of the U.S. Election Assistance Commission and Mr. Mark W. Skall, chief of the Software Diagnostics and Conformance Testing Division within the Information Technology Laboratory of the National Institute on Standards and Technology.

And we also have our newest commissioner of the Election Assistance Commission, Rosemary Rodriguez. Thank you for being here, Ms. Rodriguez. Let me thank all of you for being here today before the subcommittee and it is the policy of the Committee on Oversight and Government Reform to swear in all witnesses before they testify.

I would like to ask you both to stand and raise your right hands.

[Witnesses sworn.]

Mr. CLAY. Thank you. You may be seated. Let the record reflect that the witnesses answered in the affirmative and I will ask you both to give a brief summary of your testimony and to keep the summary under 5 minutes in duration, and those lights in front of you will indicate when you get down to 1 minute, and then when it turns red, that means your 5 minutes is up.

You complete written statement will be included in the hearing record.

Ms. Davidson, we will begin with you. Please proceed.

STATEMENTS OF DONETTA L. DAVIDSON, CHAIRMAN, U.S. ELECTION ASSISTANCE COMMISSION; AND MARK W. SKALL, CHIEF, SOFTWARE DIAGNOSTICS AND CONFORMANCE TESTING DIVISION, NATIONAL INSTITUTE ON STANDARDS AND TECHNOLOGY

STATEMENT OF DONETTA L. DAVIDSON

Ms. DAVIDSON. Thank you very much, Mr. Chairman. We are here to discuss the reliability of voting systems. With the committee's permission, I think it's important to talk, just for a moment, about how equipment has been tested in the past. The National Association of Election Directors [NASED], tested voting equipment against the guidelines created by the Federal Election Commission. They did this on a volunteer process and without any Federal funding.

The Federal Government, at that time, at 2002 standards by, and up to just recently, they did not certify, the Federal Government did not certify voting equipment.

It wasn't until the Help America Vote Act, that even—we also know it was HAVA—that put this into place, where we could test equipment, and I would like to go further into that with questions

because my statement won't allow time, but we'll go further into it.

HAVA requires EAC to create voting system guidelines and it also accredited the labs which will test voting systems.

The commission voluntary adopted voting system guidelines in December 2005. Our certification program got underway to test voting equipment this year. And let me be absolutely clear. We did not grandfather any vendors or test labs into the process.

The National Institute of Standards and Technology is EAC's valuable partner in both of these areas. NIST evaluates the test labs and provides recommendations to the EAC.

After review, NIST recommends, and we conduct additional reviews when the commission makes final decision, before we make the final decision. As of today, we have two accredited labs. There is nine manufacturers or vendors that have registered for our program. Five systems have been submitted for certification. Information about these labs and the manufacturers are on our Web site at www.eac.gov. EAC will hold the vendors and the labs to do their job and make sure they take responsibility.

We do have ability to decertify in both cases. We have set up a quality monitoring program and we will work hard with the States to investigate on reports and the voting systems irregularities and share this information with election officials and the public.

So what does the future hold for voting systems? We are working with NIST on the next iteration of guidelines and we expect to receive this a little later this year.

Just like 2005 guidelines, the version will further increase security requirements. However, no matter how thorough we test voting machinery, people ultimately ensure the voting equipment is reliable. People remove the ballots from the ballot boxes. People unlock the optical scan machines and remove the ballots. And people program all voting equipment.

To successfully compromise a voting system, any voting system on election day, you must have two things—knowledge of that system and access to that system.

Focusing on the security of voting machines in a laboratory is not enough. No voting system, ballot box, touch screen or optical scan, should be trusted unless officials store them in secure locations, prevent tampering, conduct logic and accuracy testing as well as all other testing, have well-trained workers, in other words, your poll workers, audit the result, and let the public observe the process.

I have spent most of my career in elections, and some things never change. Detail matter, whether we are using paper ballots, we use touch screen, or we use the DRE, the direct record. It is important to remember that the voting equipment must work properly as well as to have procedures and make sure that the people are well-trained to control the access and maintain the equipment properly.

Thank you. I look forward to your questions.

[The prepared statement of Ms. Davidson follows:]

TESTIMONY

THE HONORABLE DONETTA DAVIDSON, COMMISSIONER

CERTIFICATION AND TESTING OF ELECTRONIC VOTING EQUIPMENT

OVERSIGHT AND GOVERNMENT REFORM COMMITTEE
INFORMATION POLICY, CENSUS, AND NATIONAL ARCHIVES SUBCOMMITTEE

MONDAY, MAY 7, 2007

U.S. Election Assistance Commission
1225 New York Ave., NW – Suite 1100
Washington, DC 20005

Good morning Chairman Clay, Ranking Member Turner, and Members of the Subcommittee. I am pleased to be here this morning on behalf of the U.S. Election Assistance Commission (EAC) to discuss the changes in voting system requirements 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: Donetta Davidson, Chair; Rosemary Rodriguez, Vice Chair; Gracia Hillman; and Caroline Hunter. 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. The topic of this hearing involves our strategic efforts to aid in the improvement of voting systems and to provide guidance and information to States to assist in improving the voting process. These programs and EAC's efforts to assist States with implementing voting systems and procedures to safeguard those systems will be discussed in more detail below.

VOTING SYSTEMS

Effective administration of voting systems requires the use of accurate, reliable, accessible and auditable voting systems. There are various opinions on what constitutes accurate, reliable, accessible and auditable, but one clear source is the Help America Vote Act of 2002 (HAVA). HAVA establishes a number of requirements for voting systems, including that the system:

- Allow the voter the ability to change his or her selections prior to casting a vote;
- Notify the voter of an overvote and the consequences of casting an overvote;
- Provide a permanent paper record of the election that is auditable;
- Provide accessibility to individuals with disabilities including persons who are blind or visually impaired;
- Provide accessibility to persons for whom English is not their first language when required by Section 203 of the Voting Rights Act; and
- Meet or exceed the error rate as established in the 2002 Voting System Standards developed by the Federal Election Commission.

See HAVA Section 301; 42 U.S.C. Section 15481. This section requires that all voting systems used in an election for Federal office meet or exceed these requirements. States

could use HAVA funding to purchase voting systems that meet or exceed these requirements. A chart showing the funds distributed to each State is found on EAC's Web site, www.eac.gov.

In addition, HAVA also required EAC to develop guidelines for testing voting systems and required EAC to establish a program for the testing of voting systems using federally accredited laboratories. These guidelines and testing and accreditation processes establish a means to determine whether voting systems meet the base-line requirements of HAVA and the more descriptive and demanding standards of the voluntary voting system guidelines developed by EAC. This process provides assurance to election officials and members of the public that the voting systems that they use will perform in a manner that is accurate, reliable, accessible and auditable.

Voluntary Voting System Guidelines (VVSG)

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 develop voluntary testing standards.

History of Voting System Standards and Guidelines

The first set of national voting system standards (VSS) was created in 1990 by the Federal Election Commission (FEC). In 2002, FEC updated the standards and HAVA mandated that EAC develop a new iteration of the standards—which would be known as the Voluntary Voting System Guidelines (*VVSG*)—to address advancements in information security and computer technologies as well as improve usability.

HAVA mandated a 9-month period for the TGDC to develop the initial set of *VVSG*. The TGDC, working with NIST, technology experts, accessibility experts, and election officials, completed the first draft and delivered it to EAC in May 2005. In addition to providing technical support to the TGDC, NIST also reviewed the 2002 Voting System Standards (2002 VSS) to identify issues to be addressed in the 2005 guidelines, drafted core functional requirements, categorized requirements into related groups of functionality, identified security gaps, provided recommendations for implementing a voter-verifiable paper audit trail, and provided usability requirements. NIST also updated the *VVSG*'s conformance clause and glossary.

On December 13, 2005, EAC adopted the first iteration of the Voluntary Voting System

Standards (VVSG). Before the adoption of the VVSG, EAC conducted a thorough and transparent public comment process. After conducting an initial review of the draft *VVSG*, EAC released the two-volume proposed guidelines for public comment for a period of 90 days; during this period, EAC received more than 6,000 comments. Each comment was reviewed and considered before the document was finalized and adopted. The agency also held public hearings about the *VVSG* in New York City, NY, Pasadena, CA, and Denver, CO.

The *VVSG* was an initial update to the 2002 Voting System Standards focusing primarily on improving the standards for accessibility, usability and security. The *VVSG* also establishes the testing methods for assessing whether a voting system meets the guidelines. In many areas, these guidelines provide more information and guidance than HAVA. For example, these testing guidelines incorporated standards for reviewing voting systems equipped with voter verifiable paper audit trails (VVPAT) in recognition of the many States that now require this technology. Likewise, in the area of accessibility, the guidelines require that if the VVPAT is used as the official ballot, the paper record be made accessible to persons with disabilities, including persons with visual impairments or disabilities. Volume I of the *VVSG, Voting System Performance Guidelines,* includes new voluntary requirements for accessibility, usability, voting system software distribution, system setup validation, and wireless communications. It provides an overview of the voluntary requirements for independent verification systems, including voluntary requirements for a voter-verified paper audit trail for States that require this feature for their voting systems. Volume I also includes the requirement that all voting system vendors submit software to a national repository, which will allow local election officials to make sure the voting system software that they purchase is the same software that was certified.

Volume II of the *VVSG, National Certification Testing Guidelines,* describes the components of the national certification testing process for voting systems, which will be performed by independent voting system test labs accredited by EAC. EAC is mandated by HAVA to develop a national program to accredit test laboratories and certify, decertify, and recertify voting systems. The *VVSG* and the comments received from the public about the guidelines are available at www.eac.gov.

The Future of the Voluntary Voting System Guidelines

Significant work remains to be done to fully develop a comprehensive set of guidelines and testing methods for assessing voting systems and to ensure that they keep pace with technological advances. TGDC and NIST have been working since the development of the initial iteration of the VVSG in 2005 to revise that version and to completely review and update the 2002 Voting System Standards that were developed by the FEC. The next iteration of the VVSG, which EAC anticipates receiving from TGDC sometime later this year, will include the following elements:

- Software independence – use of verifiable voting records for independent audits;
- Prohibition of RF wireless;
- A process to include new and innovative voting systems with greater usability, accessibility, and security;
- Improved methods for measuring reliability and accuracy of voting systems;
- Improved and updated usability and accessibility requirements;
- Improved requirements for the overall reliability of voter verifiable paper audit trail voting systems.

In addition to this work, NIST is working to develop a uniform set of test methods that can be applied to the testing of voting equipment. Currently, accredited laboratories develop their own test methods to test voting equipment. After the completion of these uniform test methods, every accredited lab will use the same test to determine if a voting system conforms to the *VVSG*. This is a long and arduous process as test methods must be developed for each type and make of voting system. Work is beginning in 2007 on these methods, but will likely take several years to complete.

Voting system testing and certification and laboratory accreditation program

Accreditation of Voting System Testing Laboratories

HAVA Section 231 requires EAC and NIST to develop a national program for accrediting voting system testing laboratories. The National Voluntary Laboratory Accreditation Program (NVLAP) of NIST provides for the initial screening and evaluation of testing laboratories and will perform periodic re-evaluation to verify that the labs continue to meet the accreditation criteria. When NIST has determined that a lab is competent to test systems, the NIST director recommends to EAC that a lab be accredited. EAC then makes the determination to accredit the lab. EAC issues an accreditation certificate to approved labs, maintains a register of accredited labs and posts this information on its Web site.

HAVA required that NIST deliver its first set of recommended labs to the EAC "[n]ot later than 6 months after the Commission first adopts the voluntary voting system guidelines." See HAVA Section 231(b), 42 U.S.C. 15371(b). This deadline passed in June 2006. Four laboratories applied to NIST for evaluation prior to the HAVA deadline, but the required technical reviews and on-site assessments were not completed by the deadline. The first set of NIST recommended laboratories were not received by the EAC until January 18, 2007. EAC conducted additional review of the laboratories' conflict of interest policies, organizational structure, and record keeping protocols. This review was

conducted efficiently, so that EAC could move forward with accrediting the first voting system testing laboratories under its new program. The first two laboratories were accredited by EAC at its public meeting on February 21, 2007. These two labs are now accredited to test to the 2005 VSS.

The Need for EAC Interim Accreditation of Laboratories

Obviously, the need for EAC to provide accredited laboratories arose well before NIST's January 18 recommendation. First, toward the end of 2005, NIST informed the EAC that the expected timeline to complete required document collection and review, pre-assessment and formal on-site assessments of applicants made it highly unlikely that it would be able to provide a list of recommended laboratories before the end of 2006. This determination made it clear that the EAC would need to have an alternative, temporary process in place to provide accredited laboratories if it wished to implement its certification program in time for the 2006 election. Furthermore, in July of 2006, the National Association of State Election Directors (NASED) informed EAC that the organization was terminating its voting system qualification program. NASED is a non-governmental, private organization that accredited laboratories and qualified voting systems to federal standards for more than a decade. The organization's decision to terminate its voting system qualification program just before the 2006 general election required EAC to take immediate action. Without an entity to approve required voting system modifications for the 2006 election, some state election officials would be unable to field their HAVA-compliant systems. To address these situations, EAC was compelled to do two things (1) provide for interim, temporary accreditation of testing laboratories to test to the 2002 VSS and (2) initiate a preliminary, pre-election phase of its voting system testing and certification program.[1]

EAC needed to provide 2002 VSS-accredited labs on a temporary, interim basis to ensure that the agency had the means to implement its certification program. Additionally, EAC would be compelled to implement a provisional, pre-election certification program to

[1] The pre-election phase of EAC's certification program was not originally planned, but was ultimately required to serve election officials and the public. The program began on July 24, 2006. The purpose of the pre-election phase of the program is to provide voting system manufacturers with a means to obtain a Federal Certification of voting system modifications during the vital period immediately prior to the November 2006 General Elections. Many states require a Federal or national certification as a condition of state certification. Historically, the three to four month period immediately preceding a General Election produces a number of emergent situations that require the prompt modification of voting systems. These changes are often required by state or local election officials and must be made prior to Election Day. To this end, the pre-election phase of the EAC's Certification Program was designed to meet the immediate needs of election officials from the date NASED terminated its qualification program until after the November 2006 General Election. The pre-election requirements of the certification program were narrowly tailored to meet these needs. Additionally, the pre-election phase of the program was drastically limited in scope, (1) it did not certify voting systems, just modifications and (2) the certification was provisional and, thus, expired after the November 2006 election.

replace services offered by NASED. EAC could not wait for NIST to recommend laboratories. Fortunately, HAVA provided a mechanism for EAC to take such action in Section 231(b)(2)(B). This section requires that EAC publish an explanation when accrediting a laboratory without a NIST recommendation. A notice was published on EAC's Web site (www.eac.gov) to satisfy this requirement.

EAC's Interim Accreditation Program

At a public meeting in August 2005 held in Denver, the commissioners received a staff recommendation outlining the details of the interim accreditation program. The staff recommendation included a process in which the three laboratories previously accredited by NASED – CIBER, SysTest Labs, and Wyle Laboratories – would be allowed to apply for interim accreditation. In December of 2005, EAC officially began accepting applications for a limited interim accreditation program. As stated in the letters, the purpose of the interim accreditation program was to provide accredited laboratories that could test voting systems to federal standards, until such time as NIST/NVLAP was able to present its first set of recommended laboratories. This accreditation was limited in scope to the 2002 Voluntary Voting System Standards and required the laboratory to apply to the NVLAP program with the intent to receive a permanent accreditation. The letters also sought variety of administrative information from the laboratories and required them to sign a Certification of Laboratory Conditions and Practices. This certification required the laboratories to affirm, under penalty of law, information regarding laboratory personnel, conflict of interest policies, recordkeeping, financial stability, technical capabilities, contractors, and material changes.

In order to accredit a laboratory, even on an interim basis, EAC needed to contract with a competent technical expert to serve as a laboratory assessor. EAC sought a qualified assessor with real-world experience in the testing of voting systems. The contractor reviewed each of the laboratories that applied. The review was performed in accordance with international standards, the same standards used by NVLAP and other laboratory accreditation bodies. This standard is known as International Standard ISO/IEC 17025, *General Requirements for the Competence of Testing and Calibration Laboratories*. In addition, the EAC assessor (who also currently serves as a NVLAP assessor) applied NIST Handbooks 150, *Procedures and General Requirements* and NIST Handbook 150-22, *Voting System Testing*.

CIBER, SysTest Labs, and Wyle Laboratories applied for accreditation under the interim program. Each, as required, had previously received a NASED accreditation. EAC's assessor visited each of the labs and conducted a review consistent with the standards noted above. The assessor reviewed laboratory policies, procedures and capabilities to determine if the laboratories could perform the work required. Laboratory assessments do not make conclusions regarding past laboratory work product. Two of the applicant laboratories, SysTest Laboratories, L.L.C., and Wyle Laboratories, Inc. received an

interim accreditation. The assessor's reports and EAC action regarding these laboratories are available on the EAC Web site, www.eac.gov.[2] EAC promptly published on its Web site information regarding its decision on accreditation (August and September of 2006). This notice provides some brief background on the interim accreditation process, starting with the fact that three previously NASED accredited laboratories were invited to apply to the program, including information on the program's requirements and limitations, and ending with the identity and contact information of the two laboratories accredited. Information was also electronically forwarded to EAC's list of stakeholders via e-mail. The EAC stakeholders e-mail list includes almost 900 election officials and interest groups, nationwide. Staff members for EAC oversight and appropriations committees are included in this list of stakeholders. In addition to EAC's Web site and e-mail announcements, on September 21, 2006 EAC's Executive Director reiterated the Commission's decision at a public meeting Web cast to the EAC Web site. This announcement identified the interim accredited labs by name. Furthermore, in October 26, 2006, the two interim accredited laboratories testified at EAC's nationally televised public meeting.

The Interim Accreditation Program and CIBER

The third laboratory, CIBER, has yet to satisfy the requirements of the interim accreditation program. The initial assessment of CIBER revealed a number of management, procedural and policy deficiencies that required remedial action before the laboratory could be considered for accreditation. These deficiencies are identified in the initial CIBER/Wyle report. They were also brought to the attention of CIBER's President of Federal Solutions in a letter from EAC's Executive Director dated September 15, 2006. The letter outlines, consistent with recommendation of EAC's assessor, the steps the laboratory must take to achieve compliance. The letter requires CIBER to:

a. *Assign resources, adopt policies and implement systems for developing standardized tests to be used in evaluating the functionality of voting systems and voting system software. Neither ITA Practices, CIBER nor any of its partners will be permitted to rely on test plans suggested by a voting system manufacturer.*

b. *Assign resources, adopt policies and implement systems for quality review and control of all tests performed on voting systems and the report of results from those tests. This shall include provisions to assure that all required tests have been performed by ITA Practices, CIBER or its accredited partner lab.*

[2] Note: The Wyle and CIBER assessments were completed as a joint report. The two labs have a cooperative agreement to work together in testing voting systems (Wyle performing hardware testing and CIBER software testing).

Finally, the letter required an additional "follow-up" assessment of the laboratory.

The follow-up assessment of CIBER was performed by EAC's assessor in December of 2006. The findings of this assessment were documented in a report, which is available on the EAC Web site. In the findings, the assessor recognized significant changes CIBER had made to its program in response to the initial assessment, including new policies regarding test procedures, management and personnel. The report also noted a number of non-conformities that had yet to be addressed by the laboratory.

In a letter dated January 3, 2007, CIBER provided a written response to EAC's follow-up assessment and report. The response sought to address the deficiencies noted in the December assessment. Additionally, CIBER officials requested a meeting with EAC staff to discuss their January 3 response. This meeting took place at EAC on January 10, 2007. At the meeting, EAC staff informed CIBER that their report could not serve as the basis of accreditation because it failed to resolve all outstanding issues. A number of CIBER responses to noted deficiencies were listed as "TBD." EAC's assessor and Certification Program Director formally reviewed CIBER's response. EAC provided CIBER notice of the deficiencies that remained outstanding and informed them of the steps they must take to come into compliance by a letter dated February 1, 2007. Due to the fact that the purpose and usefulness of the interim accreditation program came to a close, EAC allowed CIBER 30 days in which to document their full compliance. After that time, the program was closed and no further assessment actions will be performed under the interim program. CIBER was notified of this procedure by letter dated January 26, 2007, and on February 8, 2007, EAC voted to close its interim laboratory accreditation program effective March 5, 2007.

Information related to CIBER's status in the EAC interim accreditation program was not released prior to January 26, 2007. It was EAC's belief, consistent with NVLAP policy, that it would be improper to release information regarding an incomplete assessment. However, on January 25, 2007, CIBER took the affirmative action of making this information available to a third party, the New York State Board of Elections. With this action, CIBER made the information public and EAC believed it was incumbent to provide this information to the entire public, not just the New York State Board of Elections. As such, on January 26, 2007, EAC posted on its Web site (www.eac.gov) assessment reports, correspondence, and responses from CIBER related to their progress in the EAC interim accreditation program.

Since that time, EAC has received an additional response from CIBER. That response is currently being reviewed by our assessor. Based upon the assessor's recommendation, EAC will act to accredit or to decline to accredit CIBER to test to the 2002 VSS under EAC's interim laboratory accreditation program. It is important to note, however, that this action, even if it results in accrediting CIBER to the 2002 VSS, **will not**

automatically make CIBER eligible to test to the 2005 VVSG. CIBER's application for 2005 VVSG accreditation is pending before NVLAP. Until EAC receives a recommendation from NVLAP that CIBER should be accredited to the 2005 VVSG, CIBER **will not** be accredited to test to those standards and will not therefore possess the accreditation desired by New York to test voting systems for their purchase. New York law requires that voting systems purchase in that state are tested to the 2005 VVSG. As noted above, there are currently two laboratories accredited under the joint NVLAP/EAC program that are qualified to test to the 2005 VVSG.

Voting System Certification

In 2007, EAC assumed the responsibility of certifying voting systems according to national testing guidelines. Previously, the National Association of State Election Directors (NASED) qualified voting systems to both the 1990 and 2002 Voting System Standards. EAC's certification process constitutes the Federal government's first efforts to standardize the voting system industry.

In July 2006, EAC implemented its pre-election certification program, which only focused on reviewing changes or modifications that were necessary for modifications to systems that would be used during the November 2006 elections. Three modifications were reviewed and approved under the pre-election program. Those modifications were approved only conditionally. The condition was that the authorization for the modification expired after the 2006 election. After that, no modification will be considered unless the entire system has already received an EAC certification.

In October 2006, EAC published for public comment its post-election certification program. This program encompasses an expanded and detailed review of voting systems, utilizing accredited laboratories and technical reviewers. EAC received over 400 comments during the public comment period. At a public meeting on December 7, 2006, EAC adopted its Voting System Certification Program, which became effective on January 1, 2007. Since that time, nine manufacturers have registered to participate in the EAC program. The registration process is antecedent and required prior to a manufacturer submitting a system for testing. Currently, nine manufacturers are registered with EAC. A list of registered manufacturers is available at www.eac.gov.

Once the manufacturer is registered, it may submit systems for testing to an EAC-accredited testing laboratory. Reports from that laboratory's assessment are provided to EAC for review and action. The reports are reviewed by EAC technical reviewers. If the report is in order and the system is in conformance with the applicable voting system standards or guidelines, the technical reviewers will recommend that EAC grant the system certification. EAC's executive director will consider the recommendation and make the final decision regarding certification. Once certified, a system may bear an EAC certification sticker and may be marketed as having obtained EAC certification.

The EAC's certification process includes assessment of quality control, field monitoring, decertification of voting systems, and enhanced public access to certification information. For more information concerning EAC's Voting System Testing and Certification Program, see the program manual for this program, which is available on the EAC Web site, www.eac.gov.

Federal Process Adds Transparency and Accountability

The implementation of EAC's Laboratory Accreditation Program and Voting System Testing and Certification Program mark the first time that the Federal government has funded and tested both laboratories and voting systems. Both of these processes were previously conducted by NASED in a collaborative and voluntary effort. The Federal government's involvement in these processes will shed light on the rigorous process that ensures that our nation's voting systems are accurate, reliable and ready for service in any election. Unlike our predecessors, EAC is obligated to conduct accreditation and certification processes that are open and that share information about the results of those tests with the public. EAC has developed its programs with the knowledge that public confidence is critical to the election process and that public confidence comes from public knowledge and understanding of the process. Information about EAC accredited laboratories is available on EAC's Web site, www.eac.gov. Similarly, information about EAC's testing and certification program and any systems that have been tested through that program also will be available on the EAC Web site.

THE VOTING PROCESS

Once a State or local election jurisdiction has purchased a new voting system, there is still a great deal of work to be done to assure that elections are conducted properly. Purchasing the right system is in many ways the easy part. Using it properly takes time, planning, and persistent attention to detail.

Election officials must keep in mind that in order to successfully compromise a voting system during an election, a person must have knowledge of the system and access to the system while the election is taking place – a scenario that applies to ballot boxes or e-voting machines. Any discussion or policy about implementing a secure voting system must examine all aspects of the voting process. The bottom line is that real security for any type of voting system – electronic or paper-based – comes from systematic preparation. State officials should ensure that they:

- Prepare systems to prevent tampering;
- Prepare people to detect tampering;
- Prepare poll workers and law enforcement to react to tampering; and
- Prepare election officials to recover by auditing and investigating tampering.

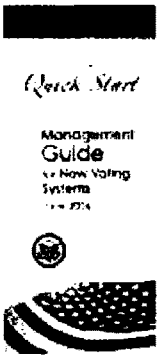
These fundamental election administration processes to protect the entire voting process will always be important, even as voting technology evolves. Focusing solely on the reliability of voting systems is not enough, and a Federal certification for the system cannot take the place of solid, thorough management procedures at the State and local levels to ensure the system is managed, tested, and operated properly. Achieving accurate and reliable election results will always be the combination of thorough testing of the equipment, training and resources for election officials and poll workers, and through election management guidelines for every aspect of election administration.

Management Guidelines

EAC is working to assist States and local election jurisdictions with identifying and managing all of the details surrounding the successful administration of elections. In 2005, EAC began work on a comprehensive set of management guidelines, collaborating with a group of experienced State and local election officials to provide subject matter expertise and to help develop the guidelines. The project focuses on developing procedures related to the use of voting equipment and procedures for all other aspects of the election administration process. These publications are intended to be a companion to the *VVSG* and assist States and local election jurisdictions with the appropriate implementation and management of their voting systems. The first set of election management guidelines will be completed in FY 2007; they will be available to all election officials to incorporate these procedures at the State and local levels.

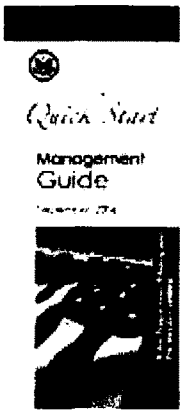
Four *Quick Start Guides* were distributed to election officials prior to the 2006 election. These guides are summaries of more extensive chapters of the Management Guidelines that will be released this year. The guides were sent to election officials throughout the nation and covered topics such as introducing a new voting system, ballot preparation, voting system security, and poll worker training. All *Quick Start* guides are available at www.eac.gov. A brief description of each *Quick Start* guide is provided below.

Quick Start Guide for New Voting Systems



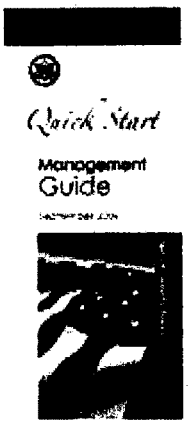
The guide provides a snapshot of processes and procedures election officials should use when introducing a new voting system. It covers receiving and testing of equipment; implementation tips, such as conducting a mock election and developing contingency plans; and programming. The guide also offers Election Day management strategies, including opening the polls, processing voters, and closing the polls.

Quick Start Guide for Ballot Preparation/ Printing and Pre-Election Testing



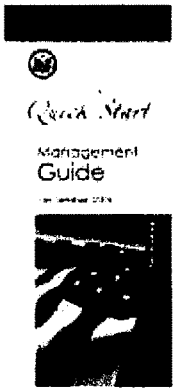
Ballot preparation and logic and accuracy testing are essential steps to ensure Election Day runs smoothly. The guide offers tips on preparing and printing ballots, which includes confirming that ballots conform to all applicable State laws as well as requiring a multilayered ballot proofing process at each stage of the design and production process. The guide also covers pre-election testing for hardware and software logic and accuracy.

Quick Start Guide for Voting System Security



The introduction of new equipment also ushered in concerns regarding voting system security. To address some of those concerns and to help election officials implement effective management procedures, the guide highlights priority items essential to securing these systems. It addresses software security, advising officials to be sure that the software installed on the systems is the exact version that has been certified. The guide advises officials to not install any software other than the voting system software on the vote tabulating computer; to verify that the voting system is not connected to any network outside the control of the election office; and to consider any results transmitted electronically to be unofficial and verify them against results contained on the media that are physically transported to the central office. Also included in the guide are recommendations regarding password maintenance, physical security, personnel security, and procedures to secure the equipment.

Quick Start Guide for Poll Workers



One of the most challenging tasks for election officials is recruiting and training poll workers. The guide contains information about identifying potential poll workers, effective training programs and techniques, as well as procedures to implement on Election Day.

A full range of Management Guideline documents will be developed to cover topics related to election administration, including:

- Pre-Election Testing

- Ballot Design
- Contingency/Disaster Planning
- Vote by Mail/Absentee Voting
- Military/Overseas Voting
- Polling Place/Vote Center Management

In addition, new *Quick Start* guides are planned for 2007, including guides on the following topics:

- Change Management
- Public Relations
- Contingency/Disaster Planning
- Certification
- Developing an Audit Trail

Proper management of elections is key to conducting a reliable, accurate, open and accessible election. Buying state of the art voting equipment with the latest security features is meaningless unless the door to the storehouse where the voting systems are kept is secured and locked. Similarly, equipment used to program voting systems should never be connected to the Internet. It is EAC's goal to communicate these suggestions and requirements to the election officials to help them increase the security and accuracy of their voting equipment by their practices and procedures.

