From Power Outages to Paper Trails:
Experiences in Incorporating Technology into the Election Process

March 2007

GEO Conference Paper

Panel on Electoral Technology

Applied Research Center
For Democracy And Elections

Bridging Theory and Practice

From Power Outages to Paper Trails:

Experiences in Incorporating Technology into the Election Process

White Paper prepared by IFES for the 2007 Global Election Officials (GEO) Conference Panel on Electoral Technology held on March 27, 2007.

The findings and conclusions in this report are those of the author(s) and do not necessarily represent the views of IFES.

© 2007 IFES

Table of Contents

Introduction

What value does a satellite vehicle tracking system bring to your country if large numbers of voters still have to walk for four hours to the nearest polling station?

How much accountability can an EMB have to the public and the election process if a vendor could threaten to pull out and effectively halt an election in Western Europe?

Is more sophisticated technology necessarily better? Can an EMB that does not use email effectively maintain elaborate civil registry databases?

Where is the line between donor priorities and EMB priorities?

IFES experts in countries around the world have run into these kinds of contradictions and difficulties in providing assistance to election officials in making decisions about and implementing election technologies.

IFES has worked in more than 120 countries across the globe in environments that have included the most rudimentary to the most advanced technologies. The level of technology does not parallel the viability of the results or the level of voter confidence despite the promises that new technology and its champions might argue. The only way to reduce this risk is for an EMB accept, adhere to, and implement the numerous steps and considerations outlined in these and other lessons-learned reports.

IFES commissioned these papers to help EMBs navigate issues of modernization and new technology. Though it seems that high technology projects are being undertaken everywhere from the Philippines to Nigeria to Kazakhstan and of course throughout the United States and Europe, the question remains:

Is the technology on the cutting edge of electoral processes being pursued for the sake of being on the cutting edge, or for the sake of the electoral process?

In the papers that follow, experts in the fields of information technology, election assistance, and electronic voting begin with this question, and discuss, from their wide experience and expertise, indicators, considerations, and guidelines that can help EMBs ensure that the answer is always the latter.

Challenges of instituting election technology stem not just from the complexity and political sensitivity of elections, but also from the difficulties of implementing any large scale technology project. According to an oft-cited 2000 study by the Gartner Group, 30 percent of all software projects fail and over half end up costing more than double the original budget.[1] In general, studies related to information technology (IT) projects show an equally gloomy forecast of success. The high risk of failure is not, however, an indication that organizations should avoid technology projects; on the contrary, a single successful automation project may more than compensate for multiple failures. The high risk does, however, serve as a warning against embarking on a new technology project without laying adequate groundwork to maximize the chances of success.

[1] Thomas Eck "Closing the IT-Business Gap," *Microsoft Certified Professional Magazine Online* (May 2000). Available at http://mcpmag.com/features/article.asp?EditorialsID=176.

A March 2007 poll by the Computing Technology Industry Association (CompTIA)[2] notes the top five factors that contribute to the failure of IT projects:

- Poor communications.
- Inadequate resource planning.
- Unrealistic schedule.
- Poor project requirements.
- Lack of stakeholder buy-in/support.

These categories are similar to the themes that each author in this report draws out:

- The importance of understanding the EMB's mission and setting goals
- Inclusive (of stakeholders) and comprehensive (addressing resources, costs, and compatibility in the short and long-term) planning
- Anticipating timeframe accurately
- Maintaining accountability with well-designed requests for proposals (rfps) from vendors
- Starting simply, with appropriate technologies

The report contains the following chapters:

- **Maximizing the Potential for Successful Election Technology Projects**
- **The Introduction of New Technologies from the Election Administrator's Perspective**
- **Perspectives on Electronic Voting**

IFES election IT experts **Michael Yard and Ronan McDermott** draw on their rich experience in provision of IT design and support to developing democracies to present lessons learned and guidelines in the adoption of new technologies or upgrades to existing technologies. Their recommendations to start with basic technologies, such as email, local area networking, and powerful desktop applications should be seriously considered by donors and EMBs alike.

Long-time IFES senior election administration specialist **Linda Edgeworth**, a renowned elections expert with more than a dozen years of experience internationally and many years prior as an administrator in the United States brings her years of experience in working with EMBs on everything from election law, polling place procedures, and strategic election management to bear in discussing, from a true administrator's point of view, the process of adopting new technologies. With an eye toward the political and practical implications for not only election officials, but legislatures, contract negotiations, and public awareness, Edgeworth describes key issues and guidelines for EMBs to keep in mind when considering implementing any new election technologies.

Leading expert in voting technology, **Dr. Douglas Jones**, of the University of Iowa computer science department, explores two questions in his paper: 1) Why pursue voting technologies? and 2) How to manage the acquisition, evaluation and use of voting technologies? Discussing voting technologies, from lever machines to optical scanners to direct recording electronic (DRE) systems, Dr. Jones details the key considerations and possible pitfalls that an EMB must navigate in implementing any kind of voting technology. This chapter brings the issues raised in the first two chapters into concrete relief.

