

# Testing Democracy: How Independent Testing of E-Voting Systems Safeguards Electoral Integrity

Mark D. Phillips  
President, SLI Global Solutions  
216 16<sup>th</sup> Street  
Denver, Colorado 80202 USA  
mphilips@sliglobalsolutions.com

Richard W. Soudriette  
President, Center for Diplomacy and Democracy  
3430 Clubhouse Court  
Colorado Springs, Colorado 80906 USA  
soudriette@aol.com

**Abstract:** When properly implemented, electronic election systems provide accurate vote counting, timely transmission of results, and secure electoral processes. Independent testing and certification by qualified testing laboratories offer election administrators, election stakeholders, and the public assurance that e-voting systems are trustworthy. Testing is an essential tool to safeguard the integrity of e-voting systems.

## 1 Introduction

In 1892, the lever voting machine was used for the first time in Lockport, New York. The inventor, Jacob H. Myers said that his invention would

*“protect mechanically the voter from rascaldom, and make the process of casting the ballot perfectly plain, simple and secret.”<sup>1</sup>*

While most electoral democracies still rely on traditional paper ballots and ballot boxes for their elections, over the past 20 years many countries have turned to e-voting technologies. E-voting systems have been implemented with a range of technologies including direct recording devices, optical scanning systems, and a variety of Internet-based systems, all of which capture, transmit, consolidate, count, and report election

---

<sup>1</sup> This notation was cited in Dr. Douglas W. Jones’s book titled, “A Brief Illustrated History of Voting,” (University of Iowa 2001), Chapter 6.

results. When implemented properly, e-voting can protect the rights of voters and safeguard electoral integrity.

Independent testing and certification of e-voting systems are essential tools that election management bodies (EMBs) should use to guarantee the performance of e-voting systems and to promote public confidence. Transparency in both testing and certifying e-voting systems also promotes credibility among election stakeholders such as political parties, the media, and civil society. This paper will discuss the following aspects of testing and certification:

- Technology challenges faced by election administrators
- Need for international election testing standards
- Review of current e-voting hardware/software testing methodologies
- Case studies in election testing and certification
- Impact of independent testing and certification on electoral integrity

If e-voting systems are in use, it is imperative conduct both internal and independent testing to ensure that e-voting systems are functioning correctly and accurately. The infamous “punch card voting machines” and “hanging chads” of Florida from the cliffhanger U.S. presidential election in 2000 demonstrated that the lack of adequate testing and maintenance of voting equipment undermines voters’ faith in the democratic process.

Election administrators who are considering implementing an e-voting or Internet voting solution should include adequate funding for the independent testing and certification of such voting systems. In 2010, the Commission on Elections (COMELEC) in the Philippines held fully-automated, nationwide elections. Overall, the election was viewed as a success in the eyes of the voters, who were pleased to know the winner of the presidential elections 48 hours after the closing of the polls. A key to the successful use of voting equipment was a robust independent testing and certification program.

## **2 Technology Challenges Faced by Election Administrators**

Despite the potential advantages of e-voting systems, many election officials are reluctant to embrace automation at the polls. This hesitance is fueled by increased opposition to new voting technologies. In countries where e-voting is in use or being considered, election administrators face resistance by opponents of e-voting technology in all its form. Many election technology foes strongly believe that legitimate elections can only be conducted with traditional paper ballots, ballot boxes, and tabulation of election results by hand.

In the U.S., opponents of direct recording electronic (DRE) machines have been successful in convincing officials at all levels of government of the unreliability of DREs and the need to add printing capabilities to existing machines to produce a paper trail of each recorded vote. This insistence on having a Voter Verified Paper Audit Trail (VVPAT) has added major costs to state and local elections.

Since the passage of the Help America Vote Act in 2002, there have been a handful of lawmakers in the U.S. Congress who have introduced legislation that would mandate a return to the use of traditional paper ballots. In 2008, two U.S. Senators introduced legislation that would have completely banned the use of touch screen DRE machines for the U.S. presidential election in 2012. While none of these measures have passed in Congress, they do help to undermine the credibility of e-voting as well as the election process.

In Europe, the anti-technology backlash has virtually halted the use of e-voting systems: The Dutch had been pioneers in the use of voting technology since the late 1960s, until a dramatic shift occurred in 2008 when anti-technology Dutch activists forced the Dutch Government to scrap nationwide use of DRE machines in elections.