CONCLUSION

Elections are a complex equation of people, equipment and processes. All three pieces work together to ensure a successful, accurate and reliable election. HAVA was careful to address them all. And, EAC is working diligently to provide States with the tools that they need to purchase accurate and reliable voting systems, to implement those systems in a secure environment, and to assure that election officials, poll workers and voters are trained on how to use the voting equipment accurately and effectively.

EAC appreciates the opportunity to provide this testimony. If you have any questions, I will be happy to address them.

Mr. CLAY. Thank you so much, Ms. Davidson, for your testimony. Mr. Skall, you may proceed.

STATEMENT OF MARK W. SKALL

Mr. SKALL. Thank you. Chairman Clay and members of the subcommittee, thank you for the opportunity to testify today. I am Mark W. Skall, chief of the Software Diagnostics and Conformance Testing Division of NIST, part of the Technology Administration of the Department of Commerce. I will discuss NIST's role in voluntary voting systems, guidelines and testing.

Some of the major items assigned to NIST by HAVA included sharing and providing technical support to the Technical Guidelines Development Committee [TGDC], in order to develop voluntary voting system guidelines and conducting an evaluation of independent non-Federal laboratories, in order to submit to the EAC a list of those laboratories that NIST proposes to be accredited by the EAC to test voting systems.

These voluntary voting system guidelines [VVSG], contain requirements for vendors when developing voting systems, and for laboratories when testing whether the systems meet the requirements of the guidelines.

The TDGC provides technical direction to NIST in the form of TDGC resolutions and reviews, and approves research material written by NIST researchers. The TDGC ultimately is responsible for approving the guidelines and submitting them to the EAC.

HAVA provided for the creation of the TDGC and mandated that the first set of recommendations for voluntary voting system guidelines be delivered to the EAC 9 months after the final creation of the TDGC.

To meet this very aggressive schedule, NIST and the TDGC conducted workshops, meeting, 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.

These guidelines built upon the strengths of the previous voting system standards, enhanced areas needing improvement, and included new material, primarily in usability, accessibility and security.

The resultant document, now known as the VVSG 2005, was delivered on schedule to the EAC in May 2005.

Immediately after completing its work on the VVSG 2005, NIST and the TDGC began working on the next iteration of the VVSG which is currently planned for delivery to the EAC in July 2007.

The new VVSG will be a larger, more comprehensive standard, with much more thorough treatment of security areas and requirements for equipment reliability. This VVSG will include updated requirements for accessibility and requirements for usability based on performance benchmarks. It prohibits radio frequency wireless communications, which includes the use of common wireless local area networks.

In December 2006, the TDGC approved a resolution to include requirements in the VVSG only for those voting systems that are software independent. This essentially means that the voting sys-

tem can be audited through the use of voter-verified paper records, so that election fraud and errors that would result in changes to election outcomes can be reliably detected.

To encourage innovations in voting systems that could produce more usable, accessible and reliable designs, the new VVSG will include an innovation class. Some innovations resulting from this class could result in secure voting systems that do not rely on voter-verified paper records.

NIST is also developing open, comprehensive test suites, so that the requirements in the draft VVSG can be tested uniformly and consistently by all of the testing labs.

NIST has been directed to recommend qualified testing laboratories to the EAC for accreditation. In order to accomplish this, NIST is utilizing its National Voluntary Laboratory Accreditation Program [NVLAP]. Simply stated, NVLAP offers an unbiased third party evaluation and formal recognition that a laboratory is competent to carry out specific tests or calibrations.

NIST first accredits voting system testing laboratories according to NVLAP's criteria and then recommends them to the EAC.

In January 2007, NIST proposed that high Beta Quality Assurance and SysTest Labs be accredited by the EAC under the provisions of HAVA. Currently, NVLAP is proceeding with the evaluation of five other laboratory applicants.

In conclusion, NIST is pleased to be working on this matter of national importance with our EAC and TDGC partners. Thank you for the opportunity to testify. I would be happy to answer any questions the subcommittee might have.

[The prepared statement of Mr. Skall follows:]

Testimony of

Mark W. Skall
Chief, Software Diagnostics and Conformance Testing Division

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

Before the

House of Representatives
Committee on Oversight and Government Reform
Subcommittee on Information Policy, Census, and National Archives

"National Institute of Standards and Technology's Role in Voluntary Voting System Guidelines and Testing"

May 7, 2007

Introduction

Chairman Clay, Ranking Member Turner, and members of the subcommittee, thank you for the opportunity to testify today on "NIST's Role in Voluntary Voting System Guidelines and Testing."

I will begin my testimony by reviewing NIST's role in meeting the requirements of the Help America Vote Act (HAVA) 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 of 2005 (the VVSG 2005). As part of that discussion I will describe the major areas of change between the VVSG 2005 and its precursor, the 2002 Voting Systems Standard (VSS). I will also discuss our current efforts in voting, which center on producing the next iteration of the VVSG and producing an associated set of comprehensive test suites. 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

NIST plays a significant role in the HAVA of 2002. HAVA provided for the creation of the Technical Guidelines Development Committee (TGDC) and mandated that the TGDC provide its first set of recommendations of voluntary voting system guidelines 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, on an on-going basis, an evaluation of independent, non-Federal laboratories and to submit to the EAC a list of those laboratories that NIST proposes to be accredited.

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

2005 VVSG and Prior Voting System Standards

I will now discuss NIST's role in producing the VVSG 2005. As part of that discussion, I will include a brief history of the voting systems standards prior to the VVSG 2005 and will address how the VVSG 2005 differs from those versions.

The VVSG 2005 was built upon the strengths of the previous voting systems standards, which were promulgated by the Federal Election Commission (FEC). In 1984, Congress appropriated funds for the FEC to develop voluntary national standards for computer-based voting systems. This resulted in the production of the first set of voting system standards, which is generally referred to as the 1990 VSS, and a national testing effort for voting systems.

The national testing effort was developed and overseen by the National Association of State Election Director's (NASED) Voting Systems Board, which was composed of election officials and independent technical advisors. The 1990 VSS was subsequently revised, beginning in 1999, to reflect the then current needs of the election community. This resulted in the 2002 VSS.

HAVA subsequently mandated that a new set of voting system 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 privacy, 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.

How the VVSG 2005 Differs from the 2002 VSS

The VVSG 2005 enhanced areas of the 2002 VSS that needed improvement and included new material. The new material added more formalism and precision to the requirements using constructs and language commonly used in rigorous, well-specified standards. This

included 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 in the VVSG 2005 focused primarily on usability, accessibility, and security. The usability section included requirements on voting system controls, displays, font sizes, lighting, and response times. It also required voting systems to alert voters who make errors such as overvoting so as to reduce the overall number of spoiled ballots. The accessibility section was greatly expanded from the previous material and included requirements for voters with limited vision and other disabilities. It also addressed the privacy of voters who require assistive technology or alternative languages on ballots.

The VVSG 2005 included the first Federal standard for Voter Verified Paper Audit Trails (VVPAT). As you know, a majority of states (28) now require that their voting systems include a voter verified paper trail. The VVSG 2005 took no position regarding the implementation of VVPAT and neither required nor endorsed it. Thus, if states choose to implement VVPAT, the VVSG 2005's requirements help to ensure that their VVPAT systems are usable, accessible, reliable and secure. The VVSG 2005 also contained requirements to make the paper record useful to election officials for audits of voting equipment.

The new security section also contained requirements for addressing how voting system software is to be distributed. This helps ensure that states and localities receive the correct version of the tested and certified voting system. Moreover, the section also included requirements for validating the voting system setup. This enables 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 then that the use of wireless technology should be approached with extreme caution but should still be permitted in the VVSG 2005 if security measures and contingency procedures are in effect. The TGDC has subsequently concluded that, for the next iteration of the VVSG, radio frequency (RF) wireless should be prohibited entirely.

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 version approved by the EAC includes changes that the EAC made after receiving and considering public comment.

Next Iteration of the VVSG

Immediately after completing its work on the VVSG 2005, NIST and the TGDC began working on the next iteration, which is currently planned for delivery to the EAC in July 2007.

This new VVSG builds upon the VVSG 2005 but takes a fresh look at many of the requirements. The new VVSG will be a larger, more comprehensive standard, with more thorough treatments of security areas and requirements for equipment integrity and reliability. The new VVSG will include updated requirements for accessibility and requirements for usability based on performance benchmarks. It will include updated requirements for data and documentation for testing laboratories. It will include a number of updated requirements dealing with voting equipment reliability, and will include many new requirements for improved security. As noted, it will prohibit radio frequency wireless communications, which includes the use of wireless local area networks. The requirements will be structured so as to improve their clarity to vendors and their testability by testing labs.

In December 2006, the TGDC approved a resolution to include requirements in the new VVSG only for those voting systems that are "software independent." A voting system is software-independent if a previously undetected change or error in its software cannot cause an undetectable change or error in an election outcome. This means essentially that the system can be audited through the use of voter-verified paper records (VVPR) so that election fraud and errors that would result in changes to election outcomes can be reliably detected. The voting systems today that meet the requirements for software independence include optical scan and VVPAT.

However, the TGDC has recognized that innovations in voting systems that could produce more usable, accessible, and reliable designs need to be encouraged. Some innovations could result in secure voting systems that do not rely on VVPR, or that use VVPR in ways that are more convenient and simple for voters and election officials to handle. To that end, the TGDC will be including an Innovation Class in the new VVSG to assist in the eventual conformance of potential innovative voting system submissions.

NIST is developing an open, comprehensive set of test suites so that the requirements in the new VVSG can be tested uniformly and consistently by all of the testing laboratories. NIST's development of this comprehensive set of test suites is a major undertaking and will add significantly to the confidence that voting systems laboratories are able to test voting systems correctly. Test suite development is planned to continue through 2007 and 2008. NIST plans to release the tests in stages.

Laboratory Accreditation

I will conclude my remarks with a status report on NIST's third major responsibility under HAVA, laboratory evaluation. NIST has been directed to recommend qualified testing laboratories to the EAC for accreditation so that the laboratories may then test voting systems under the EAC's Voting System Certification Program. To accomplish this, NIST is utilizing its National Voluntary Laboratory Accreditation Program (NVLAP). NVLAP is a voluntary, fee-supported program to accredit laboratories that are found competent to perform specific sorts of tests or calibrations. NVLAP procedures are codified in the Code of Federal Regulations (CFR, Title 15, Part 285).

Simply stated, NVLAP offers an unbiased third party evaluation and formal recognition that a laboratory is competent to carry out specific tests or calibrations. Expert technical assessors conduct a thorough evaluation of all aspects of laboratory operation that affect the production of test data, using recognized criteria and procedures. General criteria are based on the international standard ISO/IEC 17025, *General requirements for the competence of testing and calibration laboratories*, which is used for evaluating laboratories throughout the world. Laboratory accreditation bodies use this standard specifically to assess factors relevant to a laboratory's ability to produce precise, accurate test data, including the technical competence of staff, validity and appropriateness of test methods, testing and quality assurance of test and calibration data.

With regard to voting systems, NIST relies on NVLAP to first accredit voting system testing laboratories according to NVLAP's criteria, and then recommends them to the EAC. The EAC makes the final decision to accredit laboratories under the Commission's full voting system testing laboratory accreditation program based upon the information provided by NIST and the Commission's review of non-technical issues such as conflict-of-interest policies, organizational structure and record-keeping protocols. After the EAC accreditation, voting system vendors can then contract with these laboratories to test voting systems for the EAC's certification program.

Those laboratories seeking accreditation by NVLAP and subsequent recommendation to the EAC are required to meet the general NVLAP criteria for accreditation and demonstrate that they are competent to test voting systems according to the requirements of the 2002 VSS and the VVSG 2005. Rigorous onsite assessments must be conducted and laboratories undergoing assessment must resolve any identified nonconformities before NIST will recommend a laboratory to the EAC. NVLAP assessments have paid particular attention to determining laboratory competence to test to new material included in the VVSG 2005 on voting system usability, accessibility and security.

To ensure continued compliance with NVLAP requirements, voting system testing laboratories undergo an onsite assessment before initial accreditation, then during the first renewal year, and then every two years thereafter to evaluate their ongoing compliance with specific accreditation criteria.

In January, 2007, NIST informed the EAC that it had completed a comprehensive technical evaluation of the competence of two laboratories to test voting systems to Federal standards and proposed that iBeta Quality Assurance and SysTest Labs be accredited by the EAC under the provisions of HAVA. The letter to the EAC, and its attachment, can be viewed at http://vote.nist.gov/LabRec.htm.

Currently, NVLAP is proceeding with the evaluation of five other applicant laboratories: InfoGard Laboratories, Inc.; Aspect Labs, a division of BKP Security Labs; Wyle Laboratories; Ciber Labs; and atsec information security corporation.

NIST recognizes that transparency is the key to building public trust and confidence in voting systems. To that end, we have posted a document that addresses related questions

on the same website that explains the details of the NVLAP evaluation process for voting system testing laboratories. In addition, for each laboratory NIST has recommended to the EAC, we have publicly posted the assessment report and the laboratory's detailed response to that report at http://vote.nist.gov/LabRec.htm. These reports contain substantial detail that underlies the basis for NIST's recommendation.

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 Subcommittee might have.

Mr. CLAY. Thank you so much, Mr. Skall.

We will now proceed to the questioning period under the 5-minute rule, and I will start with Ms. Davidson.

Ms. Davidson, I am aware of your background in the area of systems certification, through your work as Secretary of State in Colorado, and through the National Association of State Election Directors.

With this expertise, I am hopeful that you can offer some explanation and potential solutions. What activities have the Technical Guidelines Development Committee of the EAC, in concert with NIST, and the vendor community, undertaken to bring uniformity to the accreditation process of certification labs?

Where is the EAC in determining whether to reinstate the labs that lost their interim accreditation in 2006?

Ms. DAVIDSON. Currently, Mr. Chair, we have set up a temporary process to get us through the last year's election, to make sure that we were able to test just software, not systems, because of State laws changing, or maybe a piece of equipment failed and needed some software change, and the other issue is a name of a ballot came off, or the court case. So State law, that type of thing, would cause that. We had three that was tested, only three minor changes. In that process, we said that underneath what the—and we did this at a public meeting in August 2005, where our Standards Board and our Advisory Boards were there, and we went through the process of saying this is what we will do if we cannot get laboratories that have been recommended by NIST/NVLAP process.

Because of their thorough process, we were told that it was going to take over a year to get them through the process. It is a very thorough process, to get it really worked through. So in January, we allowed the three labs that NSLAP had actually accredited as independent test labs, and we allowed them to qualify, you know, to actually register to go through the steps and the procedures.

In that, two labs were named, in October, and they testified in a public meeting that we had. So there was a public meeting with the two labs that had met that criteria, it was SysTest and it was Wyle.

At that time, CIBER had applied, they also applied, but they had not met all of the requirements that we felt they should. We went through the same process that was set up by NVLAP with NIST, and really tried to make sure that the labs would meet the needs that we needed. And this was only to 2002 requirements, not to 2005.

We weren't checking voting systems, only the software in that time. So we are still in the process with CIBER. If they meet that, you know, that interim process. But at this time, if they do not meet that, and we expect to have that, you know, information before too long, then they'll continue going through the NVLAP process and trying to meet their letter from Dr. Jeffries to us from the NIST Foundation, to come to us and recommend that they would be accredited. They are one of the five labs that have registered, that has not gone through the full process with NVLAP at this time.

Does that answer your question thoroughly enough?

Mr. CLAY. Well, wait a minute now. Are you comfortable with the other two labs that have gained certification? Are you confident that they are doing what is necessary to check these systems throughout the country?

Ms. DAVIDSON. The two labs that have the accreditation, now the full accreditation, because we received a letter in January from NIST, recommending that we accreditate SysTest, which was one of those labs, and the other one is iBeta, and those labs have gone through the whole process, through NIST, and with that process I think Congress was very wise in putting NIST in control of that, because they go through that process with all different kinds of labs. They are really very qualified to do that.

So in moving forward, yes, I feel that our labs will be able to test to the standards that have been developed, and they currently—because we did not grandfather anything in—they can test to 2002 or 2005.

The equipment that is out there right now have the recommendation from the NASED association, which was a volunteer association, no Federal money. So the two labs that are there now, yes, I feel that they definitely can.

And one of the things that we do is any time we set new standards, NVLAP will go back out to make sure that they meet that, and in our requirements, we also put that we can go into the labs at any time and verify the process they are using, to make sure that they are doing the job correctly.

Mr. CLAY. Thank you for such a thorough answer. Let me ask one more and then I will turn it over to Representative Maloney.

What is the commission doing about the system flaws that were reported during the 2006 election cycle? In particular, what will it do with reports of significant flaws or failures in systems certified under NASED for 2007 and 2008 election cycle? Will the commission decertify NASED systems, if warranted?

Ms. DAVIDSON. In our process, they have to go through our process for us to be able to decertify. But one of the things that we are doing is if there is something that has come in for certification, as we said, we have five different systems that is in now, if that is one of them that had issues, we have sent that manufacturer a letter, asking them if they are addressing that in the new process that they have gone through with the test labs.

So that the laboratories will be aware of it, and any time we get anything from the States, if the system is going through it we make the laboratories aware of what the issues are.

So we are definitely making sure that if they are going through our process, we feel that we have authority at that time.

Mr. CLAY. So you all actually report to the certification board, to NIST, if there are flaws or problems, and they are brought to your attention?

Ms. DAVIDSON. We will certify to the laboratories themself, if we are aware of any problem, so that they can check, too, what the problems—whether it is a State or whether it is an issue that has been, you know, really gone through a process some other way, we will definitely notify the labs of the issues.

Mr. CLAY. Thank you for that response.

Representative Maloney, please proceed.

Mrs. MALONEY. Thank you.

I would like to start with Mr. Skall, and if you would like to also answer, Ms. Davidson, and thank you very much. for being here, for all your hard work, both of you.

Considering that CIBER certified 70 percent of the machines in use last November, and that now they have been suspended for inadequate certification and testing, we have a huge challenge in front of us. Do we keep using machines that were certified by the ITA, or testing labs that did not meet the standards for accreditation? Or do we have to start over and recertify? What are we going to do with those 70 percent that—Mr. Skall?

Mr. SKALL. Thank you. Now of course at NIST, we are a technical agency and don't make policy decisions like that. I guess we are very lucky not to be in that situation. But I will give you my perspective from a technical analysis.

Mrs. MALONEY. Yes.

Mr. SKALL. Making sure that voting systems work correctly is a very complex process. It starts with a standard. You can only test for the most part. You can do some testing outside of the standard. You could look through the source code and find security glitches.

But the vast array of detailed testing is what we call functional testing, and it starts with having a comprehensive well-specified standard. So in my opinion, until you actually have really precise, detailed standards in place, which have tremendously precise and accurate requirements for security and accessibility, it is very difficult to get systems tested thoroughly. So the first step is to have the standards in place.

Mrs. MALONEY. Do we have those standards in place now?

Mr. SKALL. We have one standard in place, the 2005 standard. We are about to deliver to the EAC the much more comprehensive standard. We are planning to deliver that to the EAC in July 2007.

Mrs. MALONEY. So you are going to come out with it. See, what happens, though—and I just have to jump ahead—you keep improving the standards, and then, if the States go out and buy these machines, then they have to totally change them to the new standard. So that is a problem for States, and so could you address that.

Mr. SKALL. Yes; absolutely.

HAVA mandated that we produce the first set of voluntary voting system guidelines in 9 months. By definition, that meant we can only do an incremental update to the existing standards.

We knew, right away, that we needed a more comprehensive standard. The one in 2007 is the comprehensive standard. I don't have any plans, and I do not believe the EAC does, to change that standard for a long, long time. This will be the standard in place for many, many years.

It won't be a moving target. It is the one that is going to have all the requirements that we and the TDGC felt were necessary.

Mrs. MALONEY. And that will be in place. And where specifically does it change from the 2005 standard?

Mr. SKALL. Oh, it is much more comprehensive in the areas of security, access, control, cryptographic requirements, what I mentioned before, software independence, which allows for the voter to verify his or her vote. This concept of an innovation class, which is going to allow, hopefully in the future, for automated solutions

to voter verification, much more detailed requirements in usability for performance benchmarks, to allow much more innovative designs to meet the performance benchmarks, reliability, accuracy, tremendously—much more comprehensive.

Mrs. MALONEY. Sounds great. But based on your statement, then, we haven't really scientifically certified these 70 percent of machines that are being used.

So I guess the question goes to the policymaker. Ms. Davidson, are we going to keep using machines that were certified by the ITA, that did not meet the standards for accreditation, or do we have to start all over?

Ms. DAVIDSON. We felt like we had to start over.

Mrs. MALONEY. So you're starting all over to recertify them.

Ms. DAVIDSON. In January, we asked all the vendors, they had letters to all of them, asking them to come back in and be retested, because as you have stated, most of the States are using equipment that is 2002, meets those guidelines and not the 2005, because of the deadline that was set in HAVA.

So many of the States have purchased that equipment and we feel that it does need to be retested, and if they want our seal—it is a volunteer program—but if the States want the seal, where then we can go back and decertify if there is issues, we have asked for that equipment to come in.

We have five that has already got their equipment in, we expect many more, we expect another lab, within just a short time, from NVLAP. They are also through. So we are moving forward. We feel it has to go through the process that we have set up.

Mrs. MALONEY. OK. Is there any reason—again I'll start with Mr. Skall—why the testing process and test reports should be done in secret? Why shouldn't the public be able to verify that testing was done properly?

And we have some of these vendors saying everything we do has to be in secret. Well, how in the world do you certify that they're doing it properly? So my question is, is there any reason why the testing process and test reports should be done in secret?

Mr. SKALL. Again, let me give the technical answer to that. Right now, the problem, in my opinion, from a technical standpoint is there is no uniform set of tests with all the labs, publicly available uniform set of tests. Labs develop their own tests, they're proprietary, whether they should be proprietary or not I guess is a legal and policy question, but what we're doing at NIST is developing, starting in fiscal year 2007, a comprehensive set of test suites that all the labs can use. They will be publicly available, there will be tremendous transparency, and once this test suite is done——

Mrs. MALONEY. OK. Let's go to another point. Why should the labs be doing the testing? That's like the fox in the chicken house. I mean, why should the manufacturers be doing this testing? They have been certifying—or it is changing now, money is going to go to EAC and then go to the labs——

Mr. SKALL. Yes. So you are getting into the question of whether, in fact, the vendor should pay the test labs to do testing. Again, it's—would you like to——

Mrs. MALONEY. So do you see any reason, once we come out with a uniform set of tests, that this testing should be done in secret? Is there any reason why——

Mr. SKALL. Oh, no, it should not be done in secret, and, in fact, there will not be initial proprietary test suites, because we will develop them, they will be in the public domain, they will be completely open for everyone to see.

Mrs. MALONEY. That is great news. That is great news. Ms. Davidson, would you like to respond?

Ms. DAVIDSON. The one thing I believe I would like to add is we do support, that Congress gives us authority to collect the money, and then whether it is by lot, or whatever the case may be, we set up a procedure and it is an open procedure. We have hearings on issues that we bring into procedures.

So there would be a process set up where we would collect the money and then the lab would be selected for that manufacturer or vendor.

So we see that would improve it, because it is a conflict, and there is a lot of the public that is very concerned about it as well as us.

Mrs. MALONEY. I ask the chairman, may I have an additional 2 minutes to ask a question.

Mr. CLAY. Please proceed.

Mrs. MALONEY. OK. I would like to ask Commissioner Davidson, and Mr. Skall, if you would like to comment, in Section 202 of HAVA, Congress tasked the EAC with serving as a clearinghouse of information on the experiences of State and local governments in implementing the guidelines and in operating voter systems, in general.

And when a security vulnerability or a system flaw is revealed, or when your assessor determined that the main testing lab is not testing adequately, why hasn't the EAC made every effort to share this information with election officials and the public, restoring the trust of the American voter should not be a public relations effort. The trust of the American public must be earned through transparency and accountability, and if you are—you're tasked to be a clearinghouse, but I have heard concerns that this type of information, when it comes in, does not get sent out to the election officials and to the public.

Ms. DAVIDSON. Currently, the EAC is reviewing how we can move forward, because, you know, when we get things from third parties, if it is not coming from the State, how do we make sure that it's reliable information and correct information? And that is one of the things we feel is a responsibility of the EAC, that is, make sure that it is correct.

We thought about setting up a review panel. We have given consideration, you know, how do we, you know, actually walk through this process? Because it will happen in the future.

Mrs. MALONEY. But Commissioner, if a report comes in from a State election official, I mean, that is a pretty serious thing, and the question is why are you not sharing that with other State election officials? Maybe they would not have bought some of these faulty machines, if they knew some of the problems that were coming in from other States.

We want to get good machines out there and a good system out there. So if information's coming into the clearinghouse, I would say it is true, you have to verify that it is true. But if it is coming in from a State election official, from a Secretary of State or whatever, this is a very serious piece of information and what I am being told is that you are not sharing it with other States, the election officials or the public.

Ms. DAVIDSON. We have taken the position, now that we have started certifying, yes, that type of information will be shared, and because I mean, we have just now——

Mrs. MALONEY. Now you will be sharing it. OK.

Ms. DAVIDSON. That is right. That is correct. If it comes from a Secretary of State, and if it comes from a county official, we feel like we have to, beyond the ground and see if that—what was the issue with that? Because many times, whether it was a poll worker, whether it was actually somebody that did the setup of the election—you know, we have to make sure whether it is a machine problem, what, but report whatever that issue might be.

Mrs. MALONEY. And last, Commissioner, was there any communication between the White House and the EAC concerning the release of the voter fraud, voter intimidation report, or any of the other reports that have been submitted to the EAC?

Ms. DAVIDSON. Because of everything that was brought up in that, and, you know, it is such a hotly contested issue, we have asked our Inspector General to do a full audit of our process and of those reports, and to give a report and we would be more than happy to give you that once that is done. We also will be changing——

Mrs. MALONEY. When do you expect that to be done?

Ms. DAVIDSON. You know, they haven't given us a timetable but I would say, hopefully, it's done within a month.

Mrs. MALONEY. Within a month. But the question, was there any communication between the White House and the EAC? That is a simple question.

Ms. DAVIDSON. Yes. Not that I know of, but, you know, I know that they have kind—they have put a gag order on us talking to anybody else within our own office. So for me to ask somebody, I—you know, they are going through all of our e-mails, they are going through all the records, paper records, everything, to see if there was any communication with—whether it was a Congress Member or whether it was the White House.

Mrs. MALONEY. Do you know of any communication with DOG, the FEC or the RNC?

Ms. DAVIDSON. I am not aware of any.

Mrs. MALONEY. Thank you.

Mr. CLAY. Thank you, Representative.

Mrs. MALONEY. By the way, Mr. Skall, would you like to comment on the clearinghouse question of information? This is a concern that many State governments have brought to Mr. Clay and myself, that they want this information coming out from the clearinghouse, that they were tasked by HAVA.

Could you comment on that aspect.

Mr. SKALL. You know, again, as sort of the technical arm of developing the standards and tests, it's just not an area we have much expertise in.

Mrs. MALONEY. All right. Thank you very much for your testimony and thank you for your work.

Mr. CLAY. Thank you.

Mrs. MALONEY. Both of you. Thank you.

Mr. CLAY. Mr. Skall, let me ask you, are there time limits for labs to address problems found during the pre-assessment, assessment or monitoring phases of accreditation? What steps does NIST take if these time limits are not met?

Mr. SKALL. No; there are no time limits. The way NVLAP works is the NVLAP accreditation very much depends on the readiness of the labs. Some labs are further along, some labs are not very far along, and it takes them a lot of time to do remedial type actions to get up to speed, and NVLAP will not issue an accreditation until we are 100 percent confident that the lab can perform its services.

So in the procedures there is no time limit, that we ask the labs to move faster, because we want them to do it correctly.

Mr. CLAY. Thank you.

Ms. Davidson, can you explain the rationale by the EAC to exempt off-the-shelf products from the VVSG guidelines for testing of certification purposes, since so much of the software and components used in voting systems are COTS products. Isn't there an effective way to evaluate these products?

Ms. DAVIDSON. You know, I think that the technical portion of your question Mr. Skall should answer. Really——

Mr. CLAY. I'll go back to him and let me hear what the rationale is from EAC.

Ms. DAVIDSON. All right. We actually are doing exactly what the standards are saying, the voluntary voting system standards, that we don't take a position because we feel that is an independent body, the Technical Guidelines Committee setting up what the guidelines should be in those arenas, and we have not taken a position on that ourselves as an EAC.

Mr. CLAY. OK. Mr. Skall, is there an effective way to evaluate these products?

Mr. SKALL. Yes. The COTS, commonly called COTS, commercial off-the-shelf systems, has had an exemption, a limited exemption throughout the history of voting standards. The reason for this exemption—and the exemption has to do—it is not a total exemption, they are tested, but some aspects of the source code are not tested mainly because we can't acquire them.

Typically Microsoft, for instance, and other large commercial off-the-shelf vendors are not going to give their source code. That's a tremendous proprietary interest to them and they will not give out and make public their source code. So there are limitations in what we can acquire.

We, in the VVSG 2007, are really tightening this loophole. We are looking much more closely at which types of systems get exemptions and we are limiting the type of exemptions. So we are going to test these systems as much as possible within the confines of the amount of source code we can get.

Mr. CLAY. Thank you for that. I would like to hear some of your thoughts on the new VVSG guidelines that are scheduled to go into effect at the end of this year.