By no means are these papers exhaustive of the significant research done already on these issues, but they do open the door for sincere dialogue amongst EMBs that continue to share their experiences at meetings such as the GEO and through the ACE Electoral Network. It is our hope that these papers spark an even more active dialogue beyond the traditional borders of advanced democracies and can transcend to new democracies who are facing a leap-frog technology

[2] CompTIA "Poor Communications is Most Frequent Cause of Project Failure, CompTIA Web Poll Reveals," Press Release (March 6, 2007). Available at http://www.comptia.org/pressroom/get_pr.aspx?prid=1227.

opportunity that older democracies have had more time to acclimate – albeit not always successfully as we have seen in the United States after 2000.

An overview of the many core issues addressed in the following collection includes, but is not limited to:

- Understanding and appreciating cultural factors, norms and considerations
- Risks involved in shifting to new technologies too soon
- Highlighting the responsibility of vendors, donors and international assistance providers
- The important role of stakeholders, including political parties, civil society organizations, the media, and the voters themselves in determining the success or failure of any new approach
- Awareness that technology lives in a very short life line – beware of "flavors of the moment"
- Transition to new technology, approaches, and implementation takes time and planning
- Test out lower tech and lower risk mediums to prepare yourself for larger more complex initiatives
- Know your strategic and operational goals
- Proper, transparent and legal solicitation for services and equipment are crucial to ensure public confidence
- An as stated earlier too much technology without proper planning and education can actually impede democratic consolidation

We thank the readers of these papers and the attendees of the 2007 GEO Conference for their interest, participation and continued activism in the field of election administration whose primary goal is to offer a fair and transparent playing field for democracies to survive and prosper.

About the Authors

Michael Yard has worked in international development as a consultant and manager of programs supporting democracy and governance programming for many years. His areas of expertise include computerized vote counting and reporting systems, large scale database development of systems for election commissions and truth and justice commissions, design and automation of registration equipment, and database integrity auditing. Mr. Yard has managed two projects for IFES, in Bosnia and Ghana, and has consulted for IFES on projects in numerous countries, including Armenia, Bosnia, South Africa, Nigeria, Kenya, Sri Lanka, Pakistan, Lithuania, Hungary, Guyana, Yemen, Serbia, Macedonia and Tajikistan. He has also worked for numerous other development agencies, including Creative Alternatives International, Democracy International, PADCO, the United Nations and the OSCE.

Ronan McDermott
Ronan McDermott currently works for IFES as Voter Registration Advisor to the elections management body in Pakistan. Mr. McDermott has also worked with the UN and UNDP on various information technology (IT) aspects of elections such as operations manuals, voter registries, systems testing, and vote tabulation intake management. He has been involved in projects in Guyana, Sierra Leone, Liberia, DRC, Nigeria and Haiti. Mr. McDermott and is pursuing an MSc in IT at the University of Liverpool (UK)and plans to focus his thesis on election technology.

Linda Edgeworth has been a consultant specializing in international election law and administration since 1991. In that time she has worked with IFES, the OSCE, and UN, and has served in 27 countries across the Caucasus, Balkans, Central Asia, Central and Eastern Europe, Africa, and South Asia. From 1997-1999 Ms. Edgeworth was the OSCE Director of Elections in Bosnia and Herzegovina where she organized the first post-war voter registration program and conducted the countrywide elections for all levels of government. Most recently, she has consulted with several states and counties in the United States regarding implementation of the Help America Vote Act. Prior to her international work, Ms. Edgeworth was an election administrator for the State of Alaska in the United States. She has been a speaker and facilitator at many election-related conferences domestically and abroad and has been a guest lecturer at Colgate University.

Dr. Douglas Jones
Dr. Jones is an Associate Professor in the Department of Computer Science at the University of Iowa, a Principal Investigator for the National Science Foundation's A Center for Correct, Usable, Reliable, Accurate, and Transparent Elections (ACCURATE), and has served on the Iowa Board of Examiners for Voting Machines and Electronic Voting Systems from 1994 to 2004, including a term as Chair from 1999 to 2003. Dr. Jones has written and published a variety of print and web resources on voting systems and standards. and has given testimony on these issues to the U.S. Congress and various state governments. Most recently, Dr. Jones has also served on OSCE/ODHIR international electoral assessment and observation missions in the Netherlands and Kazakhstan.

Maximizing Potential for Successful Election Technology

Michael Yard and
Ronan McDermott

I. Introduction

The authors' experience in implementing technology for election management has shown at least five prerequisites that must exist in order to make successful use of technology likely:

- A clear definition of the EMB's mission to conduct free and fair elections.
- Clear goals for the technology project.
- Realistic expectations.
- Willingness to re-engineer other procedures to maximize effectiveness of the technology.
- Selection of technology appropriate for the environment in which it will be used.