Over the past decade, the U.K. has experimented with e-voting technology for pilot elections for local and E.U. parliamentary elections. At the present time, however, it appears that there is little enthusiasm nationwide for embracing new voting technologies. The only bright spot for election technology is in London, where an e-counting system was used for local elections in 2008 and will be used again in 2012.

Belgium is one of the few exceptions in Europe, having decided to use a DRE voting system on a limited basis in municipal elections in 2012.

### **3 Need for International Election Testing Standards**

To reverse the anti-technology trend in elections, EMBs should rely on independent testing and certification of e-voting systems. Presently there are no internationally recognized standards that mandate the conduct of election technology testing and certification. However, there are initiatives that are taking place in several countries.

The Council of Europe established a basic set of standards governing e-voting in 2004. These standards emphasize the need for reliable auditing of voting systems as well as certification. Yet there are no specific protocols or procedures governing independent testing and certification of e-voting systems. In 2010, the Council of Europe released an excellent publication, *The E-Voting Handbook*, which encourages the independent testing and certification of e-voting systems.

In the U.S., extensive testing and certification of voting systems is in place for both e-voting and Internet voting. The U.S. Election Assistance Commission (EAC) oversees the testing of voting systems in cooperation with the National Institute of Standards and

Technology (NIST) and is responsible for accrediting Voting Systems Test Laboratories (VSTL). Generally, when states and municipalities use federal funds to buy voting equipment, the equipment is certified by accredited VSTLs. The EAC mandates that equipment testing be conducted independently and without interference from vendors.

VSTLs test voting systems using a set of criteria developed by the EAC called the Voluntary Voting Systems Guidelines (VVSG). Most states follow the EAC guidelines and protocols. However, several states such as New York, California, and Ohio have either amended these requirements or have developed their own election testing standards and certification programs. The New York State Board of Elections concluded an extensive election testing and certification program in 2009 which helped to replace antiquated voting equipment across the state.

One way to expand the use of e-voting would be for international election experts and institutions to work together to develop a basic set of testing and certification standards. Some of the groups that might take the lead in such an effort include the United Nations Development Program, Association of European Election Officials, E-Voting CC, Carter Center, International Foundation for Electoral Systems, Electoral Institute of Southern Africa, and the OSCE Office for Democratic Initiatives and Human Rights.

#### **4 Review of Current E-voting Hardware/Software Testing Methods**

Testing and certification should be undertaken to verify the accuracy, reliability, and security of e-voting systems. Since 2003, the EAC has awarded more than USD\$2 billion in federal funds to states and municipalities to upgrade their voting systems. Independent testing and certification of voting equipment help demonstrate that taxpayers' money is being well spent on reliable voting systems.

In 2006, the Carter Center reported on the Venezuelan presidential elections and stated:

*“Impartial, independent, and transparent system certification measures should be in place to insure that the system meets national or international standards, the requirements of the election’s jurisdiction, as well as the technological specifications outlined by the vendor.”<sup>2</sup>*

---

<sup>2</sup> See Carter Center’s report on the Venezuelan Elections in 2006 entitled, *Developing a Methodology for Observing Electronic Voting*, page 6.

The major e-voting tests currently used by independent laboratories include:

- Acceptance Testing: Testing the functionality of software used in e-voting systems
- Performance Testing: Testing of performance and speed of hardware and software
- Stress Testing: Testing the endurance of voting systems even under extreme conditions
- Security Testing: Testing for data protection and functionality of e-voting systems
- Usability Testing: Testing for voter-friendly e-voting systems
- Trusted Build: E-voting systems are rebuilt under controlled conditions using the vendor specifications to insure they function properly
- Source Code Review: Systematic testing of source code for e-voting systems.<sup>3</sup>

EMBs that are considering automating voting systems are advised to engage in sufficient analysis and planning prior to moving to the procurement phase. Poor implementation of e-voting systems can result in costly errors both in terms of public finances and public confidence.