I think we all agree that a good certification process is meaningless, if the standards being used are incomplete.

What is the status of development for the 2007 Voluntary Voting System Guidelines? And are there any major topics, originally planned for this edition, that will be deferred to a later version of the guidelines?

Mr. SKALL. Yes. Let me first say, I agree 100 percent. We look at the viability of software and hardware as sort of a three-legged stool. You have the standards, you have the tests, and then you have the implementation, in this case the voting system, and if one of those legs falls over, the whole system falls over.

So you need a good standard, you need good tests, and then you need a good implementation based on that.

The VVSG 2007, as I mentioned before, is very comprehensive. We are on schedule to complete it. There is nothing that I know of, that will not be in the VVSG 2007, that we want to be there. So it will be a complete standard. Now we may discover in the future, there are more minor things, and those can be added by probably maintenance to the standard.

But there are no major areas or functionality I know of, that will be missing.

Mr. CLAY. Ms. Davidson, would you like to comment.

Ms. DAVIDSON. Yes, sir. I certainly would. I appreciate that. Once they are delivered, by law, to the EAC, we have to publish that in a public register, at least for 90 days. The last one, we got 6,500 comments that had to be vetted. From the time it was delivered to the EAC to the time that it was adopted, that was July, I believe, or it was delivered in May 2000, it took until the middle of December to get that actually vetted, and we feel this process will take longer.

We feel we need to have some open meetings. We are not sure what it is going to take the manufacturers in building this new equipment. This, as Mr. Skall has discussed, is very complex, and adds a lot of details to the voting equipment. It is the future of voting systems.

How long will it take to develop that? Also we need to know from the State officials and county officials in a hearing, what kind of timeframe are we looking at, that you would be replacing equipment? And how long do we need to consider our 2005, like you said, you can't constantly require States to purchase new equipment.

We need to get information from them. This needs to be a very public process. We need to hear from the advocacy community. So as we move forward in this process, we expect it to take some time because it has to be vetted, the public has to have their right to input in public meetings, and here in public meetings, and being able to send in their comments to the EAC.

So we will work with NIST, as we did last time, once these comments come in, to make sure that the best produce comes out, because we want the very same thing that you want. We want reliability. We want our elections to be a success in the future.

Mr. CLAY. Thank you for that response.

Ms. Davidson, since New York failed to procure new systems by 2006, it is my understanding that they will lose approximately $50 million in HAVA funds.

Due to the circumstances facing New York, will the EAC be offering the State a waiver to use the funds, once their technical concerns are satisfied? And if not, why not?

Also, can you tell us if there are other States that might not have spent their HAVA funds due to concerns over the accreditation and certification processes.

Ms. DAVIDSON. You know, we follow the law. Right now, the law says they have to return the money but we are aware that there is a bill, as mentioned by the Congresswoman, that they would be able to keep that money and obviously, with that going through the process, we would not be moving forward with that.

I kind of feel like the Congresswoman. I think that is going to be a process that gives us ability in the law, that says that States that did not spend their money can retain it. I think it's until 2008, is what is in the bill currently. But we will follow the law.

The law is what is there but, obviously, we try to make ourselves always aware of new legislation.

Mr. CLAY. So right now, the commission couldn't administratively give the waiver to the State of New York or——

Ms. DAVIDSON. We cannot give the waiver but, obviously, we know that there is a process moving forward, so we have not sent out any letters.

Mr. CLAY. Are there any other States that are also kind of caught in limbo as far as the certification process?

Ms. DAVIDSON. As far as other States, they are not caught in limbo. They have bought equipment, but maybe one county didn't, like in Pennsylvania, I believe there is one county, one individual county, so they were going to have to return back a very small amount.

There is other States, Arkansas, that has to return a very small amount. But New York is the big area, that they didn't move forward and buy equipment, and so it was because of other issues, that some of the others didn't purchase equipment.

Mr. CLAY. In New York's case, they didn't move forward because they were cautious, because they wanted to make sure they got this done correctly, I mean, and I'm sure we will make the case for this State in Congress. But I mean, you do understand that they moved very cautiously, which I can appreciate it. I think others can too.

Ms. DAVIDSON. We definitely understand their position. We asked for reports from States, like the law asks us to, and we have a full list, if you want that, of States, what kind of funds they still have out there, because it does affect more than one State, when you're passing that legislation.

Mr. CLAY. Sure. We would love to see the list and if you could provide to the subcommittee.

Ms. DAVIDSON. OK.

Representative Maloney, any other questions for this panel?

Mrs. MALONEY. Very briefly. I just wanted to comment on your statement, Commissioner Davidson, that ultimately it is a human hand and human accountability. I looked at one machine that

Smartmatic manufactured under the Sequoia name, and they literally had a yellow button on the back of the machine where you could change the vote. It was unbelievable.

So when I inquired, what do you do to make sure that someone's not changing the vote on the back of the machine? and the answer was, well, we will have people watching to make sure that no one is changing the vote on the back of the machine.

So I feel that we should not have machines like Sequoia's yellow button you can change, but that there still has to be a human element, and I hope Mr. Skall's guidelines will help remove the need for that. I have been in some New York elections where absolutely every voting machine has had a citizen-watcher to make sure that everything is done properly.

But back to your statement that everything should be public. When a system fails a test, there is no public announcement. Wouldn't that be helpful for the public and for Mr. Skall, and others, to know that this system has failed? And then, ultimately, when you test, you are testing to standards. What about the hackers? It is the hackers that are getting into these machines.

There are reports in the paper that one from Princeton hacked in, and you're not really testing to prevent the hackers from getting in there and doing their thing.

Your response?

Ms. DAVIDSON. Well, currently, the only ones that we are aware of, that has been hacked into, has been at Princeton in a lab, and not in a polling location. We are not aware of any equipment being hacked into on election day.

Mrs. MALONEY. But that is the point. You are not aware of anyone hacking in. It doesn't mean that someone hasn't hacked in, and the testing doesn't really prevent hacking or look at the hacking approach. It looks at the standards and tests the standards as opposed to how a hacker goes in and sees what's missing and how to get in there.

I mean, since we haven't tested against hackers, we don't really know whether they have gotten in on election day or any other time.

Ms. DAVIDSON. And I think that is the reason why NIST and the TDGC has definitely put a lot of area into security and going into cryptographics as Mr. Skall mentioned.

That is why the new guidelines has really gone into that area. But, you know, I think you're going to get a far more detailed answer from Mr. Skall than from myself, if you would like.

Mrs. MALONEY. But on a policy statement, when a system fails a test I'm told there is no public announcement. Maybe that is the type of thing that should go into the clearinghouse, so that election officials across the country will know what systems are failing and why, and be on the alert for it.

So my question is when a system fails a test, there is no public announcement. Why not? Why aren't we putting that in the clearinghouse and getting it out to election officials?

Ms. DAVIDSON. As I stated before, that will be a process that we are looking at, is how do we get it out, how do we make sure it's reliable. As you said, if it comes from a State or election official, it needs to be out there.

And we will also, it has been our policy to, we do a newsletter, and the newsletter also goes to our oversight committees on the Hill, and we try to make that available not only to election officials in the Nation but our oversight. I believe that NIST is on. We add anybody that would like to be put on to our list for our newsletter.

Mrs. MALONEY. Thank you.

Mr. Skall, on the hacking question, how do we know they haven't hacked in on election day, if we're not testing antihacking——

Mr. SKALL. OK. Let me answer that in a couple of ways. We are testing security requirements. So the standard itself, the new standard will have something called requirements for open-ended vulnerability testing.

This is precisely to check, to see whether, in fact, hackers have hacked in. Now it is well beyond the state-of-the-art to prove and to be certain that someone hasn't hacked in, just like it is beyond the state-of-the-art to prove the software works correctly. You can't prove it. You can only get an indication of reliability and of security.

So we will have more comprehensive tests. There are some tests now, the examination of source codes, for that very reason. We will have more tests, more requirements.

Can we be sure someone has not hacked in? No. Will we have a better feel, a better confidence that they haven't? Yes.

So we're at the point where we can be more comprehensive but we can never be sure, and we never will be able to.

Mrs. MALONEY. My time is up. I want to thank both of you. I would also like to comment that Congress is very concerned about moving forward with helping overseas residents vote, and helping our men and women in the military vote, and that is something that we'll possibly be looking at at a later time, because as we go into more of a global economy, many of our Americans are living overseas and they report they are having difficulty voting. So that is another concern.

Anyway, thank you very much for coming and thank you for all your hard work.

Mr. SKALL. Thank you.

Ms. DAVIDSON. Thank you.

Mr. CLAY. Thank you, Representative Maloney, and that will conclude the testimony for panel one.

Thank you, Ms. Davidson, and thank you, Mr. Skall, for your testimony and you may be excused.

I would like to now invite our second panel of witnesses to come forward and then we will take a recess. Voting systems from a variety of important perspectives.

Mr. Douglas Kellner, co-chair of the New York State Board of Elections, an attorney at the law firm of Kellner Herlihy, Getty and Friedman. Welcome.

Mr. David Wagner, professor of computer science at the University of California at Berkeley. Thank you for making the trip, sir.

Mr. Lawrence Norden of the Brennan Center for Justice at New York University School of Law. Thank you for being here.

And Mr. John Washburn, software quality consultant and member of the VoteTrustUSA Voting Technology Task Force.

And Mr. Mac J. Slingerlend, president and CEO of CIBER, Inc., located in Denver, CO.

Gentlemen, welcome to all of you. In addition, I understand that Mr. Slingerlend is accompanied by CIBER, Inc.'s vice president for contracts, Mr. John Pope, and thank you for being here.

It is the policy of the Committee on Oversight and Government Reform to swear in all witnesses before they testify. At this time I would like to ask all of the witnesses to stand and raise your right hands. Mr. Pope, you intend to speak on the record. I would like you to join the invited witnesses in being sworn.

[Witnesses sworn.]

Mr. CLAY. Thank you, and let the record reflect that all of the witnesses answered in the affirmative. I will now ask all of you to give an oral summary of your testimony and to keep the summary under 5 minutes in duration.

Your complete written testimony will be included in the hearing record, and Mr. Kellner, we will begin with you.

STATEMENTS OF DOUGLAS A. KELLNER, CO-CHAIR, NEW YORK STATE BOARD OF EDUCATION; DR. DAVID WAGNER, ASSOCIATE PROFESSOR, COMPUTER SCIENCE DIVISION, UNIVERSITY OF CALIFORNIA, BERKELEY; LAWRENCE NORDEN, BRENNAN CENTER FOR JUSTICE, NEW YORK UNIVERSITY SCHOOL OF LAW; JOHN WASHBURN, VOTETRUSTUSA VOTING TECHNOLOGY TASK FORCE; AND MAC J. SLINGERLEND, PRESIDENT AND CEO, CIBER, INC., ACCOMPANIED BY JOHN POPE, VICE PRESIDENT FOR CONTRACTS

STATEMENT OF DOUGLAS A. KELLNER

Mr. KELLNER. Thank you, Congressman. I thank you for calling us to testify today. I have read some of the statements that you have made at prior hearings, and I am grateful, because I believe that you do understand, very well, the issues that we need to address in order to assure that we have uniform, accurate, transparent, and verifiable elections. And I also thank Congress Member Maloney who has also worked so hard on this issue, and for her contribution on this, particularly in shedding light on Sequoia Pacific earlier this year and the fine work that she has been doing.

I believe that since it is clear to me that you understand the fundamentals, I will skip that part of my testimony and go directly to what we have done in New York.

The key thing is that we can have all these fine principles about how elections should be done, and I endorse the principles involved in the Voter Confidence and Increased Accessibility Act of 2007, H.R. 811, which is sponsored by Congressman Holt, because those are important principles to assure that we have verifiable and transparent elections.

But I add the caveat, that we have to pay careful attention to the timetable for implementation of any new law, that good intentions alone do not make wise legislation. That the timing for implementation of new voting systems and HAVA was fundamentally flawed by putting the cart before the horse. We required States to replace their punch card and lever voting machines before setting the standards for new voting systems.

And as we have heard the testimony from NIST, and from the EAC, that none of the systems that are in use today have been certified to the 2005 standards that have been set by the Election Assistance Commission, let alone the 2007 standards which are still in development.

And what New York has found is that the system for certifying under the 2002 standards, which were very weak and very summary, itself was flawed, and that there is good reason to question all of the 2002 certifications that were made by NASED.

And specifically, what have we found on this? Well, I pointed out that in the process of New York adopting its own independent testing process, that we learned that ES&S, which is one of the major suppliers of election systems throughout the country, came to New York and said we want a waiver from the 2005 standards with respect to source code, and the reason you should give us that waiver is that there was no change in that particular requirement from the 2002 standards and we got certification from NASED under those standards. So why should you make us comply now?

Well, that raised questions in my mind, and I went and inquired, well, how is it that they didn't comply with the 2002 standard and still got certification?

The answer is nobody knows. That in asking the NASED officials who were in charge of the certification process, they said, well, we got a report from CIBER that recommended certification, and there was nothing in that report that indicated that they were not in compliance with all of the applicable standards.

And then we go back and, in fact, the States that purchased this equipment were relying on the NASED certification, that relied on CIBER, and CIBER never reported the fact that they had not even tested for that particular requirement with respect to the source code.

So that is one piece of evidence questioning the 2002 certification standards.

The second thing is that we had these reports that Congress Member Maloney referred to before, where computer scientists at Princeton showed how they could hack into the Diebold optical scanning system. Computer scientists at the University of Connecticut did it from a different approach and also showed the vulnerability of the system.

The Maryland election authorities had commissioned a study also, that showed the security vulnerabilities. And these reports show that, again, that Diebold scanning system was certified to the 2002 standards, even though none of the security requirements in the 2002 standards had been tested, again by CIBER, that did the independent testing report that was given to NASED, and NASED certified that Diebold scanning system as well as other Diebold—the Diebold DREs share the same types of flaws, as pointed out in these studies, and they were certified to those 2002 standards which themselves were inadequate, even though there was no testing for those particular requirements under those standards.

Now as Commissioner Davidson has indicated, the EAC does not decertify equipment that was certified by the National Association of State Election Directors. They only decertify equipment that they themselves have certified.

So the bottom line is, is that most of the equipment that is in use in this country now, has never been properly certified, and the certification process that is in place now, to the 2002 standards, is meaningless.

Now at this time, not a single voting system has been certified to the 2005 standards and there is only one system, at least according to the EAC Web site, that has even applied for certification to the 2005 standards. The other five applications are all to the old 2002 standards.

So we really do have a crisis, in the sense that the voting equipment that is in use now does not meet current standards, and if Congress is going to require States to upgrade their voting equipment, and I certainly support that process, and I support what Congressman Holt is trying to do in H.R. 811, we have to first make sure, that before we spend all this money, we're spending it for equipment that needs proper standards, and that is what I would urge you to do.

In my written testimony, I have enumerated how the New York law actually incorporates a lot of these principles that Congressman Holt has in his bill. That New York already requires every voting system to produce a voter verifiable paper audit trail.

New York requires that there be an audit of the paper trail of at least 3 percent of the voting machines in each county, and authorizes the escalation of the audit to a greater number of machines where errors or the closeness of the results warrant.

New York already prohibits any device or functionality potentially capable of externally transmitting or receiving data via the Internet or radio waves, and New York requires that the manufacturer or vendor of each voting machine escrow a complete copy of all programming, source coding and software. New York is one of only two States that now has that requirement, and North Carolina, the other State, is not enforcing its requirement.

So New York will actually be the first to effectively require at least the escrow of source coding.

New York has also adopted a number of other reforms in the regulations that it has adopted, including being the only State so far to require compliance with the 2005 voter system guidelines.

New York requires every vendor to disclose all political contributions. New York requires and provides for public access to observe usability testing of the systems, and—OK.

Mr. CLAY. Mr. Kellner, we will let you summarize.

Mr. KELLNER. All right. I will wrap up, Congressman. So the bottom line is that to emphasize that there is no voting system on the market today that complies with the current Federal standards, and that you can't on the adequacy of the old certification, and that Congress should keep that in mind as it requires jurisdictions to upgrade their voting equipment.

[The prepared statement of Mr. Kellner follows:]

Neil W. Kelleher
Co-Chair

Helena Moses Donohue
Commissioner

Peter S. Kosinski
Co-Executive Director

40 STEUBEN STREET
ALBANY, N.Y. 12207-2108
Phone: 518/474-6220
www.elections.state.ny.us

Douglas A. Kellner
Co-Chair

Evelyn J. Aquila
Commissioner

Stanley L. Zalen
Co-Executive Director

Committee on Oversight and Government Reform,
Subcommittee on Information Policy, Census, and National Archives

United States House of Representatives

Statement of

Douglas A. Kellner

Co-Chair, New York State Board of Elections

May 7, 2007

I thank the Committee for this opportunity to present my observations concerning the state of voting technology and New York's efforts to implement the Help America Vote Act.

There are four overriding precepts that should govern the administration of elections in a democracy. Election administration should be uniform, accurate, transparent and verifiable. It is worthwhile to spend a moment on each of these concepts.

Uniformity — All voters and candidates should be treated alike. While the principle sounds simple, it can often be difficult to accomplish. All voters should have reasonable access to exercise their right to vote. All candidates should be confident in the knowledge that they have won or lost an election that was conducted openly and honestly

Accuracy — There is little argument that election results should be as accurate as possible in reflecting the voters' intent in selecting candidates. It order to attain accurate results, it is essential that voting systems be secure from tampering. It is just as essential that the voting system is reliable so that we can all be confident that the result reported does reflect how voters actually intended to cast their ballots. We should remember that there are many more incompetent programmers than talented hackers. Poor ballot design and programming errors can have significant impacts that can raise legitimate concerns whether the certified election results actually reflect the decisions of the voters. Although most of the debate over security issues has been framed to target suspicion on outside hackers and backdoors, it is in fact insiders who have the keys to the front door and complete access to the electronic ballot box. Hackers are less danger than insiders with only few minutes access to the voting equipment. These vulnerabilities to

the integrity of many voting systems widely used throughout the country were illustrated in several studies that have been released in the last two years.[i]

Transparency and Verifiability — Every step in the process of election administration should be observable by voters, candidates and public-minded citizens and organizations. We should ban the word "trust" from the vocabulary of election administration. The concern over so called "black box voting" is that neither the public nor the voter can be certain that a voter's ballot is actually going to be recorded and counted as the voter intended. We must guard against delegating to a very small group of computer and statistical experts who have access the responsibility for verifying the integrity of elections.

Twenty years ago there was an outcry by democracy advocates against the old Mexican system where the paper ballots were taken to election offices and counted in secret by the election officials appointed by the ruling party. While Mexico changed its process so that everyone could observe the ballot count, in this country we have gone in the opposite direction where the vote count has often been entrusted to computers and those who have programmed them. Instead we must make the process of counting votes transparent and provide for public verification of those results. When election monitors are denied access to the programming and source code that actually counts the votes, it is impossible to verify that the vote was cast in the manner intended by the voter. That is why it is absolutely essential that any electronic voting system have a paper trail that can be verified by the voter. Of course, that paper trail is meaningless unless it is actually audited to confirm that the machine count matches the paper verified by the voter.

I have read the very eloquent statement that Congressman Clay delivered to this subcommittee on July 20, 2004.[ii] It shows that members of Congress do understand these fundamental precepts and the problems that we must address to assure uniform, accurate, transparent and verifiable elections. I also appreciate the substantial effort that Congresswoman Maloney has invested in improving the integrity of our election process.

It is with these precepts in mind that I support the principles of HR 811, the Voter Confidence and Increased Accessibility Act of 2007, with the caveat that Congress must be realistic about the timetable for implementation of any new law.

New York State Should Be Proud of Its Leadership by *Responsibly* Implementing the Help America Vote Act.

Good intentions alone do not make wise legislation. The timing for the implementation of new voting systems in the Help America Vote Act was fundamentally flawed by putting the cart before the horse. Congress provided funding for the replacement of punch cards and lever voting machines before setting the standards for new voting systems. There were substantial delays in forming and funding the new Election Assistance Commission. Many states blindly rushed to comply with the hurried timetable established by HAVA—with disastrous consequences in many states. More than 35 states have experienced substantial problems at the polls that have

disenfranchised and inconvenienced far more voters than the problems of punch cards and lever machines that Congress sought to remedy.

The US Election Assistance Commission, established under HAVA, was not formed until a year after the statute was enacted. This delay contributed to the EAC's failure to meet a January 1, 2004 deadline for issuing new voting systems standards. The EAC did not adopt these standards until December 2005. At that time, the EAC grandfathered all previously certified voting systems until January 1, 2008. Although that date is only seven months away, the EAC has not certified a single voting system to those standards. Indeed, only one vendor, Dominion Voting, a Canadian company, has even applied for certification under the 2005 Voluntary Voting System Guidelines.

New York is committed to complying with HAVA. But we are also committed to doing it once and to get it right the first time, without impairing anyone's right to vote by a flawed implementation plan.

The New York Legislature adopted the Election Modernization and Reform Act of 2005, (Chapter 181 of the Laws of New York for 2005) cognizant of the raging debate over the accuracy, transparency and verifiability of electronic voting systems. The New York law allows our county boards of elections to choose to purchase precinct-based optical scanners or direct recording electronic voting systems, but only after those voting systems have been tested and certified to standards that assure the accuracy and verifiability of those voting systems.

The New York law addressed many of the key issues that Congress is now considering in HR 811, the Voter Confidence and Increased Accessibility Act of 2007.

- New York requires that every voting system produce a voter verifiable paper audit trail (NY Election Law § 7-202(1)(j))
- New York requires that there be an audit of the paper trail of at least 3% of the voting machines in each county, and authorizes the escalation of the audit to a greater number of machines where errors or the closeness of the results warrant. (NY Election Law § 9-211)
- New York prohibits any device or functionality potentially capable of externally transmitting or receiving data via the Internet or radio waves or other wireless means. (NY Election Law § 7-202(1)(t));
- New York requires that the manufacturer and/or vendor of each voting machine, system or equipment place into escrow a complete copy of all programming, source coding and software. (NY Election Law § 7-208).

The regulations adopted by the New York State Board of Elections to implement the New York Election Modernization and Reform Act also contain a number of positive features that have formed a model for other states: [iii]

- New York was the first state to require compliance with the 2005 Voluntary Voting System Guidelines adopted by the US Election Assistance Commission;

- New York requires that each voting system vendor and its key personnel disclose all political contributions;
- New York provides for public access to observe usability testing of the voting systems in the certification process and provides public access to all test plans and test results, except where disclosure would compromise the security features of the voting system;
- New York requires that vendors disclose all litigation and any problems experienced by the voting system in other jurisdictions, so we can learn from those problems and not repeat them here.
- New York requires that vendors disclose any pecuniary interest in the laboratories that test their products.

Both the Legislature and the New York State Board of Elections were aware that this was an ambitious undertaking in adopting these progressive reforms to assure accurate, transparent and verifiable elections, but, like Congress, we certainly underestimated the difficulty of the challenge.

We initially inquired whether the vendors would be able to comply with the new legal and regulatory requirements and we were assured that they could comply. Because the Election Assistance Commission had not certified any testing authority, New York retained CIBER, the testing authority for more than 70% of the voting equipment now used throughout the United States. Nevertheless, when we commenced the testing process, it became rapidly apparent that none of the vendors was able to make a complete submission of all of the documentation; testing also revealed that none of the systems complied with all of the applicable standards.

The National Certification Process Has Been Scandalously Flawed

New York also stumbled upon another remarkable finding. Not only were the voting systems unable to comply with the 2005 Voting System Guidelines, but voting systems that had been previously certified by the National Association of State Election Directors as complying with its 2002 Voting System Standards, also in fact, failed to comply with all of those standards.

On December 14, 2006, ES&S requested that New York waive its requirement that the ES&S Unity 3.0.1.1 optical scanner be excused from compliance with the standard contained in Volume I, section 5.2.3(b) of the 2005 Voluntary Voting System Guidelines. ES&S's argument was that the standard was unchanged from the 2002 Voting System Standards, and the National Association of State Election Directors had already certified the voting system.[iv] When I investigated further, I learned that NASED never indicated that it had waived compliance with this requirement; indeed, NASED officials said that they never were aware of the non-conformance because there was no note of the issue in the report prepared by CIBER, the independent testing authority.

The academic reports that I mentioned earlier[v] have identified many deficiencies that make electronic voting systems vulnerable to hostile programming that can change the voting results, yet those systems received certification. Further investigation has demonstrated that the relevant provisions of the Voting System Standards were never considered in the testing and certification process![vi] Professor Wagner's testimony today enumerates the gross inadequacies of the certification process. I subscribe to all of his comments. The current federal certification process, even after recent changes adopted by the US Election Assistance Commission, lacks transparency and is driven by inherent conflicts of interest. No state, indeed no voter can rely on this flawed process. That is why states like New York and California have been forced to try to create their own certification process.

New York State also confronted another problem in December of 2006. Most New York officials learned that the Election Assistance Commission had not approved CIBER's interim application for accreditation as an independent testing authority. They learned this by reading the New York Times, not by any notification from the Election Assistance Commission. Remarkably, when New York inquired about the reasons for the delay in accreditation, neither CIBER nor the Election Assistance Commission would provide the information. Public disclosure of the inadequacies in CIBER's testing process only occurred after New York threatened to subpoena the information.

While Professor Wagner has addressed many important issues relating to certification, I want to add two others.

While many complain about the profits of voting machine vendors, I do not subscribe to those complaints. In fact, the cost of proper certification testing can be substantial, particularly when it is borne by just one state, even a state as large as New York. We have already spent more than $3 million on the testing process, which is only partially completed. This is a very substantial sum for a vendor to pay without any commitment that its voting system would be purchased. Indeed, at least one vendor, Open Voting Solutions based in Brookhaven, New York has told us that this cost is an insuperable barrier for a small company that believes that it has innovative solutions that it cannot finance without a purchase commitment. In an effort to address this cost, the New York Legislature recently appropriated $5 million for the costs of preparing test plans that will not be charged to the vendors. In the end the public must pay for certification testing. It is better to do this directly by a legislative appropriation than to charge the vendor, who must ultimately include that cost when it seeks to sell voting equipment to the boards of elections.

My other observation is that New York chose to engage the services of independent technical expertise to provide independent validation of the performance of its testing authority. Those of us at the New York State Board of Elections humbly recognized that we did not have the technical resources to interpret the adequacy of the test plans proposed by CIBER. New York retained NYSTEC, the New York State Technical Enterprise Corporation, based in Rome, New York, to provide that independent technical expertise. Many in the verified voting community argued that we were making

a mistake because NYSTEC did not have any experience in dealing with election applications. They could not have been more wrong. Because NYSTEC was not blinded by the flawed prior practices in testing voting equipment, it was able to apply its substantial expertise from other applications to analyze the adequacy of the proposed security testing. It offered many constructive criticisms that have led to substantial improvements in New York's testing plans.

The US Election Assistance Commission is beginning to follow this model by greater reliance on NIST, but it has a long way to go before the states and the electorate can have any confidence in the certification process.

Conclusion

There are two key lessons from New York's experience.

First, there is no voting system on the market today that has been tested and certified as being in compliance with the current federal standards.

Second, no reasonable election administrator can rely on the adequacy of certification to even the old, deficient 2002 standards.

In view of these two important issues, it is incumbent that Congress turn its attention to the process of testing and certifying voting machines. The Voter Confidence and Increased Accessibility Act of 2007 sets a worthy set of objectives and standards, but it is essential that Congress be realistic about the timetable for implementing these standards. It makes no sense to require that states spend money now to replace their voting systems before it is clear that those voting systems do, in fact, comply with the standards. There is no reason to spend substantial funds on inferior equipment that can create more problems than the reforms are intended to resolve. It is also essential that local election officials be given adequate time to avoid repetition of the substantial problems generated by hasty and poorly implemented plans to switch to new voting equipment.

---

[i] A. Kiayias, L.Michel, A. Russell and A.A. Shvartsman, *Security Assessment of the Diebold Optical Scan Voting Terminal,* (U. Conn. Voting Technology Research Center) October 30, 2006; Harri Hursti, *Critical Security Issues with Diebold Optical Scan Design,* (Black Box Voting Project) July 4, 2005 http://www.blackboxvoting.org/BBVreport.pdf
Harri Hursti, *Diebold TSx Evaluation* (Black Box Voting Project) May 11, 2006 http://blackboxvoting.org/BBVtsxstudy.pdf
Susan Pynchon, *The Harri Hursti Hack and its Importance to our Nation* (Florida Fair Elections Codification) January 21, 2006 http://www.votetrustusa.org
Ariel J. Feldman, J. Alex Halderman, and Edward W. Felten, *Security Analysis of the Diebold AccuVote-TS Voting Machine* (Princeton Univ. Center for Information Technology Policy) September 13, 2006 http://itpolicy.princeton.edu/voting/

RABA Technologies LLC, *Trusted Agent Report Diebold AccuVote-TS Voting System*, January 20, 2004 http://www.raba.com/press/TA_Report_AccuVote.pdf

[ii] http://lacyclay.house.gov/pr040722b.htm

[iii] The New York Voting Systems Standards are found at 7 NYCRR 6209, http://www.elections.state.ny.us/NYSBOE/hava/voting_systems_standards-4-20.pdf

[iv] NASED Certification #N-2-02-22-22-004 and NASED Certification #N-1-02-22-22-003.

[v] See note 1, *supra.*

[vi] Testimony of Michael Shamos before the House Committee on Science, June 2004 http://www.votetrustusa.org/index.php?option=com_content&task=view&id=1930&Itemid=26

Mr. CLAY. Thank you so much, Mr. Kellner. I would like to remind the witnesses, let's attempt to keep it at the 5-minute rule. Thank you.

Dr. Wagner, please.