II. Prerequisites for Successful Technology Project

A. Clear Definition of Mission

The most important prerequisite for implementing technology in a way that will further an organization's objectives is that the planners have *a clear understanding of the mission of the organization*. A few examples will make this clear. In order to create a successful election logistics system, it is not enough for the planners to understand logistics; they must also understand the requirements for good elections. For a commercial application, late delivery of materials might lose a sale; for elections, late delivery of materials can jeopardize the entire election. Designers of a communication system might be satisfied with a system that can handle just over a higher-than-average load, with a result that some users might not be able to complete calls during times of peak demand. This might be an acceptable target for a mobile phone system, but could lead to disaster if applied to communication system for election results.

Even beyond the requirements for individual components of election management, it is possible to create a system that meets all the criteria for successful technology, yet still fails within the context of the mission of the EMB. For example, a vote-counting technology that is 100 percent accurate may not be appropriate for use in elections if it lacks adequate measures to ensure transparency and accountability.

It is only through a clear understanding of the mission of conducting elections, and clear communication of the same to technology implementers, that the project has a chance of success of meeting the needs of that mission.

B. Clear Goals for the Project

There are many possible goals a new technology project might achieve: saving money, boosting efficiency, increasing accuracy, aiding transparency, etc. These goals are not always compatible, and all members of management do not always have the same vision of the project's goals. Starting a project without a clear, common set of goals is a recipe for future conflict that can derail any project.

C. Realistic Expectations

New technologies are often introduced with blind faith that the technology will (in and of itself) provide a major benefit, or solve a significant problem. As an example, more than one EMB has suggested introduction of geographic information systems (GIS) to solve a problem with boundary delimitation. GIS is a great tool for mapping, and for drawing and revising boundaries, and as such it can be a powerful tool as one component of a system for defining constituencies. But a GIS

system requires substantial investment of resources to digitize maps, identify coordinates of major landmarks, populate a geospatial database with numbers of registered voters, etc. It is important to take time to understand the limitations as well as the promises of any technology, and to plan for how the technology will be integrated into an overall solution.

D. Openness to Re-engineering

Introduction of a new technology often requires extensive re-engineering of regulations and procedures in order to be effective. For instance, many EMBs have introduced automated fingerprint identification systems (AFIS) to help eliminate duplicate voter registrations.[1]

An AFIS system can only be effective when introduced as part of a comprehensive plan that includes:

- A plan for collection and storage of fingerprints with adequate controls to prevent false prints.
- Detailed procedures for how screening will be done, including filtering (or searching) by such other criteria as age, gender, race, and possibly geographical area.
- A policy for how suspected duplicates will be handled: whether one or multiple instances will be automatically removed, what further investigation may be done, what enforcement will occur in cases of suspected fraud, etc.
- How the public will be informed of the new system and its benefits.
- How other stakeholders, such as political parties, NGOs, and media, may react to the new system.

It is also possible that introduction of AFIS may require changes in the law to allow collection of fingerprints, to protect the privacy of personal data, and to indicate penalties for fraudulent registration.

Technology can serve as a powerful tool, but without a clear understanding of the problem—and a comprehensive plan that combines new procedures, new technology, and training of staff in how to use the new system—the technology is almost certain to fail.

E. Appropriate Technology

The concept of "appropriate technology" was introduced over 30 years ago by economist E.F. Schumacher,[2] who expressed concern about the start-up and maintenance costs of new technologies, as well as the environmental, social and cultural impact of those technologies. Some obvious examples of inappropriate technology may help to clarify the critical nature of appropriateness as a criterion for selecting technology. Fifteen years ago, a technical assistance project proposed to provide a fax machine to every district office in a country where few district offices had electricity or telephone connections, and some didn't even have a roof overhead. In another country, an EMB tried to introduce an electronic ballot box 10 years ago into a similar environment, despite the fact that the ballot box was designed to communicate results from the polling station via telephone landline, and almost no polling station had access to such a connection.

While these examples are glaringly inappropriate, other uses of inappropriate technology may be more subtle, such as in countries where sophisticated systems are introduced with either donor funding or large capital investments by the government, only to be abandoned because of lack of available funds to pay for ongoing maintenance of the system. A high-cost project that is used for

[1] The caution (expressed in the previous point) about realistic expectations is appropriate to repeat here with regards to AFIS, as this technology can help to identify "suspected" duplicates, but is not a perfect fit for the many-to-many comparisons required for voter registration screening of duplicates. A detailed analysis of AFIS is, however, beyond the scope of this paper.

[2] E.F. Schumacher, *Small Is Beautiful: Economics As If People Mattered: 25 Years Later...With Commentaries* (Hartley & Marks Publishers, June 2000).

only a single election cycle cannot be considered a successful project. The topic of appropriateness is important enough that it will be covered in more depth later in this paper.