The Republic of Ireland learned a tough lesson following the botched implementation of e-voting in 2004. The decision to replace traditional paper ballots with a DRE system ultimately cost Irish taxpayers approximately €55 million and a loss of electoral credibility. This ill-fated e-voting scheme was conceived by government bureaucrats with little public input from the election stakeholders. The DRE system was scrapped before it was ever used and this fiasco resulted in a major setback for e-voting across Europe. Adequate planning, thoughtful procurement, and independent testing would have produced better results.

In Ben Goldsmith's recent book *Electronic Voting & Counting Technologies* he makes the case for having sufficient lead time and preparation when EMBs modernize voting systems. This includes feasibility studies and pilot elections prior to nationwide implementation: "*Once delivered, it is essential that an EMB ensure that an electronic voting or counting system not only meets the specifications developed for the system, but also meets the requirements of the electoral environment.*"<sup>4</sup> The best way to ensure that voting systems perform as intended is to independently test and certify the systems prior to an election.

---

<sup>3</sup> See The Council of Europe Handbook for E-Voting, pages 34-35.

<sup>4</sup> See Ben Goldsmith's, "Electronic Voting & Counting Technologies--A Guide to Conducting Feasibility Studies," page 6.

## 5 Factors to Consider for Successful Testing and Certification

Independent testing must combine absolute objectivity, the highest ethical standards, and proven testing methodology. Also, test laboratories must be able to work closely with EMBs and stakeholders to engender maximum public confidence in the electronic election system.

Objective accreditation is vital for the testing, auditing, and certification of e-voting systems. The International Standards Organization (ISO) recognizes the effectiveness of testing facilities by awarding its coveted designation *ISO: 9001:2008*. Also, ISO uses the internationally recognized test standard known as *ISO-17025* to gauge the capacity of testing labs to fully replicate and audit test results as an indicator of testing competence. In the U.S., the National Voluntary Laboratory Accreditation Program of the National Institute of Standards and Technology as well as the EAC, engage in accrediting election test laboratories. These types of accreditations are useful because they provide EMBs with confidence that the testing methodologies used by test labs are reliable, repeatable, and objectively verifiable.

Voting systems have unique demands. For example, optical scan counting systems must be able to accurately and reliably read the hand written marks of voters as they indicate their candidate preferences on paper ballots. If not properly designed and tested, the variability in handwriting of the voters can impact the performance of scanning systems and may even potentially impact the accuracy of the vote count. Most generalized software testing labs have experience in code and process review but may lack specific methodology and techniques to ensure that electronic election systems operate as required. Test methods must be configured in a way to ensure the effective validation of voting systems that fully comply with the electoral law as well as the requirements of EMBs. Testing labs need to demonstrate that they stand behind their work and that they have extensive automated management, repository, and reporting tools necessary to guarantee that e-voting systems will report election results with transparency and accuracy.

Experience with a broad range of electronic election systems is important to design effective tests and provide accurate as well as timely test results. As voting systems, ballot designs, and election processes vary worldwide, it is crucial to understand how these differences can impact electronic voting. The variety of election management systems poses logistical challenges and may reveal vulnerabilities of e-voting systems. These potential weaknesses will certainly be exploited by anti-technology activists as they seek to derail the use of e-voting, which is why independent testing is so essential. Direct experience with election testing can also help EMBs better understand the importance of properly communicating test results to election stakeholders with divergent points of view such as political parties, civil society, and the media.

## 6 Case Studies in Election Testing and Certification

Since no international testing standards governing independent testing and certification of e-voting systems exist, it is useful to consider how EMBs currently using e-voting systems are dealing with this issue.

E-voting in Brazil began in the late 1980s. By 1996, the Supreme Electoral Tribunal of Brazil introduced e-voting nationwide for federal elections. The Tribunal has long understood the importance of adequate testing of voting machines in use. They have accomplished this through internal testing done by Tribunal's staff and independent testing conducted by the Brazilian National Institute of Space Research. Several scientists from this agency were involved in the original design of the Brazilian DRE machine.

The U.K. has been reluctant to move forward with full implementation of e-voting and e-counting systems. From 2000 to 2007, the U.K. Government supported many pilot elections around the country using a wide variety of voting technologies. Under current U.K. law, e-voting can only be used for local and EU parliamentary elections.<sup>5</sup> Only traditional paper ballots may be used for U.K. parliamentary elections. Intense public pressure by anti-technology activists forced the government and the U.K. Electoral Commission to temporarily suspend support for pilot schemes using e-voting technology. Using local financial resources, the one exception has been the Greater London Authority (GLA), which authorized and funded the use of an e-counting system for the municipal elections in London in 2008 and in 2012. The GLA made independent testing and certification a priority in both elections.