STATEMENT OF DR. DAVID WAGNER

Dr. WAGNER. Chairman Clay, Representative Maloney, thank you for the opportunity to testify today.

In my research into electronic voting, I have come to the conclusion that the Federal certification process is not getting the job done. The testing labs, as we have already heard today, are failing to weed out insecure and unreliable voting systems.

The testing labs have approved systems that have lost thousands of votes, they have approved systems that are unreliable, they have approved systems with serious security vulnerabilities.

For instance, in the past few years, independent security researchers have discovered security vulnerabilities in voting systems that are used throughout the country, vulnerabilities that were not detected by State and Federal certification processes.

In my own research, I too have found serious problems in federally certified voting system, systems that remain certified and in use today.

The bottom line is election officials rely upon the Federal certification process to ensure quality; but the process has failed them.

Part of the problem is that the testing labs are not doing as good a job as they could. But part of the problem is more fundamental. Paperless voting machines are incredibly hard to certify. When we use paperless voting machines, a single flaw in the software potentially caused undetectable errors in election outcome, and that places an impossible burden on vendors in testing labs because it requires perfection.

A single overlooked defect can be enough to render the whole system insecure, unreliable or inaccurate, and experience has proven that it is easy for even the most capable experts to overlook flaws and defects in software.

Given the complexity of modern election technology, it is unreasonable to expect perfection from vendors or testing labs.

If the voting system is completely reliant upon software failures and security flaws are inevitable. Therefore, one of the best ways to solve this problem may be to reduce our reliance upon software.

Our election system must be software independent. It must not rely upon the correct functioning of software. The good news is that there are solutions to these problems. The most effective solution today is to adopt voter-verified paper records and perform routine audits of those records.

These audits provide a way to independently check whether the software has counted the votes correctly. This would reduce our reliance upon the software and, in my opinion, it would make the shortcomings of the certification process less critical.

Audits are not perfect. Because they can detect problems after the fact but cannot prevent them, we will need a certification process that is capable of weeding out problematic voting system.

In my testimony, I discuss a number of steps we could take to improve the certification process, including eliminating conflicts of

interest, increasing transparency and embracing open-ended vulnerability testing.

In particular, I would like to draw your attention to a conflict of interest in the testing process. Today, vendors choose and pay the testing labs, and this creates a perverse incentive for the labs to place the vendors' interests above the public interest.

One potential solution would be for Congress to act to give the EAC the authority it would need to collect fees from vendors, so that EAC can choose and hire testing labs itself.

As I mentioned, the good news is that solutions are available; however, the bad news is that only a minority of States have adopted these solutions. My understanding is that 27 States use voter-verified paper records throughout the State, but only 13 of them audit those records.

Adopting voter-verified paper records in routine audits, more widely, would reduce the pressure on our certification process and would provide greater transparency and confidence for voters. I believe it is the single most effective thing we could do to improve the reliability and security and trustworthiness of e-voting. Thank you.

[The prepared statement of Dr. Wagner follows:]

WRITTEN TESTIMONY OF DAVID WAGNER, PH.D.
COMPUTER SCIENCE DIVISION
UNIVERSITY OF CALIFORNIA, BERKELEY
BEFORE THE COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM,
SUBCOMMITTEE ON INFORMATION POLICY, CENSUS, AND NATIONAL ARCHIVES
U.S. HOUSE OF REPRESENTATIVES
MAY 7, 2007

Chairman Clay, Ranking Member Turner, committee members, 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 cellphones, 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 and of the Election Assistance Commission's Technical Guidelines Development Committee (TGDC)[2]. I have served as a poll worker in my county, and I served as a technical advisor to my county's equipment selection committee.

SUMMARY

We have seen dramatic changes in election technology over the past decade. This new technology was introduced for laudable reasons and has brought important benefits. However, it has come at a cost.

Many of today's electronic voting machines have security problems. The ones at greatest risk are the paperless DRE voting machines. These paperless 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.

In my research into electronic voting, I have come to the conclusion that the federal certification process is not adequate. The testing labs are failing to weed out insecure and unreliable voting systems. The federal certification process has approved systems that have lost thousands of votes, systems with reliability problems, and systems with serious security vulnerabilities. Over the past four years, independent researchers have discovered security vulnerabilities in voting machines used throughout the country—vulnerabilities that were not detected by state and federal certification processes. Unfortunately, the standards and certification process has not kept pace with the advances in election technology over the past decade.

In this testimony, I outline a number of potential directions for improving the federal certification process. I am encouraged by progress that has been made at the federal and state level, though I believe that there is more to do.

[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, the EAC, the TGDC, or any other organization. Affiliations are provided for identification purposes only.

One of the most promising directions may be to reduce our reliance upon software. With today's paperless voting machines, flaws in the software can potentially cause undetectable errors in the outcome of the election. That places an impossible burden on vendors and testing labs, because it requires perfection: a single overlooked defect can be enough to render the whole system insecure, unreliable, or inaccurate, and experience has proven that it is common for even the most capable experts to overlook flaws and defects in software. It is unreasonable to expect perfection from vendors or testing labs given the complexity of modern election technology. If the system is completely reliant upon software, failures and security flaws are inevitable.

The federal standards board recently endorsed a move towards software-independent systems. A software-independent voting system is one where undetected flaws in the software cannot cause undetectable errors in the election outcome. For instance, adopting voter-verified paper records and routine audits of those records would be one way to achieve software-independence, and it has the benefit of reducing our reliance upon the security of the software. In my opinion, software-independence would make the shortcomings of the certification process and the shortcomings of the technology less critical.

A second consequence is that the spread of electronic voting machines has degraded the transparency of our elections. Steps that once were performed by hand are now being done by computer, and votes are recorded and counted using secret, proprietary code. The secrecy surrounding the computer software makes it harder for the public to observe and exercise meaningful oversight over the administration of our elections. This loss of transparency was not intentional, but the effect is unmistakable nonetheless.

In this testimony, I outline several steps that could be taken to restore some of the transparency that has been lost in the transition to electronic voting. One of the most promising directions to improve transparency may be to conduct routine manual audits after every election and provide the public with opportunities to observe and oversee the process. This would enable robust oversight by the public at large. Ultimately, the success of our elections depends upon people, procedures, and public participation in the process.

Problems with today's systems

Federal standards call for voting machines to be tested by testing labs before the machines are certified for use. However, over the past few years we have learned that machines with reliability, security, and accuracy problems are receiving certification:

- *Lost votes.* Federally certified 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, and a re-vote in one very close statewide race was avoided only when one candidate conceded[1]. 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[2] [3], and in Orange County[4]. In Fairfax County, Virginia, election officials were surprised to discover that a voting machine was erroneously subtracting a vote for one candidate for about one out of every hundred voters who used the machine[5]. In Tarrant County, Texas, a federally certified voting system counted 100,000 votes that were never cast by voters[6].

- *Reliability flaws.* Federally certified machines have suffered from reliability flaws that could have disrupted elections. California's reliability testing found that one federally certified

voting system suffered from mechanical and software reliability problems so severe that, if it had been used in a real election, about 20% of machines would have experienced at least one failure during election day and probably would have had to be taken out of service[7].

- *Security risks.* Federally certified 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], University of California[9], Princeton[10], University of Connecticut[11], Florida State University[12]), industry consultants hired by election administrators (e.g., SAIC[13], Compuware[14], InfoSENTRY[15], and RABA[16]), and interested outsiders (e.g., Finnish researcher Harri Hursti[17] [18]). None of these flaws were caught by federal or state testing. In the past five years, at least eleven 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 testing labs. In my own research, I have found flaws in federally approved voting systems. Last year, 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 at the federal and state level[19]. 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 testing labs at any point over that nine-year period[20]. This year, I participated as part of a team commissioned by the State of Florida to examine voting software from another major vendor, and I found multiple security flaws in that system as well even though the software was federally approved[21].

All of these defects were ostensibly prohibited by federal standards[22], but the testing and federal certification process failed to weed out these problematic voting systems. The consequence of these problems is that the federal certification process is at present unable to assure that voting systems meet minimum quality standards for security, reliability, and accuracy.

It is natural to ask what we can learn from past failures of the federal certification process. These failures have exposed structural problems in the federal certification process:

- *Conflict of interest.* The testing labs are paid by and chosen by the vendors whose systems they are evaluating. Testing labs are surely aware that withholding approval too frequently might send vendors to competing testing labs with a reputation for more lenient treatment. Elsewhere in the software industry, a similar "race to the bottom" has been observed in labs that test compliance to international computer security standards[23]. Thus, the testing labs are subject to conflicts of interest that raise questions about their ability to effectively safeguard the public interest. Unfortunately, at present there are few checks and balances that can be used to hold testing labs accountable if they fail to serve the public interest.

- *Insufficient transparency.* The process lacks transparency, rendering effective public oversight difficult or impossible and making it difficult to hold vendors or testing labs accountable. Under past practices, testing lab reports were proprietary—they were considered the property of the vendor—and not open to public inspection. Also, if a voting system fails testing, that fact was revealed only to the manufacturer of that voting system. In one widely publicized incident, one Secretary of State asked a testing lab whether it had approved a particular voting system submitted to the testing lab. The testing lab refused to comply: it declined to discuss its tests with anyone other than the voting system manufacturer, citing its policy of confidentiality[24].

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.

- *Lax testing.* Testing is too lax to ensure that 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 testing labs. In my opinion, California's reliability testing methodology is superior to that mandated in the federal standards, because California tests voting equipment on a large scale and under conditions designed to simulate a real election.

- *Requirements not enforced.* 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 testing labs to use, but many of the requirements are not covered by that testing methodology. The testing labs 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"; four of the major vulnerabilities revealed in the past two years have violated this requirement—for instance, two systems were found to use weak passwords (one system "1111" used as the factory-set PIN). These requirements appear to be ignored during testing and thus have little or no force in practice.

- *The COTS loophole.* Parts of the voting software are exempt from inspection, reducing the effectiveness of 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 certification process as it currently stands.

- *Reporting loopholes.* Even if a testing lab 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 a testing lab finds a flaw that could endanger elections, but where the testing lab 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 ineffective.

- *Disincentives to scrutiny.* 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 certification 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[25]. The impasse was resolved only

when the State of Florida interceded[26]. 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[27] [28]. The disincentives to performing independent security testing at the local level heighten the impact of shortcomings in the federal standards. Fortunately, many public-minded election officials have placed the public interest first and insisted upon further scrutiny despite these disincentives.

- *No way to decertify.* Under the certification process in effect until recently, 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 federal certification process is currently in flux. Responsibility for federal certification of voting systems has transferred from NASED, a non-governmental organization that previously conducted certification on a volunteer basis, to the Election Assistance Commission (EAC), a government agency which now has responsibility for the federal certification process. The testing labs are being re-examined and re-accredited by the EAC and the National Institute of Standards (NIST). The EAC has made several incremental changes to the federal certification process. These changes are going into effect for the first time this year, so it is too early to know what effect they may have.

The federal standards are also in flux. In 2005, the EAC adopted the 2005 Voluntary Voting System Guidelines (VVSG), a set of federal standards for voting systems. The 2005 VVSG were drafted over a period of approximately three months and represent only an incremental change to the federal standards; consequently, they do not address many of the fundamental issues I describe. The 2005 VVSG did not take effect until January 1, 2007. The EAC is currently overseeing the drafting of a second revision of the federal standards, dubbed "VVSG II". The VVSG II are expected to institute more sweeping changes to the standards, and are not expected to take effect until January 1, 2010.

The effects of revisions to these standards is delayed by several factors. First, the new standards do not take effect until two years after they are published by the EAC. Second, systems that are already deployed when the new standards take effect are grandfathered. Third, systems that were certified before the new standard takes effect are grandfathered. Today, most states allow local election officials to purchase equipment that was certified to the old 2002 standards, even though the 2005 VVSG have already "taken effect." Fourth, to recoup their investment in expensive voting equipment, most jurisdictions are reluctant to replace existing systems until it is absolutely necessary. Consequently, the effect of revisions to the standards is likely to be delayed significantly. We may need to wait until the middle of the next decade before most of our voting systems are certified to the VVSG II standards.

The EAC has made progress on a number of the structural problems in the federal certification process, but some issues remain:

- *Conflict of interest.* The testing labs continue to be paid by and selected by the vendors, under the EAC's certification process. The conflict of interest remains. At present the EAC lacks the statutory authority that would be needed to eliminate the conflict of interest.

- *Transparency.* The EAC has made significant improvements to the transparency of its certification process. Test reports and related documents will be made public, which is a significant step forward. However, the effect of this change will be delayed by many years. Only new voting systems submitted to the new EAC certification process benefit from this improvement to

transparency. Existing systems—including all currently deployed voting systems—are grandfathered, and their test reports remain proprietary. Because new voting technology is expected to diffuse into the market slowly in the future, I predict that most voters will continue to vote on systems that were tested in secret for many years.

Technical information and voting system source code remains proprietary and unavailable for inspection or analysis by independent experts, under the EAC certification process.

- *Lax testing.* The 2005 VVSG do not remedy the demonstrated failures of the process to screen out insecure, unreliable, and inaccurate machines. Testing for security and reliability remains inadequate under the 2005 VVSG.

  The VVSG II are expected to adopt a more rigorous test regimen similar to California's reliability testing. This shift seems likely to significantly improve the quality of reliability testing in the future. The VVSG II are also expected to contain provisions for more rigorous security testing, but the effectiveness of these provisions will be highly dependent upon how they are implemented. The effect of these changes will be delayed by many years, because of the delays before the VVSG II take effect and before vendors submit new systems for certification under the VVSG II.

- *Enforcement of requirements.* It is too early to tell whether the EAC certification process will do a better job of enforcing the requirements in the standards.

- *COTS.* The 2005 VVSG do nothing about the COTS loophole.

  The VVSG II make significant progress on this issue. The VVSG II are expected to narrow the exemption for COTS software, and to take other steps that will address many of the concerns regarding COTS software. I am optimistic that the VVSG II will mitigate the COTS issue. However, the effect of these improvements will be delayed by many years.

- *Reporting.* In its new certification process, the EAC has eliminated the loophole regarding reporting of systems that fail the testing process. When a voting system fails the tests, this fact will be reported publicly.

- *Disincentives.* The disincentives for local election officials to scrutinize voting systems more closely are not a product of the federal standards process and cannot be eliminated at the federal level. However, the EAC is free of many of these pressures and thus is in a unique position to take a leadership role in more closely scrutinizing the reliability, security, and trustworthiness of voting technology. That has not happened so far.

- *Decertification.* The EAC has made progress on this problem. The EAC has created a process for decertifying systems that were certified under the EAC's certification process, if serious flaws are discovered in those systems. However, there is still no mechanism for decertifying systems that were certified under the prior NASED certification process. All currently deployed voting systems fall under the latter category, and thus apparently cannot be decertified by any federal process.

In the short term, these shortcomings 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 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 and increasing equipment costs.

- For the next decade or so, 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 standards. Many of the security and reliability defects described above would not have been prevented even if the 2005 standards had been in force when the machines were evaluated. Approval under the 2005 standards is not a guarantee of security or reliability.

In the long term, I am more optimistic. I expect the VVSG II to significantly improve the reliability, security, and trustworthiness of voting technology. These improvements may be delayed over a period of a decade or so, but I believe they will gradually but surely make a significant difference.

Potential ways to address certification-related shortcomings

There are several possible policy options that could be considered to address issues in the federal certification process:

- *Reduce dependence upon software.* One possibility is to reduce our dependence upon the certification process to vet voting software, by reducing our dependence upon software in elections.

  At present, the best tool we have for ensuring that votes are counted accurately is to use voter-verified paper records and perform routine manual audits of the paper records[29] [30]. Adoption of voter-verified paper records and routine audits would reduce our reliance on testing labs to ferret out security and reliability problems in the software.

  Paperless voting machines are problematic, because they demand an unachievable degree of perfection from voting machine vendors and federal testing labs. A single bug or defect in these machines can potentially cause undetectable errors in the election outcome and can potentially change the result of the election, perhaps without anyone realizing it. Given the complexity of modern voting systems, it is not reasonable to expect testing labs to eliminate the possibility of bugs or defects in voting software. This introduces the possibility that certified voting machines could be subject to failures or fraud that affect the election outcome. This risk

is exacerbated by the fact that 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-related defects. Ensuring that election results can be independently audited would go a long way to reducing our reliance upon testing labs to verify that voting software is free of material bugs or defects.

The TGDC, a body which helps to set federal voting system standards, has recently endorsed a requirement that voting systems be *software-independent*[31]. A voting system is considered software-independent if an undetected change or error in the voting software cannot cause undetectable changes or errors in the outcome of the election[32]. For instance, voting systems with a voter-verified paper record are considered software-independent, because the voter-verified paper records can be used to audit or recount the election results. Software-independence reduces the urgency of the shortcomings in the federal certification process, by reducing (but not eliminating) the impact that defects in the source code can have. In the long run, I expect this to have beneficial for election integrity.

In general, we can rate voting systems by the degree to which they rely on software:

- Paperless e-voting systems are completely dependent on the correctness of their software.
- Adding a VVPAT printer reduces the dependence on software.
- Paper-based optical scan systems reduce this dependence even further, and hand-counted paper ballots eliminate dependence on software.

Generally, the more the system depends on the correctness of its software, the greater the likelihood of reliability and security problems. Of course, software independence is just one among several considerations in the choice of a voting system.

Jurisdictions that use voter-verified paper records and routine manual audits are less dependent upon the federal certification process to identify problems. Adoption of paper ballots (whether optically scanned or manually counted) would further reduce the degree of dependence upon voting software and further reduce our reliance upon the federal certification process. While I expect the VVSG II to gradually drive a migration to software-independent voting systems over the next decade or so, the sooner that jurisdictions adopt software-independent systems, the sooner they will receive the associated benefits.

Currently, only 13 states have mandated use of these measures. (At present, 27 states mandate voter-verified paper records, another 8 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[33].) 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. This provides a fallback in case of problems with the software or the electronic record of votes cast.

- *Improve local procedures.* The most effective and practical step that local election officials could take to make existing voting systems as secure and reliable as possible for upcoming elections would be to adopt the recommendations of the Brennan Center report on e-voting. 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.

Further information may be found in the Brennan Center report[34].

- *Eliminate conflicts of interest.* Congress could enable the EAC to eliminate conflicts of interest in the federal testing process. Testing labs should not be paid by the vendors whose systems they are testing. One possible solution would be for the EAC to collect a fee from vendors, when a voting system is submitted for certification, to cover the costs of hiring testing labs to evaluate the system under consideration. This would make the testing labs more directly accountable to the EAC. At present, EAC does not have statutory authority to collect a fee from vendors[35]. If Congress were to grant EAC this authority, the EAC could address the conflict of interest.

  Vendors should not choose which testing lab will evaluate their systems. Instead, the EAC should choose the testing lab. For instance, the EAC could assign each voting system to a testing lab selected at random from the list of accredited labs.

- *Consider mandating source code disclosure.* Broader disclosure of voting system source code would help to hold testing labs accountable and allow political parties, local election officials, and interested members of the public to "get a second opinion." The secrecy surrounding voting source code is a barrier to independent evaluation of machines and contributes to distrust. Disclosing voting source code more broadly could enhance transparency, improve public oversight, and help hold vendors and testing labs accountable. As a first step, source code could be made available to election officials or to independent technical experts under appropriate nondisclosure agreements. In the long run, source code could 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 is not an effective security strategy: 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 could lead to improvements to voting system security.

  Source code disclosure is a complex issue. Because of space considerations, I have omitted many details and nuances. For more discussion of the policy issues surrounding source code disclosure, I refer the interested reader to my testimony on this subject before the Elections Subcommittee of the House Administration Committee[36].

- *Learn from field experience.* It would help to 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. It would help if there were a framework for collecting, 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.

At present, the regulatory process does not provide any mechanism for investigating failures or problems with equipment in the field. When an airplane crashes, federal crash investigators descend upon the scene to learn what went wrong so we can learn from our failures and ensure that it won't happen again. The election community does not have any mechanism for performing this kind of investigatory function.

Transparency

Historically, one of the abiding principles of election administration has been that the best way to demonstrate that the election is honest is by inviting public scrutiny and being open and transparent about all aspects of the election. When any aspect of election administration is kept secret, it invites questions about whether the secrecy is intended to cover up problems or to stifle debate.

The trend in elections is towards automation of more and more tasks that were previously performed manually. However, the spread of automation has unintentionally come with the unfortunate side-effect of degrading transparency[37 38 39]. When poll workers run elections or election officials count ballots, the public can observe that these actions are being performed correctly and openly, and can spot any errors or problems. In contrast, when those same operations are performed by machines containing proprietary technology, the secrecy surrounding those machines and their programming may prevent the public from meaningfully observing or engaging in oversight of the process.

There are several steps that could be taken to restore some of the transparency that has been lost:

- *Routine manual audits.* The single most important step that local election officials could take to improve transparency would be to institute routine manual audits and allow public observation of these audits. These audits should include a transparent and random process for selecting a random sample of precincts or machines, followed by a manual hand-to-eye recount of those voter-verified paper records.

  Audits provide a way to assess the accuracy of voting software. They are one of the few opportunities for a voter to verify that the votes were counted and tabulated correctly by the voting equipment. Election officials should ensure that interested parties are able to observe all aspects of the audit and see for themselves that the votes were counted accurately. Officials should also use audits to measure how accurate their equipment and processes are, to identify shortcomings, and to improve their processes for future elections. Officials should perform an audit after every election and publish the results of the audit and the cause of every discrepancy or error detected during the audit.

- *Broader disclosure of technical information.* There has recently been considerable public debate about the trustworthiness of voting machines. Some have argued that current voting machines are severely flawed; others have disputed that characterization. However, because of the secrecy surrounding proprietary voting software, advocates on both sides of the debate have often been denied access to the information that would be needed to present evidence for their position. The result is that advocates are all too often forced to argue from first principles or based on their professional judgement, rather than from hard evidence.

  Reversing the presumption of secrecy for technical information about voting technology would make it possible to have a more informed debate on the trustworthiness of today's e-voting

machines. In particular, disclosure of source code would allow interested parties to analyze the software for themselves, without having to rely upon analysis from some testing lab. We could expect and insist that anyone who wants to argue that the voting software from one vendor is flawed should be able to point to where exactly in the source code the flaw may be found. We could expect and insist that anyone who wants to argue that the voting software is flawless should be able to show evidence that the source code is free of flaws. This would create the opportunity for a more informed and scientific debate regarding the trustworthiness of e-voting, and it might raise the level of the debate.

Activities of the ACCURATE center

As I have studied electronic voting, I have become convinced of the importance of research into better voting technology. In 2005, I was fortunate to be part of a team that received funding from the National Science Foundation (NSF) to form a center called A Center for Correct Usable Reliable Auditable and Transparent Elections (ACCURATE). The ACCURATE grant provides a total of $7.5 million in funding over five years. The mission of the ACCURATE center is to study electronic voting. We are exploring the design space for voting machines so we can better understand how the next generation of these machines should be constructed. ACCURATE researchers include a psychology professor, a law professor, and eight computer scientists.

The three primary goals of ACCURATE are research, outreach, and teaching. Our research focuses on developing technologies that can improve voting systems. Our outreach effort focuses on working with the elections community to help them understand technology and policy issues. For example, we participated in post-election audits in 2006. Finally, we have designed curriculum to teach our students about the important issues in electronic voting.

Our ACCURATE research consists of several thrusts. One ACCURATE project involves performing usability testing to compare different types of equipment. ACCURATE researchers test design prototypes against human subjects to find out whether they are usable. We also provide coordinated responses to requests, such as those from the EAC. For example, we provided detailed comments on the proposed voting standards. In addition, we are performing basic research in computer security to create technology for future generations of voting systems. More information about the activities of ACCURATE may be found in our 2006 annual report[40].

Notes

[1] "Computer loses more than 4,000 early votes in Carteret County", Associated Press, Nov. 4, 2004.

[2] "Broward Ballot Blunder Changes Amendment Result", Local 10 News, Nov. 4, 2004.

[3] "Broward Machines Count Backward", The Palm Beach Post, Nov. 5, 2004.

[4] "Distrust fuels doubts on votes: Orange's Web site posted wrong totals", Orlando Sentinel, Nov. 12, 2004.

[5] D. Cho, "Fairfax Judge Orders Logs Of Voting Machines Inspected", Washington Post, p.B01, Nov. 6, 2003. `http://www.washingtonpost.com/ac2/wp-dyn/A6291-2003Nov5`

[6] "Vote spike blamed on program snafu", Forth Worth Star-Telegram, Mar. 9, 2006.

[7] M. Bishop, L. Guarino, D. Jefferson, D. Wagner, "Analysis of Volume Testing of the AccuVote TSx/AccuView", Report of the California Secretary of State's Voting Systems Technology Assessment Advisory Board, Oct. 11, 2005.

[8] T. Kohno, A. Stubblefield, A.D. Rubin, D.S. Wallach, "Analysis of an Electronic Voting System", May, 2004.

[9] D. Wagner, D. Jefferson, M. Bishop, C. Karlof, N. Sastry, "Security Analysis of the Diebold AccuBasic Interpreter", Report of the California Secretary of State's Voting Systems Technology Assessment Advisory Board (VSTAAB), Feb. 14, 2006.

[10] A.J. Feldman, J.A. Halderman, E.W. Felten, "Security Analysis of the Diebold AccuVote-TS Voting Machine", Sept. 2006.

[11] A. Kiayias, L. Michel, A. Russell, A.A. Shvartsman, "Security Assessment of the Diebold Optical Scan Voting Terminal", Oct. 30, 2006.

[12] A. Yasinsac, D. Wagner, M. Bishop, T. Baker, B. de Medeiros, G. Tyson, M. Shamos, and M. Burmester, "Software Review and Security Analysis of the ES&S iVotronic 8.0.1.2 Voting Machine Firmware", Feb. 23, 2007.

[13] "Risk Assessment Report: Diebold AccuVote-TS Voting System and Processes", Science Applications International Corporation, Sept. 2, 2003.

[14] "Direct Recording Electronic (DRE) Technical Security Assessment Report", Compuware Corporation, Nov. 21, 2003.

[15] "Security Assessment: Summary of Findings and Recommendations", InfoSENTRY, Nov. 21, 2003.

[16] "Trusted Agent Report: Diebold AccuVote-TS System", RABA Innovative Solution Cell, Jan. 20, 2004.

[17] H. Hursti, "Critical Security Issues with Diebold Optical Scan", Black Box Voting, July 4, 2005.

[18] H. Hursti, "Critical Security Issues with Diebold TSx", Black Box Voting, May 11, 2006.

[19] D. Wagner, D. Jefferson, M. Bishop, C. Karlof, N. Sastry, "Security Analysis of the Diebold AccuBasic Interpreter", Report of the California Secretary of State's Voting Systems Technology Assessment Advisory Board (VSTAAB), Feb. 14, 2006.

[20] D.W. Jones, "Connecting Work on Threat Analysis to the Real World", June 8, 2006.

[21] A. Yasinsac, D. Wagner, M. Bishop, T. Baker, B. de Medeiros, G. Tyson, M. Shamos, and M. Burmester, "Software Review and Security Analysis of the ES&S iVotronic 8.0.1.2 Voting Machine Firmware", Feb. 23, 2007.

[22] For instance, the security vulnerabilities appear to violate the requirements of Section 6.4.2 and Section 6.2 of the 2002 FEC standards.

[23] R.J. Anderson, *Security Engineering - A Guide to Building Dependable Distributed Systems*, Wiley, 2001, §23.3.

[24] "Election Officials Rely on Private Firms", San Jose Mercury News, May 30, 2004.

[25] "Election Whistle-Blower Stymied by Vendors", Washington Post, Mar. 26, 2006.

[26] "Sort of fixed: Broader election flaws persist", Tallahassee Democrat, Apr. 15, 2006.

[27] "Cold Shoulder for E-voting Whistleblowers", The New Standard, May 17, 2006.

[28] "New Fears of Security Risks in Electronic Voting Systems", The New York Times, May 12, 2006.

[29] D.W. Jones, "Auditing Elections", Communications of the ACM 47(10), Oct. 2004, pp.46-50.

[30] A.D. Rubin, Written testimony before the Election Assistance Commission, June 30, 2005. `http://avirubin.com/vote/eac2.pdf`

[31] TGDC Resolution #06-06, "Software Independence of Voting Systems," Dec. 5, 2006.

[32] R.L. Rivest, J.P. Wack, "On the notion of 'software independence' in voting systems", `http://vote.nist.gov/SI-in-voting.pdf`.

[33] "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.

[34] "The Machinery of Democracy: Protecting Elections in an Electronic World", Brennan Center Task Force on Voting System Security, June 27, 2006.

[35] United States Election Assistance Commission, "EAC's Testing and Certification Program for Voting Systems", Jan. 19, 2007.

[36] D. Wagner, Written testimony before the Elections Subcommittee of the House Administration Committee of the U.S. House of Representatives, Mar. 15, 2007. `http://www.cs.berkeley.edu/~daw/papers/testimony-house07.pdf`

[37] D.W. Jones, "Voting System Transparency and Security: The need for standard models", written testimony before the EAC Technical Guidelines Development Committee, Sept. 20, 2004. `http://www.cs.uiowa.edu/~jones/voting/nist2004.shtml`

[38] J. Hall, "Transparency and Access to Source Code in E-Voting," USENIX/ACCURATE Electronic Voting Technology (EVT'06) Workshop. `http://josephhall.org/papers/jhall_evt06.pdf`

[39] D.K. Mulligan, J.L. Hall, written testimony before the California Senate Elections, Reapportionment & Constitutional Amendments Committee, Feb. 8, 2006. `http://josephhall.org/nqb2/media/Mulligan_Hall_OSHRG_Statement.pdf`

[40] ACCURATE, 2006 Annual Report, Feb. 2, 2007. `http://accurate-voting.org/2007/02/02/annual-report/`

Mr. CLAY. Thank you so much, Doctor.