III. Who Should Be Involved in Planning?

As noted above, the fifth factor most often responsible for the failure of software projects is lack of stakeholder buy-in. We believe this is even more important for electoral projects, where trust is such an important component. It is recommended that "stakeholders" be defined broadly to include all staff that will use or be affected by the new system, political parties, civil society, media, the electorate, and international partners. It is further recommended that these stakeholders be engaged in the project from the earliest stages so their concerns can be considered before the design phase.

In many technology design methodologies, the first phase of development is the drafting of a "Vision / Scope Document" that defines issues to be addressed, identifies the context in which the new system will be deployed, and describes the desired end result. The context should include all stakeholder concerns. When creating a new voter registration system, these concerns are likely to include transparency, adequate scrutiny of the registration process, accessibility to the electoral rolls, and a number of issues specific to the particular country. A broad stakeholder meeting (or meetings) could help to identify these concerns and could also help to anticipate and resolve conflicting goals before they become contentious issues. For example, political parties almost always want the broadest access to the details of the voter list possible, while civil society organizations may raise issues about personal privacy. Such conflicting concerns are fairly easy to resolve at a time where all stakeholders are interested in helping to define new features, but may derail a new system if not addressed until after the system is released.

It may also be appropriate, depending on the scale of technology introduced, to have public information sessions where voters can learn about the proposed technology and give feedback. Such public feedback opportunities are used too rarely, particularly in light of the reality that it is

Composite Case Study: Painted Into a Corner

It is generally unwise to make specific technology solutions a part of electoral legislation. This eliminates the freedom that EMBs have to follow best practice with respect to the use of technology.

Country X passed a new electoral law that specified the use of automated fingerprint identification systems (AFIS) in its voter registration process. Country X, an emerging democracy, has tens of millions of eligible voters and high levels of illiteracy.

Short timelines to the next election and enormous political pressure forced the EMB to outsource its voter registration process. Lacking experience in the technologies associated with the project (including AFIS, OMR/ICR, ID card production systems), the Request for Proposals was rushed to get the procurement underway and did not sufficiently taken into account the environment, necessary human resources, or operational and logistical challenges. The electoral law that mandated the use of the technology had not been specific as to how to handle duplicate registrations identified by the technology.

Other factors influencing procurement were commercial interests of donor countries and pressure from donors to select vendors from a specific country. Late commitment of government and international funds further hampered the procurement.

Halfway through the procurement, it was observed that, while the equipment required for the field and provinces (to capture and consolidate voter registration data at provincial level) was being procured, no national-level data center was included, though this was needed for the entire voter registration database to be certified by the Chairman of the EMB. A last-minute additional procurement was required that suffered from the same deficiencies as the main project.

The number of vendors capable of delivering an integrated solution with the required components (VR, ID card production and AFIS) is very small indeed. The procurement process was fraught with compromises, and allegations of irregularities were made.

With enormous effort by the EMB, the vendor consortium and the international community, the project got underway. Because of the difficulty of training ad-hoc staff in the field, the delays in implementing the data processing centers and the slow production of ID cards, several delays and extensions were necessary. Worse, not all data was processed using the new AFIS technology. Following the completion of the election process, the reports of the observer missions were highly critical of the voter registration process.

When Country X prepared to embark on the subsequent election process, the infrastructure used for the initial election had largely broken down. The IT department of the EMB had not received any meaningful training as part of the original contract (or, given the constraints of time, this training had been confined to the use of the system, not to its maintenance and support). Rather than address this human resource deficiency, the EMB decided to again outsource the voter registration technology solution.

the voters themselves who are both the "customers" of the EMB, and the owners of the electoral process.

The importance of this broad-based planning cannot be overemphasized. A technology project for elections can be enhanced or derailed by staff, political parties, media, civil society organizations, or voter response, so getting input and feedback from all of these groups can help point the project in a direction that maximizes the probability of success.

IV. Appropriate and Inappropriate Projects

A. What are the Criteria?

Can we afford it? This question is very different from "Is the money available to procure it?" The answer to the latter is frequently "Yes. Donors are lining up to fund it." The initial question—"Can the EMB afford it?"—is the more appropriate one for both EMBs and donors, and involves both the up-front and long-run investments of cash, time, and other resources. Measuring return on investment is difficult for an EMB. Unlike an enterprise, where impact on the bottom line (whether through increased revenues or reduced costs) is the main yardstick for IT investments, EMBs cannot put a dollar (or pound or euro) value on benefits such as increased accuracy or completeness of a voter register or greater transparency.[3]

EMBs and donors alike must consider whether costly IT projects divert funds from other important areas of elections, such as voter and civic education, political party outreach, domestic observation and so on.

It appears to many IT experts that large elections technology projects are currently over-prioritized in election assistance as a fix-all for election difficulties that can be applied anywhere, regardless of context, in part because of their high visibility and flashy elements. It has been suggested, with only some irony, that this could be seen as the new millennium equivalent of the overuse of the hydroelectric dam as a development and agricultural cure-all in the 1970s.