In 2004, the Electoral Commission of India (ECI) took a leading role in the use of e-voting technology. The ECI introduced the Electronic Voting Machine (EVM) which was successfully used in nationwide parliamentary elections in 2004 and 2009. While testing does play a role in the work of the ECI, it is done internally by the Electoral Commission and by the EVM manufacturer. Due to increased concerns by election stakeholders during the 2009 elections, the ECI invited critics to share specific information about perceived or actual vulnerabilities in the EVM system. For the most part, the 2009 parliamentary elections went smoothly. However, the ECI has recently shown interest in independent testing for future elections.

One of the cornerstones of the plan to enhance democratic institutions in the Philippines was the introduction of electronic devices to count votes and transmit election results more quickly and accurately. According to the former Chief Justice of the Supreme Court of the Philippines, Reynato Puno, *"Full automation will not completely cleanse the dirt in our electoral system, but it is a big leap forward which can lead us to the gateway of real democracy where the vote of the people is sacred and supreme."*<sup>6</sup>

---

<sup>5</sup> See August 2007 Bulletin of the Electoral Commission of the U.K. entitled, "Key Issues and Conclusions-Electoral Pilot Schemes."

<sup>6</sup> See interview on GMA TV News broadcast interview on September 11, 2009 with former Chief Justice Reynato Puno of the Philippines.

To accomplish this goal, COMELEC of the Philippines successfully implemented the use of 80,000 precinct count optical scan (PCOS) machines. Planning for implementation of the new automated voting system started in 2008; two years before the election. When COMELEC developed their automation plan they included independent testing and certification as major program components. Because COMELEC was unable to find international voting systems guidelines, the decision was made to adapt portions of the Voluntary Voting Systems Guidelines of the EAC and then combine these specifications with additional Philippine statutory requirements.

COMELEC was especially determined that the 2010 elections be well received by the public, so they made certain that independent testing and certification were key components of their automation efforts. With the help of independent testing, COMELEC was able to resolve design problems and ensure that the vendor delivered the PCOS machines on schedule. The testing and certification also enabled COMELEC to promote confidence in the new system among voters, political parties, civil society, and the media. Election administrators contemplating the use of e-voting should carefully study the case of the Philippines.<sup>7</sup>

The election testing and certification system in the U.S. has evolved over three decades. The U.S. Federal Election Commission (FEC) made initial efforts to establish early standards for e-voting systems in the U.S. Later, the National Association of State Election Directors launched a voluntary testing and certification program for voting systems that has evolved into the current system overseen by EAC and NIST.

The passage of the Help America Vote Act in 2002 created the EAC. One of the mandates of the EAC was to assume oversight of voting systems standards and testing. Congress gave the EAC the authority to disburse nearly USD\$3 billion in federal funds to state and local election officials to replace antiquated voting systems such as the punch card voting machines in states such as Florida, Illinois, and Ohio. EAC funds have been used to purchase voting systems that were certified by the EAC accredited testing laboratories. Currently the terms of all of the EAC commissioners have expired, and it is doubtful that any new commissioners will be named by 2013 at the earliest. Nevertheless, the testing program, protocols, and procedures of the EAC are still in force.

---

<sup>7</sup> See article by Richard W. Soudriette, "Philippines Test E-Voting," *Modern Democracy*, page 3, February 21, 2011.

A major issue faced by election administrators is the security of the source code for e-voting systems. This became the hot button issue in the Philippines prior to the 2010 elections. The review of the source code is a critical element in the testing and certification process. Many opponents of the automated voting system in the Philippines were fearful that the source code could be manipulated to rig the election, or that corrupt elements would penetrate the security of the software for the purpose of corrupting the election results. Because of this concern the COMELEC, using its independent third-party testing lab, conducted an extensive review of the source code for the PCOS machines and provided controlled access to political parties and NGOs to examine the results.