Mr. Norden, please proceed.

STATEMENT OF LAWRENCE NORDEN

Mr. NORDEN. Thank you, Chairman Clay, and Congresswoman Maloney, for holding this hearing on what is certainly an extremely important topic.

For 18 months, I chaired the Brennan Center's Task Force on Voting System Security, and that was a task force made up of the leading computer scientists and security professionals in both the private and public sector in the United States.

It included David Wagner as well as scientists from NIST, the former chief security officer from Microsoft, and the former cyber security czar for President George W. Bush.

What the task force found is no longer, I think, a matter of debate among security experts that have looked at these voting machines, and that is that they have serious security and reliability vulnerabilities.

As David Wagner mentioned, the good news is that there is substantial agreement among these experts, about what we can do to address these vulnerabilities, and among the most important things we can do is to ensure that we have an independent voter-verified record such as a paper ballot or paper trail, and that after the polls have closed, we use those paper records to check the electronic tallies.

These steps are certainly important, given the problems that we are aware of with the machines today and their certification. But I would echo what David Wagner said, and say that these steps are important, no matter how well we do the certification process or accredit labs.

That is not to say that certification of accreditation isn't extremely important. We want to catch flaws before the elections, before the systems are certified, obviously, and to maximize the chance that we catch those flaws, we have to fix what is a broken certification and accreditation process.

That process, I should say, is in transition right now, as we have heard today, and I think there is good reason to believe that it is being substantially improved. Still, there are certain things that need to be done. I detail a number of them in my written testimony. I am just going to talk about a few in the remaining time that I have.

I would say one of the most important things we can do is something that Congresswoman Maloney touched upon and David Wagner touched upon, and that is to eliminate the process where vendors choose and pay the labs that judge and certify them. For obvious reasons, this is a conflict of interest and creates perverse incentives for vendors to certify machines where they are relying on—excuse me—for testing authorities to certify machines. They are relying on those same vendors for future business.

I should add that Congressman Holt's bill, H.R. 811, does end this system along the lines of what David Wagner suggested. The second thing we can do is add an important step to testing machines, and this has also come up a little bit in some of the testimony we have heard today.

Right now, what we do is we test to guidelines. We test under normal conditions to satisfy a check list. This is certainly important to do but good security testing, as Congresswoman Maloney touched upon, will try to ensure that a system does not fail when it is attacked or misused.

There are a couple of things we can do. One of the things that we can do is what Mr. Skall suggested, which is to have independent security experts perform open-ended research and search for vulnerabilities on these machines to exploit.

This is how many of the most serious flaws in voting machines have been discovered. Unfortunately, because it wasn't part of a certification process, this isn't something we discovered until after the machines were in use.

Something else we can do is require vendors to demonstrate how they will defeat a standard set of threats that could be developed by an organization list like NIST.

We should also make sure that the process for certifying machines, for evaluating machines, excuse me, does not end with certification.

The EAC is now accepting anomaly reports from election officials and that is a good step. Unfortunately, it is not accepting such reports from voters, from technical experts that are performing field studies on these systems.

And I would say that is a problem, for a number of reasons, not least of which is that voters themselves, and technical experts, are often going to be in a better position than election officials to know if the machines aren't working when they are voting on them.

We should use their reports to investigate machines, to amend guidelines and to require machine changes, where necessary.

Finally, one thing I would urge Congress is to make sure that we fund the EAC and the certification process adequately.

The EAC is charged with some of the most important administrative tasks in Federal elections. If we are going to keep them in charge of those tasks, it is important that we give them enough funds and enough employees to do them.

In 2006, the EAC had a budget of just $15 million and less than 30 employees, and that is simply not enough, given the responsibilities that they have.

Thank you.

[NOTE.—The Brennan Center Task Force on Voting System Security publication entitled, "The Machinery of Democracy: Protecting Elections in an Electronic World," may be found in subcommittee files.]

[The prepared statement of Mr. Norden follows:]

BRENNAN
CENTER
FOR JUSTICE

Committee on Oversight and Government Reform,
Subcommittee on Information Policy, Census, and National Archives

United States House of Representatives

Statement of

Lawrence D. Norden

Counsel, Brennan Center for Justice at NYU School of Law

May 7, 2007

The Brennan Center for Justice thanks the Subcommittee on Information Policy, Census and National Archives for holding this hearing. We appreciate the opportunity to share with you the results of our extensive studies to ensure that our nation's voting systems are more secure and reliable, as well as our thoughts regarding the challenges in developing more reliable accreditation and certification of voting systems. The Brennan Center for Justice is a nonpartisan think tank and advocacy organization that focuses on democracy and justice. We are deeply involved in efforts to ensure accurate and fair voting, voter registration, and campaign finance reform.

I. SUMMARY OF CHALLENGES TO ENSURE SECURE AND RELIABLE VOTING SYSTEMS

In less than five years, the vast majority of Americans have gone from using punch card and lever machines, to having their votes counted by electronic touch screens and optical scanners.[1] Unfortunately, as the Brennan Center and others have noted, this massive change took place without adequate development and implementation of procedures necessary to ensure that our new electronic voting systems were as secure and reliable as possible. In retrospect, the result of this failure was all too obvious: a crisis in public confidence in the voting systems most widely used across our nation and the certification and use of voting systems with serious security, accuracy and reliability flaws.

Fortunately, there is widespread agreement among experts about what must be done to make electronic voting more secure and reliable.

---

[1] Election Data Services, *2006 Voting Equipment Survey, available at* http://www.electiondataservices.com/EDSInc_VEStudy2006.pdf.

First, jurisdictions around the country must adopt basic security and reliability measures for machines already in use. Far too few of our states and counties take the steps necessary to greatly increase the security of our voting systems by making the least difficult malicious attacks against them much more difficult to execute successfully. Among the most important things jurisdictions can do are:

- **Conduct regular post-election audits comparing software independent voter verified records to electronic tallies,** to ensure that those tallies are accurate; and

- **Ban most wireless components on voting machines,** as they make voting systems far more vulnerable to many types of attacks.

Second, we must improve our process for federally certifying voting machines. The current process for certifying electronic voting machines is in transition, and there is reason to be optimistic that recent public exposure of some of the past problems will force important changes. At the same time, it is clear that for the last several years, the accreditation and certification process for voting machines has been flawed. To address the most serious of these flaws, the Brennan Center makes the following recommendations:

- **Ensure That Voting System Testing Laboratories Are and Appear to be Independent of Vendors.** Recent events have left many questioning the independence and competence of the laboratories that test and certify electronic voting systems. There are at least two things that can be done to begin to change this perception and create truly independent labs. First, we should end the process whereby the Voting System Testing Laboratories are chosen and directly paid by the vendors whose machines they evaluate. This creates an appearance of conflict of interest. Worse yet, it creates perverse incentives for the testing laboratories when testing vendors' machines. Second, the periodic evaluations of testing laboratories conducted by the National Voluntary Laboratory Accreditation Program ("NVLAP") should be made public promptly, regardless of whether the laboratory's accreditation is granted, denied or revoked.

- **Make the Voting Machine Certification Process More Transparent.** The recent CIBER debacle in New York has shown that testing laboratories sometimes fail to test even to current voting machine certification requirements. If the public is to regain its trust in this process, it is critical that the Election Assistance Commission ("EAC") publish: (1) all test plans submitted by the testing laboratories; (2) the vendor's Technical Data Packages, which the vendor submits to the EAC to provide the specifics of a voting system; as well as (3) the test report that a testing laboratory submits to the EAC after it has tested that voting system.[2]

---

[2] ACCURATE, *Public Comment on the Manual for Voting System Testing & Certification Program Submitted to the United States Election Assistance Commission* (Oct. 31, 2006), joined by the Brennan Center, *available at* http://accurate-voting.org/wp-content/uploads/2006/11/ACCURATE_VSTCP_comment.pdf (hereinafter "ACCURATE Comment on VSTCP").

- **Strengthen Voting Machine Certification Process Through Threat Analyses and Open-Ended Vulnerability Testing.** Currently, systems are certified by laboratories through "conformance" testing (i.e., the system is tested under normal conditions to ensure that it responds in a way prescribed by voting system guidelines). Computer scientists and security experts agree that good security testing must do more than this – specifically, it should attempt to ensure that a system will not fail when it is intentionally attacked or misused.[3] There are at least two important ways to address concerns around the limits of conformance testing. First, vendors should be required to demonstrate how their machines will defeat a standard set of threats developed by the National Institute of Standards and Technology ("NIST"). Second, independent security experts should be allowed to perform open-ended research for security and reliability vulnerabilities on voting systems.[4]

- **Use Information From Voters and Technical Experts Who Have Used the Voting Machines to Amend Voting System Standards, Where Necessary.** The EAC's Voting System Testing and Certification Program Manual now provides a formal (though severely limited) process by which election officials may report voting system anomalies. The Brennan Center joins other organizations in recommending that this reporting process be opened to include reporting from voters and technical experts who find anomalies.[5]

- **Adequately Fund the EAC and the Voting Machine Certification Process.** The EAC is the federal agency charged with overseeing many of the most important federal election administration tasks, including the accreditation of testing laboratories and certification of voting machines. However, its annual operating budget is $15 million and it employs fewer than 30 people.[6] If we are serious about reforming and improving the federal certification process, we must increase the EAC's budget and allow it to hire more staff.

---

[3] *See, e.g.*, Letter from Eugene Spafford, Chair, U.S. Public Policy Committee of the Association for Computing Machinery, to William Jeffrey, Director, National Institute of Standards Technology (Dec. 1, 2006) *available at* http://www.acm.org/usacm/PDF/USACMCommentsSTSPaper.pdf; *Voting Machines: Will the New Standards and Guidelines Help Prevent Future Problems?: Joint Hearing Before the H. Comm. on H. Admin. and the Comm. on Science*, 109th Cong. 136-148 (2006) (Responses by David Wagner, Professor of Computer Science, University of California-Berkeley to Post-Hearing Questions), *available at* http://www.votetrustusa.org/pdfs/qfr-house06.pdf.

[4] *See, e.g.*, U.S. Election Assistance Commission Public Meeting and Hearing, Pasadena, CA (July 28, 2005) (Testimony of David L. Dill, Professor of Computer Science, Stanford University and Founder of Verified Voting Foundation and VerifiedVoting.org) *available at* http://www.eac.gov/docs/Dill.pdf (hereinafter "Testimony of David Dill").

[5] ACCURATE Comment on VSTCP, *supra* note 2, at 8.

[6] U.S. Election Assistance Commission, *Fiscal Year 2006 Annual Report* 7 (2006) *available at* http://www.eac.gov/docs/EAC%20AR2006.pdf (hereinafter "EAC 2006 Annual Report"); Memorandum from Curtis Crider, Inspector General, U.S. Election Assistance Commission, to Thomas Wilkey, Executive Director, U.S. Election Assistance Commission (Oct. 2, 2006) *available at* http://www.eac.gov/docs/Memo%20on%20EAC%20noncomply.pdf (hereinafter "EAC Memo").

II. THE BRENNAN CENTER'S WORK ON VOTING SYSTEM SECURITY: HOW JURISDICTIONS CAN MAKE CURRENT VOTING SYSTEMS MORE SECURE AND RELIABLE

In 2005, in response to growing public concern over the security of new electronic voting systems, the Brennan Center assembled a task force (the "Security Task Force") of the nation's leading technologists, election experts, and security professionals to analyze the security and reliability of the nation's electronic voting machines.[7] The goal of the Security Task Force was simple: to quantify and prioritize the greatest threats to the integrity of our voting systems and to identify steps that we can take to minimize those threats.

Working with election officials and other experts for close to eighteen months, the Security Task Force analyzed the nation's major electronic voting systems, ultimately issuing *The Machinery of Democracy: Protecting Elections in an Electronic World* (the "Brennan Center Security Report") in June 2006. The conclusions of the Brennan Center Security Report are clear: (1) all of the nation's electronic voting systems have serious security and reliability vulnerabilities (including especially, vulnerabilities to the malicious or accidental insertion of corrupt software or bugs); (2) the most troubling vulnerabilities of each system can be significantly remedied; and (3) few jurisdictions have implemented any of the key security measures that could make the least difficult attacks against voting systems substantially more difficult to complete.[8]

Most importantly, the Task Force concluded:

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

- **Voting machines with wireless components 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 Security Task Force are routine post-election audits comparing voter-verified paper records to the electronic record and bans on

[7] For a list of the members of the Security Task Force see Appendix A of this Statement.
[8] Lawrence Norden *et al.*, THE MACHINERY OF DEMOCRACY: PROTECTING ELECTIONS IN AN ELECTRONIC WORLD 3 (Brennan Center for Justice ed., 2006) *available at* http://brennancenter.org/stack_detail.asp?key=97&subkey=36343&init_key=105.

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 Security Task Force also advocated the use of "parallel testing": Election Day testing of randomly selected voting machines under real world conditions. In jurisdictions with paperless electronic voting machines, meaningful audits of voter-verified paper records are not an option. Parallel testing allows these jurisdictions to detect the presence of malicious software in voting machines.

III. IMPROVING THE VOTING MACHINE ACCREDITATION AND CERTIFICATION PROCESS

The Voter Confidence and Increased Accessibility Act of 2007 (H.R. 811), introduced by Congressman Holt, adopts a number of key recommendations endorsed by the Task Force, including a requirement for mandatory, routine audits of voter-verified paper records for all federal races.[9] These are necessary steps to deter fraud and to catch programming errors, software bugs and other problems. However, audits will not, by themselves, improve the performance of our voting machines. Rather, they will allow us to learn, *after the polls have closed*, whether something has gone wrong.

For this reason, it is also important that we improve the federal process for certifying electronic voting machines so that we catch as many problems as possible *before* machines are certified and used in elections. That means ensuring that the laboratories certifying voting systems are truly independent, that the results of their tests are publicly available, and that the standards to which they test are as rigorous as possible.

A. Ensure That Voting System Testing Laboratories Are and Appear to be Independent of Vendors

If we are to have a certification process that works and inspires public confidence, it is critical that testing laboratories both are *and appear to be* truly independent of the voting system vendors whose machines they are testing. The procedures associated with laboratory accreditation that currently exist do not sufficiently address these concerns.

1. End the system that allows vendors to choose and directly pay voting system testing laboratories

Many election integrity advocates and security experts have criticized the current process by which vendors choose and pay the laboratories that evaluate their systems.[10] This process creates an appearance of conflict of interest for the testing labs. Worse still, it

[9] H.R. 811, 110th Cong. § 5 (2007).

[10] ACCURATE Comment on VSTCP, *supra* note 2; Testimony of David Dill, *supra* note 4; *Voting Machines: Will the New Standards and Guidelines Help Prevent Future Problems?: Joint Hearing Before the H. Comm. on H. Admin. and the Comm. on Science*, 109th Cong. 66-71 (2006) (Written Statement of David Wagner, Professor of Computer Science, University of California-Berkeley), *available at* http://www.votetrustusa.org/index.php?option=com_content&task=view&id=1554&Itemid=26 (hereinafter "Testimony of David Wagner").

creates perverse incentives for the testing laboratories to certify machines to ensure that vendors choose them in the future. The testing laboratories themselves have done little to build public confidence in their independence from voting machine vendors. In a fairly well publicized written submission to the EAC, a testing laboratory recently stated that it "view[ed] the relationship between an independent testing laboratory and it's [sic] clients as similar to that between lawyer and client or between doctor and client."[11]

Given the many failures in the voting machine certification process in the last several years, it is critical that this system ends and that vendors have no role in choosing or directly paying the laboratories testing and certifying their machines. H.R. 811 would do this by establishing an escrow account with the EAC to which vendors would make payments for the costs of testing their machines. Vendors would have no role in choosing their testing labs; rather the EAC would choose the laboratories at random.[12]

2. Mandate publication of NVLAP Assessment Reports

The EAC's failure to timely publish a damning Assessment Report of CIBER, Inc. after is was completed in July 2006 provides a textbook case of how a lack of transparency can severely shake the faith of the public in the independence and competence of the laboratories testing and certifying our voting systems as secure and reliable. The report concluded, among other things, that:

> CIBER has not shown the resources to provide a reliable product. The current quality management plan requires more time to spend on managing the process than they appear to have available and it was clear during the assessment visit that they had not accepted that they have a responsibility to provide quality reports that show what was done in testing.[13]

As a result of the Assessment Report, the EAC determined it could not accredit CIBER under the interim accreditation process.[14] However, it did not publicize this decision, release the Assessment Report, or notify the State of New York, which was using CIBER to test its voting systems at the time. Only after the New York Times reported that CIBER had been barred from certifying election equipment and weeks of public pressure following that news article, did the EAC finally release the Assessment Report and other documents related to its decision.[15]

---

[11] U.S. Election Assistance Commission Public Meeting, Washington, D.C. (Oct. 26, 2006) (Written Statement of Frank Padilla, Test Supervisor, Wyle Laboratories, Inc.) *available at* http://www.eac.gov/docs/Voting%20Systems%20Briefing%20-%20Frank%20Padilla%2010-18-06%20Final.pdf.

[12] H.R. 811, *supra* note 9 at § 2.

[13] U.S. Election Assistance Commission, *Assessment Report: CIBER & Wyle* (conducted July 17-22, 2006) *available at* http://www.eac.gov/docs/Ciber%20&%20Wyle%20Assessment%20(July%202006).pdf.

[14] Christopher Drew, *Citing Problems, U.S. Bars Lab From Testing Electronic Voting*, N.Y. TIMES (Jan. 4, 2007) *available at* http://select.nytimes.com/search/restricted/article?res=F50811F63C540C778CDDA80894DF404482.

[15] These documents are available at: http://www.eac.gov/eac_vsc3_updates.htm.

Since the CIBER fiasco, NIST, through its National Voluntary Laboratory Accreditation Program ("NVLAP"), has taken over the process of assessing testing laboratories and making recommendations to the EAC regarding which testing laboratories should be accredited. To its credit, NVLAP has publicly released the Assessment Reports for the two laboratories it has reviewed and recommended for accreditation.[16]

However, there do not appear to be any written procedures requiring NVLAP to release such Assessment Reports. The public release of such reports, as well as reports connected to follow-up assessments, is critical to restoring the public's faith that the testing laboratories are competent and independent. Such publication should be required whether or not the laboratory receives or maintains its accreditation.

B. Make the Voting Machine Certification Process More Transparent

New York's recent experience with CIBER is also an excellent illustration of the importance of transparency in the voting machine certification process, and in particular the need to ensure that all test plans, Technical Data Packages and test reports are made public.

Concurrent with its hiring of CIBER to conduct its certification testing, New York also hired NYSTEC, a private, not-for-profit engineering company to conduct an independent review of CIBER's test plan. NYSTEC's review showed that the test plan lacked several security and functional testing requirements under state law and the federal Voluntary Voting System Guidelines of 2005 (to which CIBER had agreed to test). Among the items missing from the test plan were:

- A requirement that voting systems did not include any device potentially capable of externally transmitting or receiving data via the internet, radio waves or other wireless means;
- A requirement that voting system software not contain any viruses or other devices that could cause the system to cease functioning properly at a future time;
- A requirement for voting systems to provide a means by which the ballot definition code could be positively verified to ensure that it corresponded to the format of the ballot face and election configuration; and
- Test methods or procedures for the majority of the state's voting system requirements.[17]

These problems were only discovered because CIBER's test plans were subject to independent scrutiny. Short of mandating that jurisdictions hire independent reviewers for

[16] Information on the testing laboratories that NIST has reviewed is available at: http://vote.nist.gov/LabRec.htm.
[17] Howard Stanislevic, *Voting System Certification: Who's Minding the Store?*, VoteTrustUSA (Jan. 9, 2007) *available at* http://votetrustusa.org/index.php?option=com_content&task=view&id=2173&Itemid=113.

all certifications of voting machines, it is imperative that the EAC publish documents necessary for the public to ascertain the value of a testing laboratory's certification. This means not only publishing all testing laboratory test plans for a particular machine, but also the Technical Data Packages submitted by the vendor to the testing laboratory, and the laboratory's reports that assess the machines.

The EAC's Voting System Testing and Certification Program Manual now requires the publications of testing laboratory reports, *if the machines gain certification.* It does not, however require the publication of test plans or the Technical Data Packages provided by vendors that will allow the public or independent experts to judge the conclusions made in those reports.[18] This is a glaring gap in the EAC's reporting requirements and should be changed.

C. Strengthen Voting Machine Certification Process Through Threat Analyses and Open-Ended Vulnerability Testing

Currently, voting systems are certified by laboratories through "conformance" testing, which is meant to ensure that the voting system being tested will respond in a way proscribed by the federal voting system guidelines under normal conditions. Computer scientists and security experts agree that conformance testing is not sufficient to ensure that our systems are secure. As Professor David Wagner has pointed out in previous Congressional testimony, security evaluations should assume "an active, intelligent adversary; [conformance testing] concerns the presence of desired behavior, while security concerns the absence of undesired behavior."[19]

Princeton Professor Ed Felten's recent demonstration of a serious security flaw in a certified voting machine demonstrates the weakness of relying on conformance testing for security evaluations. Professor Felten and his co-authors showed that it was possible to insert malicious software onto a voting machine through the use of the machine's memory card slot. This flaw could allow a person with just a few seconds access to the memory card slot to "modify all of the records, audit logs, and counters kept by the voting machine."[20] While the flaw may have violated provisions of the voting system guidelines, these provisions were vague enough that it is easy to understand how lax testing could have missed it;[21] there was nothing in the guidelines that specifically prohibited a voting machine from being able to download code from a memory card or through a memory card slot.

---

[18] Aaron Burstein & Joseph Lorenzo Hall, *Unlike Ballots, EAC Shouldn't Be Secretive*, Roll Call (Jan. 22, 2007) *available at* http://www.rollcall.com/issues/52_66/guest/16640-1.html.

[19] Testimony of David Wagner, *supra* note 10.

[20] Ariel J. Feldman, J. Alex Halderman, & Edward W. Felten, *Security Analysis of the Diebold AccuVote-TS Voting Machine* 2 (Sept. 13, 2006) *available at* http://itpolicy.princeton.edu/voting/ts-paper.pdf.

[21] In his testimony Professor David Wagner notes that this security vulnerability may have violated Sections 6.4.2 and 6.2 of the FEC Standards. *Certification and Testing of Electronic Voting Systems: Field Hearing in New York, NY Before the Subcomm. on Info. Policy, Census, and Nat'l Archives of the H. Comm. on Oversight and Gov't Reform*, 110th Cong. 12 n.22 (2007) (Written Testimony of David Wagner, Associate Professor of Computer Science, University of California-Berkeley).

It is not reasonable to expect that we can develop a "check-list" that will imagine every possible flaw in a voting system. Clearly, however, finding such flaws before certifying machines is extremely important.

There are at least two important ways to address concerns around the limits of conformance testing. First, some form of threat analysis along the lines of that done by the Brennan Center Task Force on Voting System Security should be performed on all machines before they are certified. Specifically, vendors should be required to demonstrate how their machines will defeat a standard set of threats developed by NIST. Under no circumstances should software be the only defense against such attacks.[22]

Second, independent security experts should be allowed to perform open-ended research for security and reliability vulnerabilities on systems (these are often referred to as "red team exercises").[23] This is how many of the most serious vulnerabilities in electronic voting systems have been found.[24] Unfortunately, to this point, such flaws have been found outside the certification process, after machines were already certified and used in elections.

D. Use Information From Voters and Technical Experts Who Have Used the Voting Machines to Amend Voting System Standards, Where Necessary

Under the new Voting System Testing and Certification Program Manual, the EAC will accept reports from "[s]tate or local election officials who have experienced voting system anomalies in their jurisdiction."[25] This is an important step. Unfortunately, individual voters and technical experts performing usability, accessibility and security tests on voting machines appear to be excluded from filing such reports with the EAC.[26]

This is problematic for two reasons. First, the EAC has no method in place to protect the anonymity of election officials filing reports. Many election integrity and security experts have argued that an election official "might be reluctant to report an irregularity in a system he was responsible for administering," both because he may have

---

[22] *See* National Institute of Standards and Technology, *Requiring Software Independence in VVSG 2007: STS Recommendations for the TGDC* (draft, Nov. 2006) *available at* http://vote.nist.gov/DraftWhitePaperOnSIinVVSG2007-20061120.pdf (recommending that future systems be "software independent," meaning that an "undetected change in software cannot cause an undetectable change or outcome in an election.").

[23] Testimony of David Dill, *supra* note 4.

[24] *See, e.g.*, Michael A. Wertheimer, RABA Technologies LLC, *Trusted Agent Report: Diebold AccuVote-TS Voting System* (Jan. 20, 2004) *available at* http://www.raba.com/press/TA_Report_AccuVote.pdf; Harri Hursti, *Security Alert: July 4, 2005 – Critical Security Issues with Diebold Optical Scan Design* (on behalf of Black Box Voting, July 5, 2005) *available at* http://www.blackboxvoting.org/BBVreport.pdf; Feldman, Halderman, & Felten, *supra* note 20.

[25] U.S. Election Assistance Commission, *Testing and Certification Program Manual* section 8.7.2 (draft, Sept. 28, 2006) *available at* http://www.eac.gov/docs/Voting%20System%20Testing%20and%20Certification%20Program%20Manual%20FR%20DRAFT%20(Sept%2028).pdf.

[26] ACCURATE Comment on VSTCP, *supra* note 2, at 8.

also been responsible for purchasing that system and because he would probably need to continue to rely on technical assistance from the vendor.[27]

Second, voters and technical experts using these machines would be an excellent source of information about problems with these machines; in many instances, they will be in a far better position than election officials to know how the machines actually perform when used. We believe the reporting process should be opened to include them, and that the EAC should use credible reports from these sources to investigate potential problems with the machines, and mandate changes to the voting system guidelines or the machines themselves, when necessary.

E. Adequately Fund the EAC and Voting Machine Certification Process

The Help America Vote Act has placed the EAC in charge of many of the most important federal election administration tasks. Among other responsibilities – and aside from acting as the lead federal agency for accreditation of the Voting System Testing Laboratories and certification of voting systems – it is also charged with acting as a "clearinghouse of information on the experiences of State and local governments in implementing the guidelines and in operating voting systems in general," "conducting studies and carrying out other activities to promote the effective election administration of Federal elections," allocating election-related federal funding to the states, and carrying out administrative duties under the National Voter Registration Act of 1993 (the Motor Voter law), including developing and maintaining a mail voter registration application form for elections for federal office.[28]

Given its enormous responsibility, the EAC receives very little support. In 2006, it had an operating budget of just $15 million and employed less than 30 people.[29] Mandating the changes detailed in this testimony would be an important step in improving the accreditation and certification processes, but such mandates will have little effect if the EAC does not have the resources and staff to ensure such mandates are satisfied.

---

[27] *Id.*, at 9.
[28] 42 U.S.C. § 15322 (2003).
[29] EAC 2006 Annual Report, *supra* note 6; EAC Memo, *supra* note 6.

IV. CONCLUSION

The Brennan Center has found that the voting systems most commonly purchased today are vulnerable to attacks and errors that could change the outcome of statewide elections. This finding should surprise no one. A review of the history of both election fraud and voting systems literature in the United States shows that voting systems have always been vulnerable to attack. Indeed, it is impossible to imagine a voting system that could be impervious to attack.

But there are straightforward countermeasures that that will substantially reduce the most serious security risks presented by the three systems. The Brennan Center's recommendations point the way for jurisdictions with the political will to protect their voting systems from attack. None of the measures identified in the Brennan Center Security Report – auditing voter verified paper records, banning wireless components, using transparent and random selection processes for auditing, adopting effective policies for addressing evidence of fraud or error in vote totals, conducting parallel testing – are particularly difficult or expensive to implement.[30]

Reform and Support Process for Federally Certifying Machines. It is critical that we further develop clear standards and procedures that will mandate strict independence in the certification of machines, rigorous testing, and detailed reporting of tests and results. In addition, the entire process would benefit if the EAC used reports from voters and technical experts to amend voting systems standards and demand changes to voting systems where necessary. If we are serious about reforming the process for federally certifying machines, we must adequately fund the EAC.

---

[30] Even routine parallel testing and audits of voter-verified paper records – perhaps the most costly and time consuming countermeasures reviewed in the joint threat analysis – have been shown to be quite inexpensive. Jocelyn Whitney, Project Manager for parallel testing activities in the State of California, provided the Brennan Center with data showing that the total cost of parallel testing in California was approximately *12 cents per vote* cast on DREs. E-mail from Jocelyn Whitney (Feb. 25, 2006) (on file with the Brennan Center). Harvard L. Lomax, Registrar of Voters for Clark County, Nevada, estimates that a Task Force of auditors can review 60 votes on a voter verified paper trail in four hours. Assuming that auditors are paid $12 per hour and that each Task Force has two auditors, the cost of such audits should be little more than *3 cents per vote*, if 2% of all votes are audited. Telephone Interview with Harvard L. Lomax (Mar. 23, 2006). Each of these costs represents a tiny fraction of what jurisdictions already spend annually on elections. The Brennan Center's study of voting system costs shows that, for instance, most jurisdictions spend far more than this on printing ballots (as much as $0.92 per ballot), programming machines (frequently more than $0.30 per vote per election), or storing and transporting voting systems. Lawrence Norden *et al.*, THE MACHINERY OF DEMOCRACY: VOTING SYSTEM SECURITY, ACCESSIBILITY, USABILITY AND COST (Brennan Center for Justice ed., 2006) *available at* http://www.brennancenter.org/stack_detail.asp?key=97&subkey=38150&proj_key=76.