Can we maintain it? The world is littered (sometimes literally) with the remnants of electoral technology projects that, having helped get countries past a particular election cycle, fall into disuse, disrepair and eventually cease to exist. International experts and vendors pack their bags and depart, leaving local IT personnel to keep things running.

Maintenance of large information systems is costly, and involves more than just keeping hardware running. For example, continuous voter registration requires database maintenance, assuming the voter register is computerized to begin with. EMBs frequently overlook the effort, time and cost involved in ensuring that voter registration databases are kept up to date with the addition of new voters, alteration of voter details (change of address, marriage, corrections) and deletion of the names of the deceased. Such unmaintained data has a very short shelf-life.

Recruiting, training and retaining (as further discussed below) skilled IT personnel is costly and time-consuming, and often overlooked. Most donor-funded development projects outside of IT projects include language relating to capacity building and institutional strengthening. A small proportion of IT procurements include training components. Too often election-related IT projects are, in execution, no more than shopping lists for hardware, software and consumables. The capacity building and training components should not be overlooked because all available resources are focused on getting the election process out the door.

Will it integrate with our existing information systems? If an EMB has existing electoral information systems, any proposed new technology investment must integrate with these systems. Failure to integrate increases the work (and risk of failure), for example, to copy data from one system to another. Any efficiencies brought by the new technology are more than offset by the effort required to manually synchronize unconnected databases – e.g. when electoral areas

[3] See J. Vermillion, "Problems in the Measurement of Democracy" *Democracy at Large*, 3:1 (2006).

change. This can be seen when an EMB invests in a GIS that outputs electoral maps. These look great on the website but, if the GIS is not integrated into the voter registry databases, any changes must be entered twice – once for the database and a second time for the GIS, with a high risk that the two will soon by out of synch with each other.

B. General Guidelines on Appropriate and Inappropriate Technology

Given the above criteria, it is evident that appropriateness is not a characteristic of any single technology. A range of factors determine the appropriateness of a particular technology, including the institutional capacity of the EMB; its experience with all technology; its IT personnel; and the prevailing political, legal, environmental circumstances.

Having said that, an **appropriate** technology for elections management should be:

- Cost effective
- Easy to manage, deploy, support and extend
- Mature
- Interoperable,[4] modular and flexible
- Standards-based

Any elections technology that fails to meet the guidelines above is **inappropriate** and should be avoided. Again, for emphasis, appropriateness is hugely context-sensitive. Solutions relying on highly proprietary software or hardware (that is, for which support, maintenance, or development needs can be met by only one vendor) are generally risky investments. If, for example, the manufacturer of a particular system component (for example, a biometric fingerprint reader) goes out of business or simply stops supporting a legacy product, the EMB may be forced to scrap the entire system. EMBs should keep things modular and flexible to the greatest possible extent.

As the saying goes, the pioneers are the ones with the arrows in their backs. Enterprises may gamble shareholders' money on untried new technology, but EMBs should never gamble democracy in this manner.

V. How to Proceed

A. Avoid Common Pitfalls and Risks of Failure

Successful technology but does not advance democratic principles: What value does a satellite vehicle tracking system bring to your country if large numbers of voters still have to walk for four hours to the nearest polling station? Why spend millions of dollars on high capacity ID machines if you lack the logistical capacity to distribute them and thousands of voters don't get their cards in time to vote?

These questions are based on actual failures of elections technology. The technology worked just fine but the democracies in question were weakened (or at minimum, not strengthened) by the EMB's choices. In the former example, the money spent on the vehicle tracking system could and, arguably should, have been spent on providing more polling stations in rural areas

Unsustainable solutions: Some systems, such as voter registration databases, have an alarmingly short shelf-life. If the systems and technology put in place to create a computerized voter register are not maintained and if the procedures, resources and personnel are not in place to update the database on at least an annual basis, sustainability cannot be achieved

[4] "Interoperable" refers to the ability to integrate with existing or future technologies the EMB has or may develop/procure.

Inadequate IT staffing provided: There is a huge gulf between public sector pay scales for IT personnel and potential earnings in the private sector. EMBs struggle to find and retain qualified and experienced IT personnel. Even if you get such personnel, they will, if they are lucky, gain highly marketable skills working on the technologies typically used in elections management. The tragic irony is that the better the person, the more likely you are to lose them. The terms of reference of international IT personnel must be broadened to include capacity building. This must be facilitated by bringing them in early or keeping them on later (after the election is over). Too often international elections IT staff are fire-fighters, brought in during the heat of battle and withdrawn as soon as the elections are completed.

How can EMBs retain good IT staff? Some ideas (used in several countries) include:

- Obtain a waiver from public service/civil service payment constraints for mission-critical elections IT personnel.
- Ensure that IT personnel are able to travel overseas on secondment to international NGOs, UN, OSCE, other EMBs ,etc., and are remunerated accordingly.
- Allow lengthy leaves of absence for relevant study or personal development projects.
- Seek joint funding support for IT salaries from international donors.