Other electoral management bodies such as the Supreme Electoral Tribunal of Brazil and the New York State Board of Elections have also made source code accessible to parties, civil society and the public. In offering this access it is vital that election officials safeguard the sanctity of e-voting systems by not actually allowing the source code to be downloaded for the purpose of conducting off site testing and review. EMBs must guard against tampering with the code in an uncontrolled environment. Another issue related to source code is that election management bodies may face difficulty getting full access to the code from the equipment vendors due to intellectual property issues. When entering into vendor contracts, election administrators should ensure that the contract language grants EMBs full access to the source code. To protect intellectual property rights, the vendors may require election administrators to sign confidentiality agreements to eliminate the fear that corporate secrets will be tapped by competitors. The use of Internet voting is increasingly seen as an important tool by election administrators. For the elections in 2012 in Mexico City, the election authorities plan to use Internet voting to permit out-of-country voting. In 2011, the Norwegian Ministry of Local Government and Regional Development conducted pilot local elections in 10 municipalities using Internet voting. The OSCE/ODHIR election team that observed these pilot elections noted that, for the most part, the pilot elections were successful. More than 27,000 voters cast their ballots via the Internet. In their report, the OSCE/ODHIR observer team stated that some voters experienced difficulty using the Internet voting system. The same report mentioned a lack of adequate auditing and certification of the internet voting system.<sup>8</sup>

Critics of Internet voting have pointed out that limited pilot projects, such as the one in Norway, do not adequately reflect the threats that could occur in larger elections. Threats including denial of service (DOS), DNS routing manipulations, and the generally uncontrolled environment of the Internet are cited as being more attractive to persons with malicious intent as the stakes and visibility of elections increase. Proponents point out the convenience and improvements in citizen participation promised by properly implemented Internet solutions. Given the open nature of Internet solutions that may permit voting anytime, anywhere, and regardless of device, it is necessary to have trusted third party penetration, testing, vulnerability testing, code review, and security audits of the voting servers to ensure a strong defense for any Internet voting system.

---

<sup>8</sup> OSCE/ODHIR election reports regarding Norway can be found at <http://osce.org/odhir/elections/norway>.

## 7 Impact of Testing and Certification on Electoral Integrity

Election administrators often view e-voting systems as a panacea to resolve all election problems. E-voting is merely a tool, not a replacement for competent and professional election administration.

In the Republic of Georgia in 2004, some politicians viewed the Central Election Commission (CEC) with disdain and suspicion. A bill was introduced to replace the CEC with e-voting. That same year the International Foundation for Electoral System invited the Deputy Speaker of the Georgian Parliament and several of his colleagues to observe elections in the U.S. They visited many American polling stations using a variety of e-voting systems. Their overall observation was that the key to good elections lies not in the voting equipment but in the work of election administrators.

Automation of voting systems can represent a major investment of public funds. The budget for the development and operation of the automated voting system in the Philippines for the 2010 election was about USD\$150 million. While this is a substantial investment, the e-counting system used in the Philippines accurately recorded, consolidated, and reported the votes of over 50 million Filipinos within hours of the close of the polls. The 2010 elections stood in contrast with the previous elections when voters had to wait for days, weeks, and months before election winners and losers were known. Additionally, the e-counting system has the potential of holding down costs if used for future elections.

On the issue of e-voting systems and potential cost savings, the experience of Mexico should be noted. Since 2008, the Electoral Institute for Citizen Participation – *Instituto Electoral de Participación Ciudadana* (IEPC) of the state of Jalisco has systematically developed an e-voting system through phased implementation. IEPC has found that while initial development and deployment costs of e-voting systems are high, the long-term use of e-voting systems is cost effective.<sup>9</sup>

Given the high initial cost of voting equipment, a number of steps should be taken before the green light is given to purchase e-voting equipment. These steps include feasibility studies, pilot elections, open procurement processes, independent testing and certification, and effective outreach to election stakeholders to inform them of every step in the process. Given the considerable opposition to e-voting technology worldwide, it is a duty incumbent upon election administrators to procure e-voting systems that are voter friendly, accurate, and secure. An independent testing and certification program should be an essential part of the selection and procurement process to ensure that the system operates as promised on election day.

---

<sup>9</sup> See the 2011 report of the IEPC of Jalisco entitled “Proyecto Urna Electrónica de Jalisco.”