APPENDIX A: ABOUT THE TASK FORCE

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

The members of the Task Force are:

Chair
Lawrence D. Norden, Brennan Center for Justice

Principal Investigator
Eric L. Lazarus, DecisionSmith

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

Professor Matt Bishop, University of California at Davis

Lillie Coney, Electronic Privacy Information Center

Professor David Dill, Stanford University

Jeremy Epstein, PhD, Cyber Defense Agency LLC

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

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

Professor Douglas W. Jones, University of Iowa

John Kelsey, PhD, NIST

Rene Peralta, PhD, NIST

Professor Ronald Rivest, MIT

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

Dr. Bruce Schneier, Counterpane Internet Security

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

Professor David Wagner, University of California at Berkeley

Professor Dan Wallach, Rice University

Matthew Zimmerman, Electronic Frontier Foundation

Mr. CLAY. Thank you so much, Mr. Norden.

Mr. Washburn, please proceed.

STATEMENT OF JOHN WASHBURN

Mr. WASHBURN. Thank you, Chairman Clay, and Mrs. Maloney, Congresswoman Maloney, for having this hearing and for giving me this opportunity to present testimony to you on testing and certification of voting systems.

I have worked in the field of software quality assurance since 1994, and for the 10-years prior to that, I was a commercial programmer developing commercial software.

It is important to consider both past testing done under NASED and the present testing process of the EAC, for two reasons. First, as has been mentioned, all the equipment currently in use has been tested under the former NASED process, and most of this equipment will be used again in the subsequent years, in this year, and 2008.

Second, the new EAC program has made some steps toward greater transparency and oversight. It retains some of the systemic flaws of the NASED program. The NASED and EAC testing and certification framework suffer from three systematic flaws.

Both systems are opaque to most primary stakeholders in the election process. These stakeholders are State election officials, local election officials, candidates for public office, and most importantly, the voters themselves, and due to the lack of transparency and accountability, neither system adequately assures the public that rigorous, thorough and effective testing has actually been done, and neither system permits or encourages the reporting of system defects, nor do they include a responsive corrective action plan.

Under the NASED system, the entire process was a private sector transaction between the manufacturer and the testing laboratory, shielded from public oversight by vigorously enforced nondisclosure agreements.

The reports of test results as well as documentation of the testing undertaken to confirm a voting system's compliance with standards are considered the property of the manufacturer of that system. It is extremely rare for citizens to gain access to these reports.

For jurisdictions without their own State level testing programs, all that is available is a list of systems which have been granted a certification number, and the assurance that NASED has ruled that the certified system is in conformance with the standards.

Without test plans, and results of the test executions, there is no evidence, there is just an appeal to authority, and with the reports from the New York Board of Elections and the nonconformances revealed in penetration analysis and academic reviews, this authority has been called into question.

Over the last several years, numerous security and design effects have been uncovered, and each of these discoveries has left unanswered the simple question: How did these noncompliant systems ever get certified?

For example, use of a programming technique called interpreted code, is prohibited by both the 1990 and 2002 standards, yet is in use by the Diebold systems.

The vote tabulation software found in ES&S equipment varies from machine to machine and from election to election and from jurisdiction to jurisdiction.

For each election, a new and unique version of the vote tabulation software is created. If the software changes from election to election and jurisdiction to jurisdiction, how can there be any version that is the certified version? The central election management system for Sequoia, which accumulates vote totals on election night, includes both source code and the compiler for that source code.

The source code and compiler combination make it easy to change the operation of this software "on the fly," and in the field. This is a violation of both the 2002 and 2005 standards.

These examples of nonconformance, though, went undetected for multiple rounds of testing over several years. So it is not just a one-time miss here.

The profound and real world consequences of not following these standards, even as weak as they are, is found at the hour hour and 9 minute mark of the documentation, Hacking Democracy, which I have included with my testimony. In this realistic simulation of an election, the outcome of the mock election was altered in spite of the election official following all of the correct administrative procedures.

This manipulation was only possible because that system did not follow the standards. The NASED testing framework provided no mechanism to report problems and no way to receive suggestions for improvement. The EAC has created a new—for example, I think some of the Sequoia systems don't have sufficient accessibility for the ADA. That is my opinion; but who am I going to tell that to?

The EAC has created a new program called the Quality Monitoring Program. The Quality Monitoring Program, though, limits itself to fielded systems. As Commissioner Davidson had pointed out, a fielded system is defined as a system which is certified by the EAC and used in a Federal election.

Since the EAC has not yet certified any systems, there are no fielded systems. The Quality Monitoring Program also records only anomalies, but the definition of anomaly in this section is exceptionally narrow and permits the dismissal of any report on the basis the report is due to administrative error or a procedural defect.

So, for example, a programming error in Pottawattamie County, IA, caused the election system to incorrectly tally the results of the June 6, 2006 primary election. This error, though, does not meet the EAC's definition of an anomaly, because the preelection testing done by the county auditor was insufficient and thus is a procedural deficiency.

The failure of the system to not correctly tally votes is not considered an anomaly by this definition, and further, only credible reports will be published and distributed to other election officials. Information in a credible report must first meet this narrow definition of anomaly, second, must only come from an election official, and third, the events included in the report have to have occurred during an election.

If an election official discovers a defect in a voting system during preelection testing, or during other testing, or were to undertake an independent review, the results would not be shared with other election officials.

The Quality Monitoring Program fails to meet the mandate laid upon the EAC in section 202, to be a clearinghouse of information on all voting systems, not just those systems which meet the limited definitions of fielded, anomaly and credible reports.

There is not much time before the 2008 Presidential election, and because of the short time, the EAC should use its authority already granted to the commission under section 242, to set up a second parallel testing framework. A suggestion for that is in my written testimony.

So, in conclusion, the NASED testing framework is opaque to every stakeholder in the elections, except, it seems, the election manufacturers. It gives the illusion of rigorous testing without the substance and resists reports of problems and resists suggestions for improvement.

The new EAC testing framework has these same deep flaws. In the meantime, an alternate framework needs to be created, which is more nimble, more effective and more efficient than either the NASED or EAC framework.

I would like to add as a software test professional, the activities over the last several years do offend me, that they have been allowed to be called software testing.

[NOTE.—The U.S. Election Assistance Commission publication entitled, "Testing and Certification Program Manual," may be found in subcommittee files.]

[The prepared statement of Mr. Washburn follows:]

Written Testimony of
John Washburn, VoteTrustUSA Voting System Technical Advisor
before the Subcommittee on Information Policy, Census and National Archive
of the Committee on Oversight and Government Reform
U.S. House of Representatives
May 7, 2007

Thank you, Chairman Clay and distinguished members of the committee, for holding this hearing and for giving me this opportunity to present testimony to you on the testing and certification of voting systems.

My name is John Washburn. I have worked in the field of software quality assurance since 1994 and for the 10 years prior to that I was a computer programmer developing commercial software. Since 1998, I have held the certification, Certified Software Quality Engineer, from the American Society for Quality. For the last year I have been a technical advisor to VoteTrustUSA a nonpartisan national organization serving state and local groups working on election integrity.

I am here to present an outside assessment of the testing framework under which voting systems have been tested and certified to Federal standards from the perspective of a software quality assurance professional. I will address both the recently terminated program administered by the National Association of State Election Directors (NASED) and the program recently adopted by the Election Assistance Commission (EAC), established as a result of the Help America Vote Act (HAVA). It is important to consider both past and present testing processes for two reasons – first, all equipment currently in use has been tested under the former NASED/ITA testing process and most of this equipment will be used again in the next federal election. Neither program provides sufficient public oversight or accountability to ensure voter confidence that fielded equipment is in conformance with Federal standards. While the new EAC program has made some steps towards greater transparency and oversight, it retains some of the systemic flaws of the previous program.

I will also suggest a testing framework which can be implemented and administered immediately under the authority of section 241 of the Help America Vote Act. This alternate framework can executed in parallel with and in addition to the EAC framework.

The NASED and EAC testing and certification frameworks suffer from three systemic flaws, which I will explain in greater detail below.

1. Both systems are opaque to most primary stakeholders in the election process. These stakeholders are state election officials, local election officials, candidates for public office, and most importantly the voters.
2. Due to the lack of transparency and accountability, neither system adequately ensures the public that rigorous, thorough, and effective testing has been performed.
3. Neither system permits or encourages the reporting of system defects, nor do they include a responsive corrective action plan.

The System is Opaque

Under the NASED system, the entire testing process was a private sector transaction between the manufacturer and the testing laboratory, shielded from public oversight by vigorously enforced non-disclosure agreements. The reports of test results, as well as documentation of the testing undertaken to confirm a voting system's compliance with standards are considered the property of the manufacturer of the system. In cases where reports have been shared with state or local election officials, the reports have been routinely exempted from open records requests because the whole report is considered a trade secret rather than isolated sentences and paragraphs therein. After considerable effort I have been able to obtain redacted copies of some reports from the Wisconsin State Elections Board, but it is extremely rare for citizens to gain access to even redacted reports.

Trade secret protection is established by the manufacturers in the contracts they negotiate with jurisdictions purchasing their equipment and recognition of the manufacturer's claim to trade secret protection continues in the EAC program as well, as described in the Voting System Testing and Certification Program Manual. A complete copy of this manual can be found in Appendix A of my testimony.

The fact that complete documentation of test plans and results are treated as trade secrets means that necessary evidence to verify that a system is fit for use in administering an election is unavailable for public inspection and oversight.

While some states have the resources to undertake their own state level testing and certification, many states rely entirely upon national certification to ensure that systems that are purchased are in conformance with Federal standards.

Also considered a trade secret and thus closed to public review under both the past and present system is the testing harness itself. What specific tests are done to see if a system meets the requirements of paragraph 5.3 of the 1990 FEC Voting system Guidelines? How is the system identified and where is the physical configuration audit located so a state or local election official can verify the system which was delivered to him is the same system which was certified? Where is the list of types of software inspected? How is the source code inspected? All of these questions of how the testing and certification are done are considered trade secrets and closed to review.

The number and nature of the defects discovered in the testing process, as well as how and if the discovered defects were repaired is also considered a trade secret

For jurisdictions without state-level testing and certification, all that is available is a list of systems which have been granted certification numbers and the assurance that NASED has ruled that the certified system is in conformance with the standards.

Without the test plans and results of the test executions there is no evidence. There is only an appeal to authority. The inadequacy of the test plans, methods, and documentation in independent reviews of testing labs like the one commissioned by the New York Board of Elections, and the non-conformance revealed in penetration attacks and academic reviews has undermined confidence in that authority.

The Testing is not Rigorous

Over the last several years numerous security and design defects have been uncovered by independent researchers and election officials. Each of these discoveries has left unanswered the simple question: How did these non-compliant systems ever get certified?
Here are four examples:

1. Use of a programming technique called "interpreted code" is prohibited by both section 5.3 of the 1990 FEC Voting System Standards and section 4.2.2 of the 2002 Voting System Standards. This prohibition is extremely important because the use of interpreted code makes it easy for someone to change the operation of the voting system on the fly in the field. But, in spite of this prohibition, Diebold systems with interpreted code were qualified by NASED on 11 separate occasions over a span of 3 years. Details of this violation can be found in Appendix B of my testimony.
2. A member of the Technical Subcommittee of NASED's own Voting Systems Board has stated that the vote-tabulation software found on ES&S equipment varies from machine to machine and from election to election because for each election jurisdiction and for each election in each jurisdiction, a new and unique version of the vote-tabulation software is created. This is a violation of sections 8.7.1 Volume I and Appendix B.3 of the 2002 Voting System Standards and sections 9.7.1 Volume I and Appendix B.3 of the 2005 Voluntary Voting System Guidelines. These four sections relate to the identification of the software being certified. If the software changes from election to election how can any version be – "**the**" – certified version? Details of this violation can be found in Appendix C of my testimony.
3. The central election management system from Sequoia, which accumulates the vote totals, includes both source code and the compiler for that source code. This is violation of section 6.4.1.e of the 2002 Voting System Standards and a violation of section 7.4.1.e of the 2005 Voting System Guidelines. The prohibition against the use of source code and compilers in election systems is as important as the prohibition against interpreted code. They make it easy to change the operation of the software on the fly in the field. For details about this violation, see Appendix D of my testimony.

These examples of non-conformance went undetected in multiple rounds of testing conducted over the course of years. Because these violations were found without the benefit of access to test results, I cannot help but wonder how many other violations those results might reveal.

The 2005 Voluntary Voting System Guidelines (VVSG) are stronger than the 2002 Voting System Standards but the 2005 VVSG are still a very weak standard. It has been stated to this committee that the move from the NASED framework to the EAC framework is analogous to moving from college ball and profession ball. This is incorrect. The proper analogy is that the move between the two testing frameworks is the same as the move from sand lot baseball to little league ball. As with little league ball, the 2005 VVSG and the EAC testing framework are the first effort to operate with consistent rules and introduce an umpire to call balls, strikes, and fouls. Since the 2005 VVSG do not require a voting system be as reliable as an incandescent light bulb, the EAC framework has a long way to go before it is in the major leagues.

The profound and real world consequences of this illusion of testing can be found at the one hour and nine minute mark of the documentary, ***Hacking Democracy***. In a realistic simulation of an election, the outcome of the mock election is altered in spite of the election officials following all of the proper election administration procedures. This manipulation of the mock election would not have been possible if the voting system, which NASED declared met the 2002 Voting System Standards, had actually met those standards. A copy of this DVD is included with my testimony.

The System Does Not Promote Self Correction

The NASED testing frame work provided absolutely no mechanism to report problems and no way to receive suggestions for improvement. The EAC has created a new program called the QMP, Quality Monitoring Program, which is defined in chapter 8 of the Voting System Testing and Certification Program Manual; Program manual for short. Excerpts of this manual are included in Appendix A of my testimony.

The EAC's Quality Monitoring Program falls far short of any professional quality monitoring program I have encountered, both in its effectiveness for addressing testing deficits and in its implementation of corrections.

First, the Quality Monitoring Program limits itself to ***fielded*** systems, which are defined broadly in Chapter 1 of the Program manual. This definition is contracted throughout the rest of the Program manual such that only systems which have been certified by the EAC and are used in a federal election are considered ***fielded systems***. Since the EAC has not yet certified any systems, no system currently in use meets this definition. This means that any system in use in 2006 and the vast majority of those that will be in use in 2008 do not qualify for assessment under the EAC's Quality Monitoring Program. Thus, the Quality Monitoring Program fails to meet the mandate laid upon the EAC by section 202 of HAVA to be a clearinghouse of information on ALL voting systems, not just those which meet the limited definition of fielded. Section 202 of HAVA can be found in Appendix F of my testimony.

Second, the Quality Monitoring Program will only record ***anomalies*** as defined by section 8.7.3 of the Program manual. The definition of an anomaly in this section is exceptionally narrow. It permits the dismissal of any report on the basis that the report is an "administrative error" or a "procedural defect".

In contrast, the common practice in the software quality industry is to report and record everything and classify and categorize later. Applying gate keeping definitions such as those found in section 8.7.3 of the Program manual are not only frowned upon in professional software quality assurance, such gate keeping can be regarded as a sign of manipulating the QA process.

Two examples from last year suffice to demonstrate the power the gate keeping aspect used to define an anomaly.

One of the more interesting failures of a voting system last year was in Pottawatomie County, Iowa. The details of this can be found in Appendix G of my testimony. A programming error caused the election system to incorrectly tally the results of 10 races on the June 6, 2006 primary ballot. This error does not meet the EAC's definition of an anomaly because it was ruled the pre-election testing done by Ms. Drake, the County Auditor, was insufficient. Since insufficient testing is a procedural deficiency, the failure of the system to correctly tally votes is not considered an anomaly.

Similarly, the mysterious 18,000 vote under count in Sarasota County would not be considered an anomaly because the official explanation is administrative error. The Sarasota County Supervisor of Elections, Ms. Dent, laid out the ballot pages poorly and it is speculated that this

administrative error led to the 18,000 under votes. Such administrative errors are not considered anomalies and will not be included in the Quality Monitoring Program.

Finally, the EAC has adopted a limited definition of ***credible report*** found in Chapter 9 of the Program manual, which may further hinder the effective recording and response to system deficits. Only ***credible reports*** will be published and distributed to other election officials by the EAC under the Quality Monitoring Program. Information in a credible report must first meet the definition of anomaly. Second, only election officials may file such reports. Third, the events included in the report had to have happened during an election.

If an election official discovers defects in a voting system during pre-election testing or during other testing, this also is not a credible report because it did happen during an election. If an election official were to undertake an independent review and report the security vulnerabilities they uncovered, neither report would be shared with other election officials, because their information does not meet the definition of a credible report. Even though they are election officials, the failures they may find did not occur during an election.

Lastly, the new, untried EAC framework for testing actively resists opportunities for improvement in two ways. The testing plan used to determine if a system meets 2005 VVSG can only be improved based on credible reports. Without such credible reports the NIST has no authority under the provision of Handbook 150-22 to require the labs to improve their testing methods. This provision could inhibit correction or improvement of the testing process. The second way the EAC framework resists improvement is the long lead time needed to make even modest improvements to the standards. For example, in the 2007 standards currently under formulation the modest proposal that voting systems work as described in user and technical manuals was not approved as a guideline. Thus, the soonest this modest requirement can be come part of a standard is 2009 and would not applied to any system prior to 2011.

A Better Way.

While I have been quite critical of the EAC model of testing using slowly changing standards, there is great value in such testing. But, it must be seen as the minimum base and nothing more.

All good software testing follows several general principals:

1. The tests are by design. The design is the tester's design not that of the developer. Testing is not a haphazard or ad-hoc process.
2. The tests are designed to discover defects not success. The operating assumption of effective testing is the system and software under test has defects, and it is the tester's job to discover where.
3. Tests predict expected results. If you are not counting every stroke, it is not golf. If you are not calling your pockets it is not pool. If you are not predicting results, it is not testing. Without prediction there is no testing only documentation.
4. The test results – good, bad, or ugly – are recorded accurately and immediately. Categorization as to cause and relevance is postponed until after the defect is recorded.
5. The test plans and test results form a body of evidence which supports the claims made about the system tested.
6. The system under test can be positively and affirmatively identified.

The NASED framework and the proposed EAC framework fail all six of these simple precepts. Even at this late date there is the possibility the EAC framework can be changed to incorporate these precepts of good software testing. Unfortunately, there is not much time before the primary season for the 2008 presidential election begins. Because of this short time, I propose the EAC use the authority already granted to the Commission under section 241 of the Help America Vote Act to set up a second parallel framework for testing. The details can be found in Appendix H of my testimony. A brief description follows.

The HAVA 241 testing framework purchases a pool of voting equipment. The pool of systems would be identical to those purchased by local election officials. The pool of systems would be made available to academics and others from the public in order to execute tests on the systems. The access to the systems would be granted by auctioning, random lot or some combination of both. The stipulation for testing is that all contact with the equipment is recorded in full video and sound so there is no dispute later as to what was or was not done. These recordings are then available to anyone for a modest reproduction fee.

This HAVA 241 testing framework would be effective and efficient and would preserve the intellectual property of the equipment manufacturers. It would be effective because there is currently a backlog of testing to be performed which only requires access to equipment. It would be efficient (finds the most new information in the least time) because those who bid high are those who have the greatest confidence of their success and paying for access fosters efficient use of time.

In Conclusion

The NASED testing framework

- is opaque to every stake holder in election equipment except the manufacturers
- gives the illusion of rigorous testing without the substance, and
- resists to reports of problems or suggestions for improvement.

The new, untried EAC testing framework has these same, deep flaws.

Before the first system is granted certification the EAC framework needs to be substantially re-structured to remove these systemic flaws.

In the meantime, an alternate testing framework needs to be created. I have suggested one such framework which is more nimble, more effective, and more efficient than either the NASED framework or the EAC framework.

Explanation of Acronyms

DRE	Direct Recording Electronic
EAC	Election Assistance Commission
HAVA	Help America Vote Act
ITA	Independent Test Authority
NASED	National Association of State Election Directors
NIST	National Institute of Standards and Technology
NVLAP	National Voluntary Lab Accreditation Program
QMP	Quality Monitoring Program
VSTCP	Voting System Testing and Certification Program
VSS	Voting System Standards
VVSG	Voluntary Voting System Guidelines

Mr. CLAY. Thank you.

STATEMENT OF MAC J. SLINGERLEND

Mr. SLINGERLEND. I will loan a couple of my minutes to a couple colleagues that used a couple extra minutes, so we can stay on track here. We realize that we didn't predeliver a standard written statement, and thank you, Mr. Chairman and Mrs. Maloney, for having us here today.

This was not to offend or otherwise indicate a lack of cooperation on CIBER's part. A letter by the committee was sent to us 10 days ago, faxed last Saturday, handed to me last Monday afternoon, but for me, last week was a board of directors meeting and a shareholders meeting, so as soon as those were over, I began to work on this activity.

That said, I contacted Tony Haywood and discussed today's hearing, changed my schedule and that of John Pope, who is the left of me. I spent the weekend preparing and getting further updated on what has been going on in this activity of our company, so I could be here.

Ladies and gentlemen, we have nothing to hide. We are a 33-year-old New York Stock Exchange billion dollar IT services company with 8,000 people in 18 countries and a 96 percent customer satisfaction rating.

The business we are here to discuss represents about one-quarter of 1 percent of what we do. That said, we take all of our business seriously. I am, and have been, at least generally familiar with the questions asked of us in the chairman's letter to be here today. I cannot say I know every detail of any one project but I have prepared and believe I can speak with you today about the matters you are asking.

With respect to the New York Board of Elections, and Mr. Kellner, in particular, and I have read his criticisms, in part, of us, or one of our counsel, we have nothing except good things to say about the State of New York's activity with respect to electronic voting.

They have taken their responsibility seriously. They picked a good company to do the work for them and they have been victims, I believe as have we, with circumstances primarily beyond our control since some time, in particular, in 2006.

We have done good work for them and it is currently on hold. In our opinion, we should either finish the work or perhaps be paid and asked to go away, but in any case, we are happy to do either, as directed.

With respect to the EAC, this is a more complicated situation. The EAC, like we, and our customer, have been caught in the middle of changing responsibilities, changing technology, changing test procedures, likely a lack of sufficient funding for the EAC, and changing testers.

Specifically, we have dealt with moving targets, slow turn-around times on assessments, and a general lack of sufficient direct EAC resources, such that they have to rely on others, and then part-time others, nondirect, and inexperienced auditing, in part, to help them with their systems and their accreditation.

In conclusion, some of the tabloids have been accurate; some not. I think some of the statements Mrs. Maloney made this morning weren't exactly—I would say accurate, from the standpoint that you were led in the wrong direction, not that I would criticize anything you had to say, but relying on some statements that weren't accurate. Therefore, your questions came from that standpoint.

It appears that there are multiple agendas that our customer, the New York State Board of Elections, and we, are affected by, and perhaps this meeting this morning will push these to resolution.

Thank you for having us here today.

Mr. CLAY. Thank you so much, Mr. Slingerlend, and Mr. Pope, for being here. We appreciate your accommodating the committee. Let me go to the 5-minute questioning now and I will start with Mr. Kellner, and let me first thank the entire panel of witnesses for the expert testimony that you have just provided.

Mr. Kellner, in light of CIBER's inability to earn interim accreditation from the EAC last year, what are the major issues New York is currently facing in using the nationally accredited Voting System Test Labs for the upcoming election cycle?

What are the timelines that are necessary to adequately address the EAC's accreditation process in order to ensure a smooth election cycle for 2008?

Mr. KELLNER. Congressman, the New York State Board of Elections has issued a RFP to accredited laboratories and the deadline for response to that is next week or so, and we will be very shortly then evaluating our options on restarting the testing process as soon as possible.

We would hope that within the next couple of months, we would be able to restart the testing process.

Now hopefully, the vendors have used this time delay of the testing process to get their equipment up to snuff, so that when the testing process resumes, the equipment will pass, and if that happens, then we expect that we would be able to certify to the county boards of elections acceptable voting systems by this December, and that would be in sufficient time for them to acquire new voting systems for the 2008 primary in September and the general election in November 2008.

Mr. CLAY. Pardon my ignorance. Is New York involved in a February 5, 2008——

Mr. KELLNER. That is correct, Congressman.

Mr. CLAY. OK. So they will not be ready for——

Mr. KELLNER. That is correct; not for February.

Mr. CLAY. OK. One topic that I believe does not get enough attention in the larger debate over system integrity and security is the topic of information sharing about system flaws.

As the national clearinghouse for election information, what role should the EAC play in developing stronger mechanisms for sharing information among election officials about system flaws that are identified by officials or industry stakeholders?

And anyone on the panel can attempt to answer that.

To followup, should the EAC work together and disseminate information about flaws not found through its prescribed national

certification processing, including NASED qualification for upcoming elections?

Yes, Mr. Washburn. You may start.

Mr. WASHBURN. My customary experience with software testing, when you are reporting and recording defects, is to record everything and then categorize later. That is why I am particularly disturbed with the gatekeeping functions on the definition of anomaly.

So I guess my opinion would be is that the EAC should take a report of everything, from everyone, and vet those out, and then categorize them as credible, not credible, after the fact, because many times, it's in the pattern of the minutia, in the pattern of the many reports, that you actually see something—ah, there is a recurring issue here in some administrative—you know, even though it may be an administrative error, it is one that everyone's having.

So the general custom in software testing is to record everything immediately and then categorize, prioritize and essentially cite its significance later.

Mr. CLAY. Do you think the response time is quick enough? Is it timely, to flaws and problems?

Mr. WASHBURN. We are under a very short timeframe for the 2008 election cycle. I am not sure, even if they started setting up a very high end, you know, defect reporting system like ClearCase, you know, tomorrow, I doubt that the responses—it would be better, but I don't know if it would be enough to correct the systems. But it would at least allow the local election officials to know what problems to watch for and perhaps adopt local procedures to help avoid them and mitigate them.

Mr. CLAY. Anyone else? Mr. Norden.

Mr. NORDEN. Chairman Clay, I just wanted to add a couple of things. Certainly, there should be some process for all systems, including NASED-certified systems, to get reports from election officials, and I would add, as I said before, also from voters who are voting on these machines and are actually using them on election day, about things that go wrong with the system.

Another thing I would add is that as I understand it right now, if election officials file a report with the EAC and that report is deemed credible, there is no way for the election official to have that complaint made anonymous, and that seems to me to be a problem, for a couple of reasons.

No. 1, the election official that may be filing the complaint is often the one who bought the system. So they might have an incentive for not wanting that to be attributed to them. They are also reliant on the vendors for technical assistance in the future, and we have instances in the past, where there has been retribution against election officials for making complaints, or showing the vulnerabilities in voting systems.

So I would say three critical things would be providing some way for there to be anonymous publication of these complaints from election officials, if they requested, include voters in the complaints that are taken, and make sure that there is a clearinghouse for all systems, not just the ones that have been, or are going to be certified in the near future.

Mr. CLAY. That is a great point. In Congress, we also deal with that same issue when it comes to HAVA, from the original authors

who don't want any alteration of HAVA, but we know it is much overdue and needed.

Let me ask Dr. Wagner, many people compare computerized voting machines to bank ATM machines. They argue that these bank machines are perfectly safe and accepted by the public.

Therefore, we should have the same confidence in computerized voting machines. Are these voting machines constructed with the same security as bank machines and is the physical security of voting machines the same? What are the differences in the security and reliability standards and would using such security standards enable us to better test and evaluate e-voting systems?

Dr. WAGNER. Thank you. First, I would say that our voting systems are not up to the standards in the financial system that we are using to protect our bank ATMs.

Second, I would say that the voting problem is a much more challenging problem than the problem of securing bank ATMS because of the secret ballot. If we didn't have a secret ballot, we may be able to apply some of the techniques from the financial world, which include associating names, multiple paper trails, and auditing those, cross-checking them.

But because of the requirement for a secret ballot, we are much more constrained in the voting world by what kinds of audit logs we can keep, so it is much more challenging to provide the necessary level of security in the voting world.

Mr. CLAY. Thank you so much for that response.

Representative Maloney, your turn.

Mrs. MALONEY. Thank you, and I really thank all of the panelists. I particularly would like to thank Mr. Kellner and Mr. Norden who are from the district and communities that I have had the honor to represent, and they have been longstanding advocates for voter reform, machine reform, honesty in voting, and I congratulate all of your efforts.

I congratulate all of your efforts. I am just more familiar with theirs since they are from my city.

Mr. Slingerlend, I understand that you have already responded to many of the concerns raised in the initial EAC assessment review from last July. However, the EAC review and the NYSDEC review commissioned by the New York Board of Elections, described the state of your testing methods and procedures that prevailed during the period in which you were testing most of the voting system software in use across the country. These independent reviews suggest that CIBER is unable to adequately document the testing undertaken to establish the conformance of voting systems to Federal standards.

Are you able to document the test plans, methods and results of testing performed under the NASED/ITA program?

Mr. SLINGERLEND. Thank you. I think the answer to that question is yes. If I may, in kind of a broader sense, say how we got to where we were, and my comment on, by the way, one of your earlier comments that we have certified machines, we have never certified machines, and unfortunately for Commissioner Clay, it says regained accreditation from the EAC, well, we have never had accreditation from the EAC so we don't regain that either.

But in some respects, we have been involved in this business for a decade. We have been involved in the business under the NASEd leadership and it was completely voluntary because I think the Federal Government just did not adequately approach this subject, historically, and consequently the States found it necessary to take it on themselves, although there were a few Federal standards that they were identified with.

I have talked to myself, if you will, about this, over the weekend, saying that, you know, we were lulled to sleep by the process, which wasn't our fault. The fact that we slept probably was our fault. I think the individual, in particular, that was leading this effort for us, was like a cook that doesn't have recipes. He knew the systems very well. He knew the vendors very well. He knew everything very well. He behaved in pretty much the same manner for the last 5 or 10 years, as far as how he was testing machines, and going through his procedures.