B. Start with Basics

E-mail: Email is the bread and butter of efficient communications. Despite this, many EMBs in developing democracies lack the skill to effectively utilize email, or lack email systems entirely. In the 25 countries where the authors have worked, only a handful of EMBs could be said to use email effectively. There is an EMB in a large country (tens of millions of voters) that still communicates entirely on paper. Every official has a computer on his/her desk and an email address, but all incoming emails are printed and photocopied for circulation. All outgoing messages are dictated and hand-written on paper, transcribed by junior (and sometimes not-so-junior) staff onto computers. To this EMB, email IS new technology.

Composite Case Study: Doing it Right

In Country Y, the process of computerizing the voter registry was begun by the EMB more than three years before the next scheduled election. International donors were engaged, and agreed to an assistance project that lasted more than two years, with goals of fully implementing the new system and training local staff to maintain it. The EMB selected technologies that had been used widely in the country, including Polaroid photos and optical mark recognition (OMR) for data entry. OMR technology was particularly well-suited for this country's data capture since it was already familiar to all teachers, and registration was scheduled during school break when teachers could serve as registrars.

Local IT staff received training in database management and software development over a two-year period, were certified for providing maintenance on the optical scanners, and a local print shop was certified for printing OMR forms.

Registration forms were designed by a forms specialist, then refined through a series of pilot tests. All registrars received training, during which they completed sample registration forms that were scanned, with feedback given on the most frequent errors.

Polling stations were established before the beginning of registration, and voters registered at the same location where they would later return to vote.

The end result was one of the most accurate voter registers in the world, and an EMB that has maintained the system on its own, as well as provided several experts to help other countries create computerized voter registration systems.

Acknowledging the difficulties with reliable, speedy and inexpensive Internet connections in developing or post-conflict countries, EMBs should prioritize electronic mail as the foundation of its use of technology. The vision is simple: every official with a computer should also have an email address on the EMBs' own domain (that is, internal network),[5] a connection to a local email server and the necessary training in the use of an email client application (such as Microsoft Outlook).

[5] The use of Yahoo, Hotmail, GMail or similar free, web-based email services should be discouraged; these are insecure and hugely inefficient where bandwidth is scarce.

To make this vision a reality would require modest resources, both in terms of cost and technical skill. Successfully implementing an email system at the EMB is an easy and capacity-building "win" scenario for the EMB's IT staff. The experience gained in networking, server and database administration (as email servers are database-driven), security, user support, and vendor liaison (ISP and software vendors) is highly relevant to future, more ambitious, elections technology projects.

It is difficult to underestimate the benefits of email both in terms of improving an EMB's internal communications and building its IT staff's capacity. Few donor-supported projects recognize the benefit of the "start small" approach. Donors should attempt to encourage and support EMBs in modest, "winnable" technology projects prior to embarking on more ambitious programs.

Local area networking: In order to bring about improved communication, productivity and efficiency, desktop computers should, where possible, be connected to a local area network (LAN). This allows file and printer sharing, email and Internet connectivity, and sharing of printers. EMBs should harness the inexpensive technology of a LAN before embarking on more ambitious or expensive wide area networking (WAN) projects. As with email, the skills and experience gained by IT personnel in building LANs will provide a solid foundation for future projects.

One large EMB in Africa had[6] over 50 full-time IT professionals on its headquarter staff housed in a brand new building. Because of a culture of procurement, the EMB did not allow the IT department to wire and configure its own LAN. Because the large sum of money required to outsource the task was not available, the network remained an elusive dream. The head of the IT department wished aloud (to this author) that he had ten rolls of ethernet cable and some switches so he could implement a local area network. His staff could not share a single printer or connect to the Internet.

Internet access*:* The Internet is an essential tool for communicating with support resources (updates, patches), with vendors and potential vendors, and with donors and other stakeholders.

Connecting an EMB to the Internet brings its own challenges in terms of policy, productivity, security (virus, mal/spyware, hacking) but, in turn, it also develops the capacity of the EMB and its IT personnel in disciplines such as LAN and WAN, security (policy and enforcement), encryption, email and antivirus solutions.

Skills and experience gained with, for example, building an intranet, will permit the EMB to develop its own Internet presence (website).

Desktop applications: One of the most under-rated technologies for elections management is the humble spreadsheet application. Typically, this will be Microsoft Excel, though others are available.[7] Most of the information associated with elections management includes lists of text

Platform	Average Cost
Excel	$ 500
Access Individual	$ 3,000
Access Simple Multi-user	$ 10,000
Access Workgroup/Department	$ 50,000
VB and Jet	$ 200,000
VB/VS.NET/Java and SQL Server	$ 500,000
Oracle, IBM db2	$ 2,000,000
SAP, Tandem, etc.	$ 10,000,000+

Figure 1. The estimated cost to produce databases (Source: FMS, Inc. www.fms-inc.com)

[6] This was true as of December 2005.
[7] For example, Open Office's Calc is an option. See http://www.openoffice.org/product/calc.html

(lists of districts, registration centers, polling stations, candidates, poll workers, or vehicles) together with numbers (numbers of registered voters, ballot papers, results, payments). Many EMBs also create databases using Excel; the distinction is blurred and the technical differences are beyond the scope of this paper.