In countries accustomed to contentious elections, the lack of adequate testing of e-voting systems can undermine democracy. Independent testing in 2010 helped COMELEC diffuse concerns about the potential for manipulation of the Philippine elections. By keeping election stakeholders informed about the testing and certification process, COMELEC was able to maintain public confidence in the new election system.

## 8 Conclusion

Election administrators face a small but vocal group of anti-election technology opponents. While some EMBs may not wish to automate their electoral processes, e-voting holds great potential as a valuable tool in the advancement of democratic rights.

For successful implementation of e-voting, independent testing and certification programs should be required. By embracing testing as an essential tool, election officials can ensure that the e-voting systems they procure have the best possible chance of operating flawlessly on election day. Testing and certification can also reassure citizens, candidates, and election stakeholders about the transparency and accuracy of e-voting.

The best assistance that the international election community can provide to expand the reach of e-voting is to work toward the development of international standards and protocols governing the independent testing and certification of e-voting systems. Enlisting the support of international and regional election organizations in the development of international voluntary voting systems guidelines would also be a major advancement in the field of election administration.

When properly implemented, electronic election systems count quickly and accurately. E-voting systems make the voting process more accessible and speed up the release of accurate election results. There are many examples worldwide where the slow release of election results has increased public anxiety and sparked civil unrest. If voters have confidence in the credibility of e-voting machines, they will trust the results. Independent testing and certification of e-voting systems are vital tools to safeguard the sanctity of the ballot box and the integrity of the democratic election process.

## Glossary of Acronyms

COMELEC	Commission on Elections of the Philippines
DRE	Direct Recording Electronic Machine
EAC	Election Assistance Commission (USA)
ECI	Electoral Commission of India
EMB	Electoral Management Body
EVM	Electronic Voting Machine (India)
FEC	Federal Electoral Commission (USA)
GLA	Greater London Authority
HAVA	Help America Vote Act

IEPC	Electoral Institute for Citizen Participation – <i>Instituto Electoral de Participación Ciudadana</i> of Jalisco, México
ISO	International Standards Organization
NIST	National Institute of Standards and Technology
OSCE/ODHIR	Organization for Security and Cooperation in Europe/ Office of Democratic Institutions and Human Rights
PCOS	Precinct Count Optical Scanner
VSTL	Voting Systems Testing Laboratory
VVPAT	Voter Verified Paper Audit Trail
VVSG	Voluntary Voting Systems Guidelines

## Bibliography

- [Ca06] Carter Center. Developing a Methodology for Observing Electronic Voting. Atlanta 2006.
- [Co10] Council of Europe. Handbook for E-Voting. Brussels 2010.
- [El11] Election Assistance Commission (USA). Voting System Testing and Certification Program Manual. Washington, D.C. 2011.
- [El05] Election Assistance Commission (USA). Voluntary Voting Systems Guidelines-Vol. I & II. Washington, D.C. 2005.
- [El07] Electoral Commission of the U.K. Key Issues and Conclusions—Electoral Pilot Schemes,” EC Bulletin, August 2007.
- [Go11] Goldsmith, Ben. Electronic Voting & Counting Technologies—A Guide to Conducting Feasibility Studies. Washington, D.C.: IFES 2011.
- [Go05] Government and Accountability Office (USA). Elections—Federal Efforts to Improve Security and Reliability of Electronic Voting Systems are Underway but Key Activities Need to Be Completed. Washington, D. C. 2005.
- [Jo01] Jones, Douglas W. A Brief Illustrated History of Voting. Des Moines: University of Iowa 2001.
- [Os11] OSCE/ODHIR. Norway Internet Voting Pilot Project - Local Government Elections on 12 September 2011- Election Expert Team Report. Warsaw 2011.
- [Sa06] Saltman, Roy. Independent Verification: Essential Action to Assure Integrity in the Voting Process .Gaithersburg, MD: National Institute of Standards and Technology 2006.
- [So11] Soudriette, Richard W. “Philippines Test E-Voting,” Modern Democracy, February 21, 2011.
- [Sw09] Swamy, Subramanian. “Are Electronic Voting Machines Tamperproof?” The Hindu. June 17, 2009.
- [Ya10] Yard, Michael. Ed. Direct Democracy: Progress and Pitfalls of Election Technology. Washington, D.C.: IFES 2010.