But the documentations of his efforts were not what you or I would call "buttoned up," to a standard that would be acceptable, and when the EAC came around last summer with respect to testing to a standard, it was a new standard, hadn't been used previously, which was OK. I would say that we weren't documenting things, that we were physically doing. Nobody has ever questioned the quality of our work, or the fact that we have tested things, or attested to things accurately.

The documentation to that, of that fact, though, is not as good as it should have been. We spent the summer, probably early fall, after we were told about this, getting things, if you will, buttoned up, perhaps not completely but substantially better. The EAC came back—and I am feeling like I am running out on my answer but there is a timeline here. The EAC came back in early December and asked to review what progress we had made, and said you guys have made tremendous progress, but now we also need you to meet the 2005 standards. So the people that were certified by the EAC, last summer, weren't asked to meet the 2005 standards, and we have buttoned ourselves up for 2002. We were then told we had to be—2005. Then it was February before we get another response. We turned back in a—and asked by EAC to respond by March 5th. We further responded on February 26th, which is—you can, you know, take the months now, but it is 2½ months, or whatever that might be. We still have not heard back, the status of that submission.

So, you know, we feel for the State of New York. You might even say we feel for ourselves. But I do believe at this point, we are fully capable of meeting the 2002 standards as the other currently accredited companies are doing, or have been accredited to.

Mrs. MALONEY. OK. I would like to submit a formal request on behalf of the subcommittee for documentation related to the testing by the CIBER of NASED-qualified systems, and it is a documentation request for each of the systems listed before. If you would produce the following set of records.

Mr. CLAY. Without objection.

Mrs. MALONEY. I would like to submit it to you, and to the record. Thank you.

[The information referred to follows:]

CIBER Document Request

For each of the system listed below please produce the following sets of records:

1. The date the system was initially presented to the laboratory for testing
2. All reports submitted or otherwise delivered to the NASED Voting Systems Board by the Laboratory.
3. All reports submitted or otherwise delivered to a particular individual member of the NASED Voting Systems Board by the Laboratory.
4. All reports submitted or otherwise delivered to the Laboratory by the NASED Voting Systems Board.
5. All reports submitted or otherwise delivered to the Laboratory by any individual member of the NASED Voting Systems Board.
6. E-Mails, written correspondences, or other communications between the Laboratory and the NASED Voting Systems Board.
7. E-Mails, written correspondences, or other communications between the Laboratory and any individual member of the NASED Voting Systems Board.
8. All reports submitted or otherwise delivered to the equipment manufacturer by the Laboratory.
9. All reports submitted or otherwise delivered to the Laboratory by the equipment manufacturer which relate to the repair and cure of defects found by the laboratory.
10. E-Mails, written correspondences, or other communications between the Laboratory and the equipment manufacturer which relate to failures to conform to standards or other defects found in the system under test.
11. E-Mails, written correspondences, or other communications between the Laboratory and the equipment manufacturer regarding the interpretation of how or if elements of a voting system standard apply to the system under test.
12. E-Mails, written correspondences, or other communications between the Laboratory and the NASED Voting Systems Board regarding the interpretation of how or if elements of a voting system standard apply the system under test.
13. The test plans, traceability matrix, test scripts, and other documents which demonstrate the system under test conforms to each element of the voting system standard applied to the system under test.
14. The date, location, and persons present at the witness build performed by the laboratory for the system under test.
15. For systems tested to the 2002 VSS, a copy of Physical Configuration Audit document created pursuant to section 8.7.1 of Volume I of the 2002 VSS.
16. For systems tested to the 2002 VSS, a list of the cryptographic hash values of the configuration items enumerated in the Physical Configuration Audit document pursuant to section 8.7.1 of Volume I of the 2002 VSS.

Please produce the 16 sets of documents described above for each of the following NASED Qualified systems:

N-1-02-12-11-001
N-1-02-21-21-002
N-1-02-22-22-003
N-1-04-12-12-001
N-1-04-12-12-002
N-1-04-12-12-003
N-1-04-12-12-004
N-1-04-12-12-005
N-1-04-22-22-001
N-1-04-22-22-002
N-1-06-12-12-001
N-1-06-12-12-002
N-1-06-12-12-003
N-1-06-12-12-004
N-1-06-12-12-005
N-1-06-12-12-006
N-1-06-12-12-007
N-1-06-12-12-009
N-1-06-12-22-008
N-1-06-22-22-001
N-1-07-12-12-001
N-1-07-22-11-001
N-1-07-22-11-002
N-1-07-22-11-003
N-1-07-22-11-004
N-1-07-22-11-005
N-1-07-22-11-006
N-1-07-22-11-007
N-1-12-22-12-001
N-1-12-22-22-002
N-1-16-22-12-001

Please produce the 16 sets of documents described above any system which has begun the NASED qualification process, but for which no NASED System Qualification Number has been issued.

Mrs. MALONEY. Mr. Slingerlend, is there any reason why the testing process and test reports should be done in secret?

Mr. SLINGERLEND. I have listened to some of the comments about the—I will probably say no to the question, with the exception of that it is a very iterative process, and one can draw conclusions. It is a little bit like Donetta Davidson was saying earlier, that you are not always sure the information that you are getting is accurate, so you are not quite sure you want to publish it, until you have the ability, yourself, to verify whether it is accurate.

And for Mr. Washburn and I—and he and I obviously don't know each other—but I am sure that he has been through lots of testings of software, over time, just based on his testimony, and it is an iterative process.

What we have found, and what has been explained to me about what we have done with the vendors in the past, they may give us something, we say, well, that doesn't meet Federal guidelines. And so you go back and forth, and back and forth. You may do it 50 times.

I don't know that it is healthy, or wise, or necessary, to indicate the status, sort of an iterative process between a vendor and a testing lab, whether it is NIST, whether it is ourselves, etc. And by the way, we have no problem with the concept that any vendor money would go to NIST or EAC, and then they would select people to do testing. That means nothing to us.

Mrs. MALONEY. But once you have tested and sent the results to EAC, why shouldn't the public be able to verify that the testing, see what the testing was, to see if it was done properly or not? Why keep that secret? When you are in a "give and take," I can understand. But once you have made a decision and relayed it to EAC, why not have that open to the public, as the prior two panelists said, should be open to the public?

Mr. SLINGERLEND. I think that sounds fine with us. I mean, I think from our standpoint, we have never certified any machine works. We have attested to the fact that it has met Federal guidelines. The fact that we say something meets Federal guidelines, we have no problem with that information being public, ourselves.

Mrs. MALONEY. OK. Did CIBER serve as the independent testing authority for the ES&S Unity System that was certified by the National Association of State Election Directors in 2003 and 2004?

Mr. POPE. Yes, ma'am. I believe that is correct.

Mrs. MALONEY. OK. Did CIBER do a review, at that time, to determine if the source code used in the ES&S Unity System complied with the 2002 voting system standards?

Mr. POPE. I am not the technical expert on that. We would have to ask our technical folks about that.

Mrs. MALONEY. But you were reviewing and testing to see if they met 2002 standards; right?

Mr. POPE. Yes.

Mrs. MALONEY. But you can't say whether or not you tested to see whether they met 2002 voting system standards?

Mr. POPE. I believe that is a correct statement but I would like to have the chance to verify that.

Mrs. MALONEY. Well, could you verify and get back to the committee on whether or not you tested to see if they met the 2002 standards?

Mr. POPE. Yes, ma'am.

Mrs. MALONEY. Now you testified that you believe they did since it was certified in 2003 and 2004. So my question is really, how does CIBER explain the ES&S request to the New York State Board of Elections for a waiver of these standards? So when they came to New York, they asked for a waiver of the 2002 voting system standards.

Mr. POPE. That issue is between ES&S and the State of New York, not between us and ES&S.

Mrs. MALONEY. Well, were there other standards in the 2002 voting system standards, that CIBER did not test? We are talking about testing—70 percent of the voting machines out there now were tested by CIBER. Now, because of the GAO report, and it is not my words, I was quoting from the GAO report, the GAO report said that they were not done properly. We just heard, from the prior two panelists from the Election Commission, that they are not going to have to recertify all of those voting machines to the standards.

So I want to know, are there standards in the 2002 voting system standards that CIBER did not test?

Now you testified earlier that you are working now to get up to the 2005 standards. But were there some standards that you eliminated, or did not test in the 2002 voting system standards?

Mr. SLINGERLEND. Ma'am, I don't think we have ever—first of all, I do believe we tested everything with respect to 2002. Nobody has ever indicated that we haven't tested everything with 2002. The issue has been with the documentation with respect to the testing, not the fact that testing wasn't done, or that the systems didn't work to Federal standards.

Mrs. MALONEY. OK. Then if I could have an additional minute for one question, Mr. Chairman.

Mr. CLAY. Please proceed.

Mrs. MALONEY. What individual, or individuals, are responsible for carrying out and supervising the testing of voting systems at CIBER?

Mr. SLINGERLEND. Historically, that responsibility has fallen, in Huntsville, AL, under a name, Sean Southworth.

Mrs. MALONEY. Prior to serving in this capacity, what were Mr. Southworth's qualifications and how was he chosen for this role?

Mr. SLINGERLEND. Ma'am, I can't tell you that. I can tell you that he has been doing it for approximately 10 years. We made an acquisition in October 2001, and this was a small portion of that company, and it was an ongoing activity of that company. It wasn't the target of the acquisition but was an ongoing activity of the company at the time. They had been doing it for several years, are very familiar with NASED, the people involved in NASED, and continue to do the work they had been doing prior to the acquisition, after the acquisition.

Mrs. MALONEY. Could you please provide the subcommittee with Mr. Southworth's biography, resume, documents attesting to his qualifications to perform voting system testing.

Mr. SLINGERLEND. Sure.

Mr. CLAY. Thank you very much, Representative.

Mr. Slingerlend, first, could you please characterize for us the meaning of the term "confidential, competition sensitive." Does this mean these documents have trade secrets or proprietary information? Why was there not adequate justification made to the board for these designations?

Mr. SLINGERLEND. My understanding, in part, with respect to the software work that we perform, we believe that the way we perform the work we were doing was unique to ourselves and consequently, you would tend as a business competing with other business and having competitors and testing, that you don't like to release those testing procedures to other companies, in particular.

I think the whole activity that—now that EAC is here, now that NIST is here, I think that whole program can change. I don't have any particular reason, other than just we didn't find it necessary to disclosure how, if you will, Sean Southworth was doing his work to our competitors.

Mr. CLAY. Now according to the New York State Board of Elections, CIBER had been submitting reports to the board, that were paid for with New York State funds, but were somehow restricted from public disclosure.

It seems to me as though CIBER was looking to prevent public scrutiny of its work.

Mr. SLINGERLEND. Yes. I don't think there is any intent to that. I do believe that Mr. Kellner talked to one of our attorneys, but Mr. Kellner, I did not verify that. I am happy, if you want to comment on this, and I believe that the discussion between Mr. Kellner and our attorney was such, that we removed the confidential labeling of the documents and they were made public. If that is not the case—I don't know that is not the case.

Mr. CLAY. OK. Well, we will let Mr. Kellner respond. Go ahead.

Mr. KELLNER. Mr. Chairman, I think the problem is that the habit of CIBER was to keep everything secret and confidential, and New York's process has been to keep everything open to the public, and CIBER really wasn't prepared to deal with that, and I was not satisfied with the way my requests were handled in terms of telling them, look, you have marked all this stuff confidential, I want to release it.

And we had a report that had been very carefully negotiated between New York's independent technical experts, the New York State Technical Enterprise Corp., and CIBER, on the extent of the COTS exemptions for source code testing, and CIBER insisted that agreement that they had be marked confidential, and then the lawyer at CIBER, when I protested this, rewrote the report, not the experts but the lawyer rewrote the report, and then said, here you can release this version that I've cleaned up.

And I really thought that was an inappropriate way to deal with an expert report, and of course the New York State board then, following the complicated legal procedures in our State law, disclosed the report, but only after we went through the formal procedures to determine that CIBER had no right to claim confidentiality for the agreed report.

Mr. CLAY. Thank you. Thank you for that response.

Mr. Washburn, any commentary or thoughts about the testimony?

Mr. WASHBURN. It is my amateur legal opinion, but I don't think trade secrets apply in voting systems for the test procedures, because that is the evidence that it does conform. You are talking about public moneys spent for the, you know, spent by public officials to administer public elections, for candidates to public office. What part of that is private?

And so I don't think half of the trade secret definition is met, because part of trade secret is subject to reasonable efforts to keep secret, and it is unreasonable to keep secrets here.

Mr. CLAY. Thank you for that response.

Mr. Slingerlend, I picked up on something that you said, that I am really concerned about, when you say that there were first 2002 standards and now there are 2005 standards, like this, and it seems to me like there is a moving ball or a moving target that the industry has to keep up with.

But what I find to be so disconcerting is that, you know, we are talking about the public's voting rights, the integrity of elections, making sure that we get it right once, the first time, making sure that people's votes are accurately tallied, that they are actually counted.

I mean, is this a process that we will never be able to satisfy? Or can we get this right?

Mr. SLINGERLEND. Sir, I believe it certainly can be done. If I took off my CIBER hat for a second and I just put on my American hat——

Mr. CLAY. Put on your American cap.

Mr. SLINGERLEND. I do think that when you look back, then, how this was done over time—and you should give credit to Ms. Davidson and the other people of NASED, that took their time, unpaid, etc., to work on having these machines certified to some level of Federal standard over the last decade, I think this has just been, you know, the minister's kids without shoes. You know, it is just basically a system that has been neglected, in an official sense, as it should have been done, over time.

I don't know that the two thousand and—you know, we were certified as the 1997 standards, the 2002 standards were better but certainly not adequate, we are sitting here today being told the 2005 standards are better, but by July 2007 there is even going to be better ones.

And when we were asked, which we had never been asked to behave in a certain manner, as I said we were kind of lulled to sleep, not our fault, but the fact we slept is—when we were asked last July to go through a testing process that our guys hadn't done before, weren't behaving in a manner that they would qualify for "our fault," but doesn't necessarily mean that they hadn't been, you know, basically steered in that direction.

When we came back for retesting, it was yet a different set of rules, after submitting first answers, and then there is a different set of rules, and now it has been from February 26th to May 6th or 7th, and we haven't heard about our last response because EAC really hasn't had the funding, the full-time auditors, NIST isn't quite on the ground—and that is not trying to criticize NIST.

I think you have an evolving process here that is going to be much better, very quickly. But it has been not a great process over the last couple of years or the last few to several years.

Mr. CLAY. Thank you for that response.

Mr. Washburn, can you identify specific examples of e-voting systems that had previously been certified by the former NASED program, even though they were not compliant with the appropriate standards. If so, can you offer examples of the types of problems with each system, and are any of these systems still being used by local election boards?

Mr. WASHBURN. Well, all through the ones I gave, I cited in my oral statement, and also my written statement, are currently in use. So the use of interpreted code is prohibited by section 5.3 of the 1990 standards, it is prohibited by section 4.2.2 of the 2002 standards, and there were, I believe, 11 systems that have that property, that were tested over the course of about 4 years. I could get you the actual numbers, if you would like, of the systems involved.

Similarly, because of an open records request in California, it was discovered that one of the members of the technical subcommittee of the NASED voting systems board, stated that the ES&S scanners have a unique executable for every election, and there is no single version of the firmware. It changes from election to election, to election to election, because it incorporates the election information as a commingled integral part. You cannot separate the ballot definition from the scanner firmware. So it is always different.

And similarly, the Sequoia system, Win EDS, which is in use by a number of systems still in use, has source code in the form of Transact SQL, as well as the compiler for it which is Enterprise Manager.

And what this means is that you can alter the behavior of the stored procedures, triggers—I am probably getting a little technical here—but what the Win EDS system does is it just calls it by name. So whatever SQL is behind that name, that is what gets executed at that moment in time, and it may not be the same stuff that was delivered, it may not be the same SQL that was certified, and it may not be the same stuff that you audit, the day after.

So those are currently in use.

Mr. CLAY. Mr. Norden, what systems send out alarms for you?

Mr. NORDEN. I think Mr. Washburn did a pretty good job there.

Mr. CLAY. Got everything that you were concerned with?

Mr. NORDEN. Yes.

Mr. CLAY. And how about you, Doctor?

Dr. WAGNER. Well, I am a technologist, and I consider the question of what meets the certification standards a policy question. But I believe there is room for serious concern about a number of the systems from three of the four major vendors out there. The Princeton vulnerability testing has demonstrated serious security problems in machines from one vendor, which I think there is a credible argument, violates the standards.

The problem that we face today is that there has been no process and no attempt to investigate these claims. This has been a bit of a political "hot potato" that no one wants to touch, because if we

were to—if there were to be a finding that these systems did not comply with the standards, local election officials would be in a major bind.

So for that reason, the EAC has been reluctant to investigate these claims about—they perhaps reasonably have said NASED certified these systems, let NASED deal with its mess. NASED has been silent on this issue.

So we haven't come to terms. There has been no serious attempt to grapple with these allegations.

Mr. CLAY. Thank you so much for that response.

Representative Maloney, do you have any questions?

Mrs. MALONEY. That is truly horrifying, that there has not been any serious attempt to grapple with this, and everyone's hiding behind the fact that NASED certified it.

So I would like to ask Mr. Slingerlend, since he is involved in testing, is it fair to say that having certification from the National Association of State Election Directors does not necessarily mean that the voting equipment complies with each and every one of the voting standards?

Maybe let me back up a little bit. Did CIBER test the Diebold AccuVote TS optical scan terminals that were the subject of the reports by computer scientists at Princeton and the University of Connecticut that Dr. Wagner mentioned? Did CIBER test them?

Mr. SLINGERLEND. Do you know? I don't know.

Mr. POPE. We have tested Diebold systems but I'm not particular about the one that you mention.

Mrs. MALONEY. Well, the Diebold system is the one that Princeton and Connecticut hacked into.

Mr. SLINGERLEND. As Mr. Washburn said, is it the one that was tested, the one that was delivered, the one that was implemented, or as other people were saying, we have—they have been a client from time to time. That specific item, we would have to check into, ma'am.

Mrs. MALONEY. Well, maybe you could check into it and get back to the committee.

Mr. SLINGERLEND. Let me just make sure that I get the right question, so I get them the right answer.

[The information referred to follows:]

Mac J. Slingerlend
CIBER, Inc.
5251 DTC Parkway
Suite 1400
Greenwood Village, CO
80111

303-220-0100
Fax: 303-267-3899

May 8, 2007

Congresswoman Carolyn Maloney
2331 Rayburn HOB
Washington, DC 20515-3214

Dear Congresswoman Maloney:

Thank you for inviting us to participate in the hearing in City Hall on Monday.

I would like to revisit your question of "was a NASED certificate meaningless?" and my answer of "not meaningless, just not sufficiently meaningful." It is like a 1950 Buick and a 2007 Buick. They both were meaningful in their time, but the 2007 Buick has more features.

ciber

That said, CIBER's a very good company, but we were not documenting our good work in this situation. We were doing what we did over the years and what had been acceptable, but this is a new day and we needed to upgrade our processes. The EAC newly sponsored assessment sought more (and we have done those), but the EAC now wants 2005 items to get 2002 accreditation. This moving target has been a challenge to react to, and a catalyst for negative implications to all – and we are still awaiting a reply from our February 26, 2007 submission.

Lastly, we never certified "the machines," nor have we ever lost or been denied certification by either NASED or the EAC.

Please feel free to contact me if you believe I can assist you.

Sincerely,

Mac Slingerlend

Mrs. MALONEY. And isn't it true, that those reports showed security vulnerabilities that were not tested in the certification process, obviously, in the Connecticut and Princeton tests?

Mr. SLINGERLEND. Can I address what you are—the general topic of what you are saying right now. I believe with 100 percent, you know, certainty—and again I guess put the word "believe" there—but I believe we have done a fine and good job of testing the software in machines, not the hardware of machines, cause we have never been said to be testing the hardware of the machine. But the software of the machines to meet the 2002 standards that are out there.

That does not mean to say that the 2002 standards were as great as they should have been, or that they weren't changed in 2005, and it sounds like they are changing again in 2007. But I do believe that if we were asked to certify something, or attest to something, as to how it worked to 2002 standards, we did our job properly.

Those standards may not have been sufficient and that may be exactly your point.

Mrs. MALONEY. Prior to the time that you were suspended from further testing in New York State, did any of the voting systems submitted pass each of the tests that were given? Did any of the voting systems pass prior?

Mr. POPE. With regard to the State of New York, all the systems that we have tested are still in an incomplete state.

Mrs. MALONEY. All right. Let me go back to the question that, really, the point that Dr. Wagner raised, and just go down the panel, starting with Mr. Kellner, and let everybody answer.

Is it fair to say that having certification from the National Association of State Election Directors does not necessarily mean that the voting equipment complies with each and every one of the voting standards?

Can you replay to that, Mr. Kellner.

Mr. KELLNER. I think that is completely true. I think that everyone has to follow California's lead, and California's Secretary of State has announced that she is going to retest every single piece of voting equipment, and it is based on the bankruptcy of the 2002 standards testing that was done under NASED supervision, that NASED certification is meaningless.

Mrs. MALONEY. That is a powerful statement.

Dr. Wagner.

Dr. WAGNER. Representative Maloney, I think it is indeed fair to say. I would concur with your assessment.

Mrs. MALONEY. That NASED certification is meaningless. OK. Mr. Norden.

Mr. NORDEN. Yes, I would agree with that, and I would add a couple of things. That is one reason why having software independent records and audits is so critical.

And in addition, something that Mr. Kellner mentioned I think bears some further explanation. I am troubled by the fact that this system has been so—on top of everything else, and certainly, the security of our elections is the most important thing.

But on top of everything else, it has been an incredibly inefficient system, and we have States like New York and States like Califor-

nia not trusting Federal certification and having to run very expensive tests on their own. This is expensive to, obviously, the people of the State of New York, to the people of California, it is expensive to the vendors.

And what I would like to see is that, at some point, when we get these standards right on the Federal level, that this isn't just voluntary, that it is a mandatory thing that all of the States comply with, and that we can actually trust the certification process, so we don't have to go through what we have gone through in New York, so that we don't have to do the kind of additional testing that we do in California, unless there are very specific reasons for doing so.

Mr. WASHBURN. I too would agree that a certification number has no connection at all to whether that system complied or doesn't comply with the standards, and echoing Mr. Norden's point on the testing, the proposal I was talking about, that is in my written testimony, would propose that a consortium of States buy a pool of election equipment exactly as bought by election officials, and essentially allow anyone who would like to do a test on it, in a manner similar to, with access similar to what an election official has, the stipulation being is it has to be videotaped and audio recorded for everything you do, so there is no dispute what they did, what they didn't do, what the findings were, good, bad or ugly, whatever the result is.

And then that information could be made public and help election officials evaluate changes in the local security procedures.

Mrs. MALONEY. That is a very strong statement, if I understand what you said. You said no certification system up to this point can verify that the voting machines are meeting the required standards of 2002, not to mention 2005, that they are now required to meet.

Mr. WASHBURN. Well, I haven't looked at all of them. I looked at most of those that are sold in the State of Wisconsin. But I find problems with all of—I can find a section of the standards that the system does not meet for every one of those in Wisconsin.

Mrs. MALONEY. And Mr. Slingerlend, do you agree with the comments or Mr. Kellner, Dr. Wagner, Mr. Norden and Mr. Washburn, that the certification from the National Association of State Election Directors is not a certification you can rely on? Is it fair to say you are saying it is not workable, it is not doing the job?

Mr. SLINGERLEND. If you knew me better, you would probably know I disagree with most anybody. But I would go back to what these gentlemen were saying, and your question earlier was are they meaningless, and I think I would say these are good people doing unpaid work, not sufficiently funded or done by the Federal Government, doing the best they could.

I would say it wasn't sufficiently meaningful, but I'm not going to say it was meaningless.

Mrs. MALONEY. But back to Dr. Wagner's statement, you were saying that the EAC would not go back and look at these systems because they were certified by the National Association of State Election Directors. Is that what you said?

Dr. WAGNER. I can't speak for the EAC of course, but my understanding is that the position the EAC has taken is that they will not go back to investigate these allegations and systems that were certified by NASED, that they are developing a new process. If

manufacturers choose to submit their systems to the EAC's new process, then the EAC will investigate reports, may consider decertification, if that is warranted. They have developed a new process with these safeguards but those safeguards don't apply to the old NASED process.

Mrs. MALONEY. That is very discouraging. I would like, Mr. Kellner, just go down the line, for each of you to comment on what you have examined in voting systems that were certified, and do you think they are fine? Can we trust them? What are your statements? I will just get you on the record.

Mr. KELLNER. I certainly subscribe to the view that Debra Bowen in California has adopted, which is that we need to have recertification of every voting system that is in use in this country, and that is a responsibility Congress should give the EAC, and I would add that we shouldn't be spending a lot of new money to buy voting equipment until that process has been completed.

Dr. WAGNER. It is a difficult question with a complex answer. I would say despite the flaws and the deficiencies in the certification process, I believe that many of the systems out there, for instance, the systems that provide a voter-verified paper record, if they are used appropriately, can provide a good basis for trust in our elections.

However, I have serious concerns about the use of paperless e-voting systems.

Mr. NORDEN. I would echo exactly what David Wagner just said. If we are going to continue using these systems, and I think to a certain extent there is no choice, that for the next few elections we have to, we need to ensure that we have paper records and that we are using those paper records to check the electronic tallies that we get at the end of election day.

Mr. WASHBURN. I once knew a whitewater outfitter who used to say there comes a point in the river where there is no way out but through, and I think we are at that point with the current crop of systems. There is no way it is going to be fixed in time.

But that said, as Mr. Wagner said, certain systems are less vulnerable than others, and specifically what you want is a system that provides an objective record, that the voter has made, that might possibly contradict what the electronics are telling you. Systems that don't have that are inherently more vulnerable.

Mr. SLINGERLEND. I think paper systems are great for Third World countries. I like your comment about if you can't find a way I will go through it. I think we are on the cusp, with EAC and NIST, to making progress in an area that was never sufficiently addressed before, and you should press on.

I mean, I think that this country should press on with electronic voting system, and you have smart people that care, that are in charge of this activity now. Go with it. That would be my recommendation.

Mrs. MALONEY. Thank you.

Mr. CLAY. Thank you, Mrs. Maloney.

Let me thank all of the panel for their testimony today, and thank our gracious host, again, Representative Maloney, for inviting us here today. I think that the hearing brought out the fact

that we must be able to verify the reliability and security of our Nation's voting machinery.

The EAC, the States, and local election authorities, must work hand in hand to ensure that our elections are conducted in a manner that gives our citizens the utmost confidence in the election process.

Vendors of election machines should not be paying labs, and all machines must have a verifiable paper trail.

H.R. 811, introduced by Representative Holt of New Jersey, would apparently give us that extra protection, and Congress needs to move on it.

The certification process must be transparent, and sunshine must be allowed to expose the process. We must get the voting procedure correct the first time in New York and across this Nation, and I will yield to my friend for closing remarks.

Mrs. MALONEY. I want to thank all of the panelists for coming, and my colleague and good friend, Mr. Clay, for having this Federal hearing. It is obviously a critical issue. What is more important than the security of our voting machines? And it is a part of our democracy, it is a top priority and one that we will continue to pursue as a Congress and as a committee.

I am delighted that tomorrow, Congress Holt's bill, on which he has worked for 8 years, will be marked up in committee and I hope it will move to the floor and be passed. It will strengthen it and address many of the issues that you brought up today. The need for a verifiable paper trail to check the electronic voting. The need for checking conflicts of interest, that the payment by vendors will go to the EAC who will then select the testing labs to find out how accurate they are.

It provides funding for purchasing these machines, and for audits. It is very important to have an independent audit, to see if they are working properly.

All of you have helped move this country forward to a safer, more reliable voting system, and I thank all of you for your tremendous contributions to it. Nothing is more upsetting than hearing questions about more people voting than were registered and more people voting than signed up to vote on the machine, and all types of really questionable items, that really, you expect to be happening in Third World countries, not in the great democracy of the United States.

So we need to correct it, we need to all continue with oversight, and to continue with our eye on making sure that these elections are as safe as they possibly can be, and I want to thank all of you for your research, your time, for being here today, and for your continued commitment for safe and reliable voting machines and election system in the United States. And all the advocates.

Mr. CLAY. Thank you so much, Representative, and at this time we will excuse the panel, gavel the committee to a close, and hold an impromptu press conference with Representative Maloney and myself for members of the press.

Without objection, the hearing is adjourned.

[Whereupon, at 11:30 a.m., the subcommittee was adjourned.]

[Additional information submitted for the hearing record follows:]

VotersUnite!

Submitted for the record 05/07/07
Field Hearing - New York
Statement Filing

John Gideon
Ellen Theisen
Co-Directors
www.VotersUnite.org

Statement to the Subcommittee on Information Policy, Census and National Archives of the House Committee on Oversight and Government Reform, House of Representatives
by Ellen Theisen. May 11, 2007

The Voting System Certification Process is Based on a False Assumption

The Subcommittee heard compelling testimony in its field hearing in New York City on Monday, May 7, 2007. All panel experts agreed that the federal testing and certification process for voting systems is broken and that severely flawed equipment is in use throughout the country.

The question remains: can this situation be corrected before the 2008 election?

The situation can be corrected, but the certification process, as currently conceived, cannot be repaired. It is based on the invalid assumption that with sufficient testing, a computerized system can be trusted to manage mission-critical tasks without human oversight.

Computers Cannot Be Trustworthy Managers

A computer's sole purpose is to ASSIST humans. To ask any certification process to change the inherent nature of a computer from an assistant to a trustworthy manager is to ask the impossible.