Anecdotally,[8] organizations that are experienced users of spreadsheet applications are better placed to succeed with database-driven elections information systems.

Financial management: Accountability, one of the principles of good governance, is enhanced by use of financial management software applications. An EMB with adequate desktop computer and local area infrastructure can, with relative ease, implement accounting software. Donors may not be enthusiastic about supporting such projects, preferring to focus on elections technology as distinct from technology for elections management.

C. In-house vs. Outsourced

In any organization that relies on mission-critical information systems, a strategic decision is required early on: do we develop our solutions in-house or do we procure/outsource? Naturally, a hybrid of the two approaches is also possible. Where the in-house approach is preferred, the IT function must be staffed with:

- Systems analysts, preferably with domain knowledge;
- Software programmers; and
- Generic systems/network administrators and support personnel.

Where the emphasis is on outsourcing or procurement of solutions, a very different human resource profile is called for. In this second scenario, expertise is required in:

- Business needs analysis;
- Writing of generic technical tender documents;
- Liaison with contract and legal staff;
- Project management (especially in a multi-vendor environment); and
- Negotiation.

Outsourcing is justifiable where a single huge effort will be undertaken just once (such as the creation of new identification cards for the entire voting population) but will be followed thereafter by a lower level of activity (new voters coming of age, issuing of replacements for lost cards, changing voter details, etc.).

Cost difference: Saving money by outsourcing software development is available only for highly homogenous, mass market applications. Despite the conceptual simplicity of computerizing a voter register (after all, a voter roll is just a list of names and addresses, isn't it?), the reality is that no two countries are alike and, with information systems, the devil (and therefore the cost) is in the detail.

Elections technology vendors will, quite reasonably, argue that they are entitled to a profit and only the most foolish bidder will leave out some contingency figure. The winning bid for a recent, large voter registration system was approximately twice the estimated in-house cost as estimated by both local IT staff and international consultants.

Another factor frequently overlooked is the cost of managing outsourced tasks. Hours of management time is spent on contract negotiations, project steering, technical review and, where necessary, legal oversight.

Sustainability: If developed in-house, then in-house staff know how to operate and modify the system. Third-party maintenance and support contracts for customized software products are

[8] That there is little research on the benefits of spreadsheets may either reflect their ubiquity or refute the statement.

extremely expensive. There is the real possibility that the company that delivered the solution may no longer exist (this is common where consortia are assembled for the contract and dissolve soon after).

If outsourced support is required throughout the project life-cycle, costs will increase accordingly. However, building the capacity to support, maintain and, ideally, extend the functionality of a vendor-provided electoral information system in-house also requires time and money.

Contracting process can bring greater discipline to the planning: There's a saying in procurement: if it's not right in the RFP, it will never be right. If sufficient time is spent getting the RFP to clearly and comprehensively state what the EMB needs to procure and if the evaluation of received bids and the subsequent contract negotiations help to clarify the requirements, this in itself adds value to the process.

All this assumes that the EMB has the capacity (based on its experience with in-house technology projects, previous contracts and general IT proficiency) to properly engage in these demanding activities and, further, that sufficient time is available.

A good solutions provider will work hard to find out exactly what the EMB wants. Time spent on gathering information about customer requirements, including careful business process analysis and, where necessary, re-engineering, will pay dividends in the longer term.

Problem with vendor-centric requirements analysis: A vendor that has a single product to sell will expect the EMB to yield to the implied methodology: the tail will wag the dog every time. In a newspaper advertisement for expressions of interest in electronic voting systems, one EMB actually stated:

> Interested reputable organizations are expected to lead study groups of [EMB] officials to conduct the studies and consequently conduct Pilot Schemes.

This was an invitation to disaster. EMBs must arrive at a clear determination of its technology needs prior to any engagement with vendors. This determination will naturally involve surveys of available technologies,[9] study visits to other EMBs to learn from their experiences and a realistic appraisal of their own capacity (both financial and in IT human resources). Then, and only then, should expressions of interest be sought. All ongoing studies and pilot schemes must be firmly led by the EMB—not the vendors.

Susceptibility to marketing hype: Procuring large and expensive technology is difficult, time-consuming and requires significant technical information. Marketing hype is just one obstacle to getting answers to the most challenging questions of all: "Will this product solve my problem?"

VI. Conclusion

Technology does not create good electoral processes. Too often the failure of an election technology project is a failure to live up to inflated expectations that the technology will magically solve complex problems without hard work and sacrifice on the part of election managers and stakeholders. This is not to say that technology has no value in elections; rather, technology can put a powerful set of tools into the hands of electoral managers. Whether these tools are constructive or destructive depends a great deal on the competence of those managers and the degree of diligence exercised in using the tools.