Computers assist doctors in diagnosing, but computers are not diagnosticians. Computers assist pilots in navigating, but computers are not navigators. Computers assist accountants, but computers are not accountants.

Computers could ASSIST voters to cast their votes, election workers to tabulate votes, and election directors to aggregate the results. However, as currently used in elections, computers themselves cast votes, tabulate votes, and aggregate results.

When voters indicate their selections on a Direct Record Electronic (DRE) touch screen voting machine and then press the "Vote" button, they are not casting their ballot (contrary to common belief). The computer itself actually casts the ballot by converting the verifiable information on the screen into unverifiable electrical charges inside the computer. These electrical charges are the official ballot, but they may not match the selections that the voter verified on the screen.

Since no voter can verify the electrical charges that represent the final ballot, systems that provide these "electronic ballots" prevent voters from verifying the ballot before it is cast and counted. This violates Section 301(a)(1)(A)(i) of HAVA, which states that every voting system must *"permit the voter to verify (in a private and independent manner) the votes selected by the voter on the ballot before the ballot is cast and counted."*

When election officials press a button on a DRE, scanner, or tabulator to accumulate and print vote totals, the officials are not tabulating the votes. The computer is tabulating and reporting results. Without an independent, non-computerized, verified record of the voter's intent, election officials have no way to verify that the processes inside the computer have calculated the results correctly. This is the reason why citizens want a voter-verified paper ballot AND audits of election equipment.

Many election officials have made clear, however, that they do not believe they should be required to conduct audits to confirm the correct operation of computers used in elections. But, unless computers are used responsibly, it is better to eliminate them from use in voting.

Congress Can Address the Problem

Computers are not inherently accurate; they are obedient. In other professional fields, procedures are in place to provide human verification of the computer's accuracy.

Congress can ensure that when computers are used in elections, they are used **only to assist** in performing election-related tasks rather than given the responsibility of controlling these tasks. Specifically:

1. **Congress can prohibit the use of "electronic ballots," which are unverifiable.**

   Congress must reinforce Section 301(a)(1)(A)(i) of HAVA, which states that every voting system must *"permit the voter to verify (in a private and independent manner) the votes selected by the voter on the ballot before the ballot is cast and counted."*

   Voters cannot verify "electronic ballots" before they are cast and counted. Voting systems that produce such ballots violate HAVA and they violate fundamental democratic principles.

   Where DRE-type devices are used to assist voters with special needs, those devices must allow for human verification of the ballot that is cast and counted. They must produce a paper ballot the voter **can** verify, and that paper ballot must be used in all counts – the initial tally, all recounts, and all audits.

   Time is not a barrier to eliminating electronic ballots.

   New Mexico converted from electronic ballots to paper ballots a matter of months. Moving to a simpler technology is quicker to implement than moving to a more complex one. Operation is simpler, so training is simpler and quicker as well.

   Cost is not a barrier to eliminating electronic ballots.

   Paper ballot systems cost less to acquire and use than electronic ballot systems. Every jurisdiction that switches from electronic to paper ballots will save money – initially and in the long term.

2. **Congress can restructure the voting system certification process to ensure that humans verify all vote-tabulation and vote-aggregation tasks performed by computerized election equipment.**

   No certification process can ensure that election equipment reads, records, tabulates, and aggregates votes correctly. Realistic certification would include a requirement for specific oversight procedures — pre-election testing, post-election testing, and auditing — to be conducted by election officials in each election in which the equipment is used. Congress can mandate that federal elections cannot be certified unless those procedures are conducted.

Conclusion

The voting system certification process, as created by the National Association of State Election Directors and handed over to the Election Assistance Commission by Congress, is fundamentally flawed. It falsely assumes that computerized equipment does not require constant verification by humans.

The certification process, as currently conceived, cannot be repaired. However, it can be restructured to ensure that all tasks performed by computerized election equipment are both verifiable and verified by humans.

Trusting computers to cast, count, and accumulate votes is **not** a way of bringing elections into the twenty-first century. **Trusting computers to manage elections is entrusting democracy to a tool that is only capable of assisting.**

Congress can stop the problems caused by the irresponsible use of computerized election equipment. Congress can and should require clearly-defined, meaningful, citizen-observed independent audits of computers that assist in elections. Or, Congress should ban the use of computerized election equipment.

Ellen Theisen
Co-Director and Managing Editor
VotersUnite.Org
660 Jefferson Ave.
Port Ludlow, WA 98365
360-437-9922

Hon. Doretta L. Davidson
Submitted for the record
05/07/07
Field Hearing
New York

EAC's Testing and Certification Program for Voting Systems

Updated 01/19/07

Prior to the passage of the Help America Vote Act of 2002 (HAVA), voting systems were assessed and qualified by the National Association of State Election Directors (NASED), a nonpartisan association consisting of state level election directors nationwide. These voting systems were tested against the 1990 and 2002 voting system standards developed by the Federal Election Commission (FEC). With HAVA's enactment, the responsibility for developing voting system standards was transferred from the FEC to the U.S. Election Assistance Commission (EAC) and they are now called Voluntary Voting System Guidelines.

In 2005, EAC adopted the first set of voluntary voting system guidelines, as mandated under HAVA. HAVA also requires that EAC provide certification, decertification, and recertification of voting systems and the accreditation of testing laboratories, marking the first time the federal government will be responsible for these activities. Under HAVA, the National Institute of Standards and Technology (NIST) will assist the EAC with the certification program through its National Voluntary Laboratory Accreditation Program (NVLAP), and will provide recommendations to the EAC regarding laboratory accreditation. EAC will make the final decision to accredit laboratories based upon the information provided by NVLAP. Participation by states in EAC's certification program is voluntary; however, most states currently require national certification for the voting systems used in their jurisdictions.

EAC's Voting System Testing and Certification Program

In July 2006, EAC adopted a two phase implementation of its Voting System Testing and Certification Program. The two phases consist of (1) the pre-election or interim phase, and (2) the full testing and certification program. The interim phase began in July, and covers only modifications to voting systems. On December 7, 2006, EAC Commissioners voted to approve adoption of the full program with implementation beginning in January 2007.

The purpose of EAC's national voting system certification program is to independently verify that voting systems comply with the functional capabilities, accessibility, and security requirements necessary to ensure the integrity and reliability of voting system operation, as established in the Voluntary Voting System Guidelines.

Frequently Asked Questions

Q: How long has the federal government tested voting equipment?
A: The Help America Vote Act of 2002 (HAVA) ushered in federal assistance for the certification of voting equipment for the first time, tasking EAC and the National Institute of Standards and Technology (NIST) to partner in implementing and administering the program.

Q: Who had the authority to certify voting equipment in the past?
A: In the past, voting systems have been reviewed and certified by the National Association of State Election Directors (NASED). NASED performed this service on a volunteer basis and received no federal funding. Most of the voting systems in use today were qualified by NASED.

Q: How will the certification process work?
A: Under HAVA, NIST and the EAC are jointly responsible for creating the voluntary voting system guidelines. These guidelines include a set of specifications and requirements against which voting systems can be tested to determine if the systems provide all of the basic functionality, accessibility and security capabilities required of these systems. In addition, the guidelines establish evaluation criteria for the national certification of voting systems. NIST assists the EAC with the certification program through its National Voluntary Laboratory Accreditation Program (NVLAP), which will provide recommendations to the EAC regarding laboratory accreditation. After EAC receives the recommendations from NVLAP, EAC will conduct further review of the recommended labs to address non-technical issues such as conflict of interest policies, organizational structure, and recordkeeping protocols. After the EAC review, the Commission will vote regarding full accreditation. (NOTE: This answer has been updated to reflect the HAVA mandate that the Commission make the final determination regarding accreditation. An earlier version of this response incorrectly stated that the EAC executive director would make this decision.)

Q: Why will manufacturers be allowed to pay test labs directly?
A: EAC does not have the legal authority to collect money from voting system manufacturers to pay for the testing of voting systems. (see 31 U.S.C. §3302(b), *Miscellaneous Receipts Act*). However, if Congress grants the EAC statutory authority to collect and use such funds, the Commission would establish a procedure to directly assign voting systems to a lab and pay the corresponding costs for the testing procedures.

Q: Why will manufacturers be allowed to choose which test lab to use?
A: Regardless of which lab conducts the work, all labs will be held accountable under the accreditation requirements and international lab standards. If a lab violates either EAC policy or the international standards, it could risk losing its accreditation by both EAC and NVLAP. The concept of manufacturers contracting with independent test labs is consistent with numerous other federal government and private sector testing programs. However, if Congress grants EAC statutory authority and funding to pay the test labs

directly, it will establish procedures to also assign which labs will test the various systems that are submitted for testing by the manufacturers.

Q: Will the source code be available to the public?
A: EAC will make all information available to the public consistent with federal law. EAC is prohibited under the Trade Secrets Act (18 U.S.C. §1905) from making the source code information available to the public. However, the test labs will examine the source code to ensure compliance with the voluntary voting system guidelines.

Q: What does EAC's interim accreditation program cover?
A: EAC's interim program issued temporary accreditation to test labs to check modifications to voting systems currently in use. In order to participate in the program, labs applying for interim certification had to attest to a set of EAC required laboratory conditions and practices. EAC requirements for these labs included certifying the integrity of personnel; no conflicts of interest, which covers not only personnel but also their immediate family; as well as the financial stability of the laboratory. EAC hired a NVLAP-trained assessor to verify that these labs successfully met the 17025 standards set by the International Standards Organization. Interim accreditation was necessary to ensure there was no interruption in this process leading up to the November 2006 elections, as NVLAP is currently processing laboratory applications under the HAVA-required program. EAC received the first set of lab recommendations from NIST on January 18, 2007.

Q: Will EAC track problems that occur in the field?
A: Absolutely. EAC's certification program establishes accountability through its Quality Monitoring Program which ensures, through various check points, that the voting systems used in the field are in fact the same systems EAC has certified. For instance, under the program, EAC has the ability to conduct site visits to production facilities to determine whether systems produced are consistent with those that have received EAC certification. EAC will collect reports from election officials regarding voting system anomalies. After reviewing the reports, EAC will share credible information with election officials. In addition, upon invitation or with permission from election officials, EAC will conduct reviews of systems that are in use in the field.

Q: Did EAC track problems that occurred during the November 2006 election?
A: EAC worked with elections officials throughout the country to track potential issues and concerns. As we move forward with implementation of the full program, we will continue to work with election officials to share information and provide assistance.

Q: Why didn't EAC vote to adopt the full certification program prior to the November 2006 election?
A: EAC began its first year of operation in 2004. The first priority under HAVA was the distribution of $3 billion in federal payments to the states to help improve the administration of federal elections. The second priority was adoption of voluntary voting system guidelines. EAC issued the payments to states in 2004 and 2005, and adopted the

guidelines in 2005. EAC began a year-long process to develop the certification program immediately following adoption of the guidelines.

Q: Will EAC make test reports available to the public?
A: EAC will make test reports and all related information available to the public consistent with federal law.

Q: Under the EAC certification program, will there be any repercussions for a manufacturer that misrepresents its product or refuses to address valid system failures?
A: For the first time, manufacturers will be held accountable through EAC's Quality Monitoring Program and its decertification process, which would be the ultimate sanction against a manufacturer. If a system is decertified, the manufacturer may not represent the system as being certified, may not label the system as certified, and the system will be removed from the EAC's list of certified voting systems. Election officials will be notified about the decertification.

Q: Do states have to use voting systems that have been certified by the EAC?
A: According to HAVA, participation in EAC's certification program is voluntary. However, approximately 40 states have required that voting systems used in their jurisdictions to have a national certification.

Submitted for the Record

Hearing in New York City, May 7, 2007

United States House of Representatives
Committee on Oversight and Government Reform,
Subcommittee on Information Policy, Census, and National Archives

Statement of
Teresa Hommel
www.wheresthepaper.org
212 228-3803
10 St. Marks Place, New York, NY 10003
Chair, Task Force on Election Integrity, Community Church of New York

Limitations of Certification Testing, "Transparency," and Current Standards and What Congress Can Do

Standards and testing, the subject of this hearing, are only one part of what would be needed to make computerized elections capable of supporting election legitimacy and legitimate democratic government.

Standards and testing must be understood in a realistic, overarching context. Without that understanding, Congress cannot mandate proper use of computers in elections or exercise proper oversight of the small part that standards and testing represent.

For example, the Help America Vote Act of 2002 and the currently proposed HR811, the "Voter Confidence and Increased Accessibility Act of 2007," both focus on details, and fail to put those details into an overarching structure of proper management of computer use.[1]

In my comments below, I refer to all computerized voting systems as "computers" for simplicity, and specify Direct Recording Electronic voting machines ("DREs") when referring only to them.

A. Limitations of certification testing

Standards and testing are useful to minimize malfunctions, but they cannot guarantee that a computer will work on election day.

1. Are the computers used on election day the same as the ones tested for certification? Election administrators do not know how to verify this. They do not know what equipment they have, how to verify that their equipment is indeed what they think they have purchased, nor how to verify that it has not been tampered with by maintenance personnel or other insiders with access to the equipment. Election administrators are not demanding to verify their equipment, and no law requires them to verify it. The law has actually allowed vendors to prevent verification of equipment by claiming that the products are "trade secret".

2. Computers are volatile, unlike, for example, mechanical lever machines which are stable. After a lever machine is programmed, it won't change itself, no one can change it via remote communications, and no one can change its functionality by taking two seconds to insert a different memory card. The law allows computers to be treated like mechanical devices by not requiring pre- and post-election publicly observable verification of equipment.

3. Physical security is impossible during elections since the computers used for voting are used by the public and managed by non-computer-literate poll workers. A dishonest person would have unlimited opportunities to tamper. He or she could simply go into a poll site, claim to be a technician from the Board of Elections with the job of "checking the computer" and tamper. A good comparison is ATM machines, which most people use and trust. Yet banks routinely lose millions of dollars annually through thefts through their ATMs, and this money is written off as "a cost of doing business." A Google search for "ATM Theft" yields over a million entries.

4. There is widespread belief in the field of elections that standards and testing can ensure correct and accurate computer function on election day. This belief is false. A test can show that a computer is capable of working today under tested conditions, but no test can guarantee that the computer will work tomorrow under the same or different conditions. In the professional world, no installation tests their equipment once and then assumes that all future processing will be correct. Instead, they verify continuously. I speak as a computer professional for 40 years (since 1967). For the last 24 years I have been a short-term contractor and have worked for hundreds of major companies and governmental agencies. It is my personal observation that every professional installation verifies every transaction, and has a staff that monitors the equipment twenty-four hours a day, seven days a week. In contrast, the law does not require election administrators to verify that their computers have worked properly. The problem is that election administrators have been assured by vendors that "the equipment is certified, therefore we can trust that it works properly." Our law fails to require realistic verification.

5. The idea that you can trust a computer because that model has been certified rests on false assumptions, such as:

> If a computer works today, it will work tomorrow.
> If a computer works today, it will work the same way tomorrow.
> If one computer works, another computer of the same make and model will also work.
> If you buy a large number of computers, they will all work the same and none of them will be lemons.

6. Computer security is impossible to control, and assumptions that computers used for voting will be secure is out of line. In spite of the continuous, routine verification of results in professional installations, as well as expensive security monitoring, the FBI Computer Crime Survey of 2005 reported that in that one year 87% of organizations had "security incidents", 64% lost money (showing that the incident was not trivial), and 44% had intrusions from within their own organization (showing that insider tampering is common, and that outside hacking over the internet is only one small part of the security picture).[2] Within this context, the idea that standards and certification testing can guarantee computer security is bizarrely inaccurate, yet widely held by election administrators.

B. Limitations of the term "transparency"

"Transparency" is an inadequate word because different people have different ideas of what it means. I urge everyone to use the term "understandable and observable" when speaking about elections.

Election legitimacy requires that ordinary non-technical citizens be able to appropriately observe the handling of votes and ballots, understand what they observe, and attest that procedures were proper and honest.

- Voters must be able to observe the recording and casting of their own votes.
- Observers must be able to observe the handling, storage, and counting of votes.

DREs produce and count electronic votes and ballots. When DREs are used, the votes that are counted for election tallies consist of invisible electrical charges inside computer circuits. This means that no voters or observers can understand or observe the votes and ballots.

Use of electronic votes forces investigation of election irregularities to focus on computers rather than votes and ballots, and to be performed by "experts" rather than average citizens. Use of electronic votes has also enabled the trade secret claims of vendors to prevent appropriate investigation.

DREs provide one or two placebos for voters to "verify" -- the computer screen and in some jurisdictions a voter-verifiable paper audit trail ("VVPAT"). Yet neither the screen nor the VVPAT is used to create initial tallies, and the law does not require meaningful verification of computer results to occur before initial tallies are announced. The tiny spot-checks that may be mandated under the name of "recount" or "audit" will allow unverified computer tallies of electronic votes to be used in the vast majority of cases.

The history of American election fraud provides many examples of dishonest people who marked and cast paper ballots "for" real or non-existent voters. DREs continue the tradition of this type of fraud but automate it and prevent subsequent opening of the ballot box to examine evidence. DREs force voters to turn over their ballots to be marked and cast by others.

C. Limitations of current standards

Even if a system is certified to the 2005 standards, this is not an indication of good quality because the standards are themselves seriously flawed. [3]

1. The standards do not require computerized voting systems to provide a means for independent verification of vote recording, casting, or counting. In other words, systems that have been designed to be impossible to independently verify are legal under these standards.

2. The standards give the EAC blanket authority to violate any of the standards and approve any system whether or not it passes tests. From Vol. II, Appendix B5:

> "Of note, any uncorrected deficiency that does not involve the loss or corruption of voting data shall not necessarily be cause for rejection. Deficiencies of this type may include failure to fully achieve the levels of performance specified in Volume I or failure to fully implement formal programs for quality assurance and configuration management described in Volume I, Sections 8 and 9. The nature of the deficiency is described in detail sufficient to support the recommendation either to accept or to reject the system. The recommendation is based on consideration of the probable effect the deficiency will have on safe and efficient system operation during all phases of election use."

The problem here is that no one can know in advance if a deficiency will "involve the loss or corruption of voting data."

3. The standards require a minimum Mean Time Between Failure of 163 hours. This allows a 9% failure rate in an election day of 15-hours. Vol I, 4.3.3 Reliability:

> The reliability of voting system devices shall be measured as Mean Time Between Failure (MTBF) for the system submitted for testing. MTBF is defined as the value of the ratio of operating time to the number of failures which have occurred in the specified time interval. A typical system operations scenario consists of approximately 45 hours of equipment operation, consisting of 30 hours of equipment set-up and readiness testing and 15 hours of elections operations. For the purpose of demonstrating compliance with this requirement, a failure is defined as any event which results in either the:
> • Loss of one or more functions
> • Degradation of performance such that the device is unable to perform its intended function for longer than 10 seconds
>
> The MTBF demonstrated during certification testing shall be at least 163 hours.

For purposes of comparison, an ordinary incandescent light bulb has a MTBF of 1000 hours, a DVD player has a MTBF of 40,000 hours (4.5 years), and a computer hard drive has a MTBF of 1,000,000 hours (114 years). Some computer scientists have speculated that more failures of voting systems are due to software than hardware; in fact both types of failures have occurred.

The Election Assistance Commission has not addressed this deficiency in the standards, although public comments called it to their attention in 2005. Once the standards are improved, it will take years for equipment in the field to be improved also.

The testing process in Vol II, Appendix C.4 "Time-based Failure Testing Criteria" allows even higher rates of failure: 6 failures after 466 hours, which is a MTBF of only 78 hours.

D. What Congress Can Do

1. Define terms.

The Help America Vote Act of 2002 ("HAVA") requires voting systems to "produce a permanent paper record with a manual audit capacity" yet the term was not defined, and

currently many jurisdictions use paperless DREs that cannot be meaningfully audited. New legislation should not be necessary to require VVPAT and independent auditability.

The same failure to define terms appears in HR811, the "Voter Confidence and Increased Accessibility Act of 2007." This bill requires recounts and audits but does not define the terms. This paves the way for meaningless and useless procedures, such as reprinting DRE or optical scanner tally reports, which will be called recounts or audits.

2. Require the opportunity for meaningful citizen observation, and prohibit use of equipment that prevents it.

Elections conducted in secret cannot support legitimate democratic government. Citizens must be able to observe and understand what they are observing.

If computers are used, citizens including voters, election observers and candidates, must be guaranteed proper access to closely and meaningfully observe. In a jurisdiction's central tabulating location, this would require the use of several cameras focused on the screen, keyboard, and mouse of central tabulators, while the continuous images are displayed on large-screen TVs where citizens can observe.

Meaningful observation requires observers to understand what they are observing. Use of computers in elections means that observers would have to become computer experts, and be trained by their Board of Elections to understand all the procedures to be used. Even if voters, observers, and candidates designate hired experts to observe for them, these experts would need to be trained in the use of the equipment. It is likely that computers place an insurmountable barrier between observers and the handling of votes and ballots.

3. Require jurisdictions to provide backup emergency paper ballots.

Immediate resolution of computer problems is rarely possible on election day. For this reason emergency paper ballots must be on hand.

4. Require elections to be held again if voters are disenfranchised due to computer failure.
5. Mandate that voters have standing to sue when they are disenfranchised due to computer failures, and mandate remedies.
6. Mandate that candidates have standing to sue if their elections involved computer failures.

Allowing computer failure to disenfranchise voters will guarantee that computer failure occurs early and often.

If voters can't vote because computers failed and the jurisdiction does not provide backup emergency paper ballots, elections must be held again.

After computer malfunctions cause the outcome of elections to be called into question, we have learned from experience that the controversies either cannot be resolved, or cannot be resolved soon enough, to ensure that the election reflects the will of the voters. The concept of a "large

margin of victory" is meaningless in computerized elections (since any margin of victory can be achieved by tampering) so remedies should not be tied to margin of victory.

Similarly, if computers handle voter registration lists at poll sites on election day ("electronic poll books"), the computer's failure to find names of registered voters must be discouraged by providing penalties for the jurisdiction, and mandating standing and remedies for voters and candidates.

7. Prohibit secret certification testing.

Secrecy of certification testing does not serve the public, whether or not vendors claim that "disclosure would compromise security features." Computer scientists have repeatedly said that security cannot rely on people not knowing how a computer works (called "security by obscurity").

8. Prohibit use of equipment that is subject to "trade secret" vendor claims.

Use of computers that are subject to trade secret claims has prevented investigation of election irregularities. The law must prohibit vendor claims of trade secrets or prohibit the use of equipment that contain trade secret parts. This must apply to voting and vote-tabulating computers as well as electronic pollbooks and central voter registration systems.

E. Microvote, New York State and Ciber

The problem of inadequate federal and state testing has been an open secret, the details of which have been concealed by the secrecy of the process as well as the ignorance and complacency of state and local election officials. New York is the first state to have properly and independently overseen the work of our former state testing lab, Ciber.

Over 3 years ago, an inteview with the executives of Microvote, a voting machine vendor in the midwest, revealed the basic flaws with our federal and state testing and certification problems.[4]

> **Bill Carson:** Unfortunately the ITA (independent testing authority) has a limited scope in what they can test and check on the system. It is based on time and economics. For an independent test authority to absolutely, thoroughly test under all possible conditions that the device will operate properly they would have to spend, in my estimation, 10 times the amount of time and money as it took to develop it in the first place.... And the technology changes so rapidly, by the time they get done testing it, it's obsolete.
>
> **I-Team:** So what do ITAs not test?
>
> **Carson:** (Picks up electrical cord.) UL says that this will not shock you and it will not catch fire. They don't tell you that it actually works. That's beyond the scope of UL testing. Absolutely nothing will you see in the FEC requirements that this (puts hand on DRE voting machine) has to work. It has to have these functions. But it doesn't have to work.

I-Team: What about state certification testing?

Ries Jr.: We've been somewhat loosely monitored by the states. There's a lot of trust that the vendors are out for the best interest of the local jurisdictions. The states basically look at the federal qualification testing as being kind of the ultimate testing ground. As a vendor working with these independent testing authorities, they do a good job of following the test plans afforded to them by the vendors. They don't really go outside of those test plans. In the state of Indiana - and I'm not criticizing by any means - we just don't have the technical expertise to take these test result plans that the independent testing authorities provide them and really go through them in detail. Maybe it's just the leap of faith that the states feel that the federal testing authorities have done an adequate job and that they will adopt that product pursuant to state compliance.

I-Team: What about evaluation of equipment at the local level prior to a purchase? Do those buying or approving the purchase even know what questions to ask?

Ries Jr.: Local council, local commissioners typically don't get involved in the evaluation of equipment. And that's not a bad thing.

I-Team: Local jurisdictions conduct public tests of new voting equipment, but few members of the public actually attend. Why do you think that is?

Ries Jr.: I guess it's just a leap of faith and understanding that what we're doing is what we're presenting to the county. So there is a bit of uncertainty there. There has to be faith in their local election boards. It's one of those areas of a leap of faith. That you really do have to have a faith in your local jurisdiction, that they are conducting equitable elections in the best faith of the voters. The larger the jurisdiction, the more scrutiny should exist.

Failure to thoroughly test computers used in elections is unwise given industry statistics. 72% of software projects in a typical year, 2000, were complete or partial failures, including 23% that were completely abandoned after huge expenditures (and waste) of time and money. Regarding partial failures, if a computer system "partially" doesn't work, that means it doesn't work.[5]

F. Conclusion

Computerized election errors and fraud cannot be prevented, detected, or corrected by standards and testing. However, the use of computers in elections has shifted the focus of discourse away from votes, voters, ballots, observers, poll workers, and candidates. When computers are used, the conversation is solely about computers. No one has more than circumstantial evidence of what might have happened to the votes and ballots.

In order to evaluate election integrity, then, everyone is forced to rely on computer experts. Statisticians are called in to determine confidence levels. The focus shifts from "open the ballot box, let me see the ballots" to "let my expert examine the computer."

Elections may be acceptable without verification if the procedures for handling votes and ballots are properly observed and understood, but when computers are used, computers always need to

be verified--that is the nature of the technology. The idea that computers need to be only "verifiable" is wrong. Computers need to be verified. Due to the difficulty of making computers work in the first place, and also of maintaining computer security, verification is the correct practice.

Many citizens and election integrity activists oppose computerization of elections for two reasons:

First, the computers are being used without proper verification.

Second, the need for meaningful observation to support election legitimacy may be unable to be met, due to the difficulty of making all election observers sufficiently computer literate and making all Boards of Elections provide large-screen TVs to enable observers to watch the use of central tabulators on election night.

I hope that the members of the Committee on Oversight and Government Reform, Subcommittee on Information Policy, Census, and National Archives, can carry these ideas forward, share them with other members of Congress, and improve any federal legislation that is to be voted on by Congress.

The United States has spent a large amount of money on unverifiable and shoddy computerized voting systems. It is better to take a financial loss, however, than to lose our democracy due to the use of expensive and wrongly designed, wrongly used voting equipment.

---

1. HR811 with embedded comments:
http://www.wheresthepaper.org/HR811withCmt070225.htm
2. FBI report. Re the 87% with security incidents, it has been said, only half jokingly, that the other 13% hasn't noticed it yet. The FBI's report itself mysteriously "was lost" for several months from the FBI web site, and I got a copy on paper from their Houston office.
http://houston.fbi.gov/pressrel/2006/ho011906.htm
http://www.wheresthepaper.org/YahooNews060120FBI_MostCompaniesGetHacked.htm
Financial institutions with the most sophisticated computer security in the world have had massive losses: USA Today. 40 Million credit card holders may be at risk
http://www.usatoday.com/money/perfi/general/2005-06-19-breach-usat_x.htm?csp=34
3. This section was drawn from the work of Howard Stanislevic:
http://www.wheresthepaper.org/StanislevicAreStandardsSolvingTheProblems.pdf
http://www.wheresthepaper.org/StanislevicCertificationWhosMindingTheStore.pdf
http://www.wheresthepaper.org/StanislevicCiberFailures.pdf
http://www.wheresthepaper.org/StanislevicDRE_ReliabilityMTBF.pdf
http://www.wheresthepaper.org/StanislevicGapingHole.pdf
4. An I-Team 8 Investigation, Excerpts from Interviews with MicroVote Executives. Posted February, 2004. http://www.wishtv.com/Global/story.asp?S=1647598&nav=0Ra7JXq2
or http://www.wheresthepaper.org/iTeam01_20MicroVoteInterview.htm
5. Why the Current Touch Screen Voting Fiasco Was Pretty Much Inevitable" by Robert X. Cringely, December 4, 2003. . http://www.pbs.org/cringely/pulpit/pulpit20031204.html

THE COUNCIL OF
THE CITY OF NEW YORK
OFFICE OF THE SPEAKER
CITY HALL
NEW YORK, N.Y. 10007

GARY ALTMAN
LEGISLATIVE COUNSEL

TELEPHONE
212-788-7210

April 27, 2007

Hon. Carolyn B. Maloney
U.S. House of Representatives
1651 Third Avenue, Suite 311
New York, New York 10128

Dear ~~Congresswoman Maloney~~ Carolyn:

This will acknowledge receipt of your recent request for the use of the **Council Chambers, City Hall, on Monday, May 7, 2007** for the Congressional hearing by the Subcommittee on Information Policy, Census and National Archives of the Committee on Oversight and Government Reform.

Permission is granted for the use of the Council Chambers **starting at 9:00 a.m.** and **ending at app. 1:00 p.m.**

Arrangements for the use of any equipment (sound, staging, tables, chairs, etc.) need to be requested, by fax, to Marty Preston at DCAS (212-313-3101). Any questions on security should be addressed to Insp. Dunne at 788-6688.

Cordially,

Gary

Gary Altman
Legislative Counsel

GA/jl
C: Joe Soldevere
Insp. Dunne
E. Cabrera
M. Preston