This chapter has attempted to help shape realistic attitudes about what technology systems can and cannot accomplish and to provide some guidelines to help maximize the effectiveness of such tools. To summarize:

[9] To research available technologies, Internet access to resources such as vendor white papers, websites such as http://www.aceproject.org and http://www.ifesbuyersguide.org are important.

- Technology can only effectively help an EMB accomplish its mission if the EMB has a strong sense of that mission and invests the time and energy to communicate it to the system designers.
- A clear statement of the goals of the project, coupled with realistic expectations about what the tools can and cannot accomplish, is essential.
- Introduction of new technologies often requires re-engineering of legal and procedural frameworks and retraining of staff to take advantage of the new capabilities.
- Stakeholders—including political parties, civil society, media and the voters themselves—play a crucial role in determining the success or failure of the new technologies. Therefore, it is crucial to involve these stakeholders from the very beginning of planning the implementation of a new technology.
- In order for a technology to be deemed appropriate, it must make a positive impact on the electoral process that is commensurate with the cost, and it must be sustainable in the environment in which it is used. Sustainability implies ongoing financial and human resources are available to support the new technology.
- EMBs searching for the "next great technology" are encouraged to evaluate existing and well-established technologies first, as these provide a cost-effective set of tools that can have an immediate and powerful impact on effectiveness of management.

Technology can help to improve accuracy, reduce costs, increase efficiency, and provide greater transparency—or it can be a huge waste of resources, or worse, damage the trust and confidence of voters. It is up to the EMB to proceed in a manner that promotes, rather than impedes, effective electoral processes.

The Introduction of New Technologies From the Election Administrator's Perspective

Linda Edgeworth

I. Introduction

The administration of elections is a complex business. Most senior administrators, whether they are elected officials, politically appointed or employed as civil servants, come from other fields with little or no specific election experience. Many are lawyers or judges; others are employees of government offices responsible for civil registries, tax records, or vital statistics. Still others are politically prominent citizens nominated by political parties to serve on election commissions activated during election cycles. Most of them become "election professionals" through actual experience on the job. As all election officials learn, the picture is never static. And, now, with the ever more rapid pace with which new technologies are introduced in the marketplace, new pressures to modernize bring new challenges to the election administrator, who must now add a sound grasp of the world of high tech to his or her skill set.

II. The Lure of New Technologies

Election management bodies (EMBs) around the world are constantly looking for ways to improve election processes. Without a doubt, the lure of new technologies is compelling. The "buzz" about the "latest best thing" not only reaches the ear of the election administrator, but the ear of every elected official who has ever had to wait until the wee hours of the morning for the last precinct to report, or who has ever had to respond to a constituent whose name could not be found on the voter register. Every news story about a real or perceived problem or delay in the election process brings with it new demands for reform. And, in this day and age, "reform" often translates as a demand for expedience and speed through technology. In the wings is a stream of vendors ready and waiting to offer their services and their wares to satisfy those demands.

III. Removing the Mystique

In moving forward, EMBs have some solid ground to stand on. All elections and the results they render—whether they are achieved manually or with high tech devices and sophisticated network applications—must still be conducted on the firm foundation of common principles. They must be accessible, secure, accountable, auditable, and transparent. There should be no mystique. Regardless of the voting system utilized, the basic functions are the same. Manually or electronically, election management and voting systems will continue to center on the same functional components.

- A system must be in place to distinguish those people who are eligible to vote from those who are not eligible; it must also provide a mechanism that ensures each eligible person is allowed to vote only once.
- A voter must have an instrument on which to express his or her voting intent, whether by pen on a paper ballot or by touch on a DRE.
- The security and secrecy of the vote must be maintained, whether by sealed ballot box or secured electronic data storage device.
- Voters' votes must be read accurately, by human eye, optical reader and/or digitally.
- Precinct returns must be transmitted, by personal delivery or secure electronic transmission.
- Results must be consolidated, whether manually or by machine.
- Preliminary and final results must be reported accurately and on a timely basis, whether electronically or manually, on the Internet or in printed form.

Modernization will never alter the fundamental requirements of free, fair and transparent election processes; rather, it will alter the manner in which optimal conditions related to integrity, security, credibility and accuracy are achieved. The challenge for the EMB is to respond to the demands for change responsibly and to oversee the introduction of new technologies in voter registration, automated voting, counting systems or electronic transmission of results without succumbing to the common pitfalls that can undermine the planning process along the way.

IV. Common Pitfalls in Moving Forward

On the pages that follow are discussions of some of the most common pitfalls found in preparing for the introduction of new technologies. Examples of success stories and lessons learned are also included to illustrate how some jurisdictions have dealt with their own transitions. Among them, examples are drawn from the author's experience in the U.S. and the Philippines. They include two counties in Florida where world attention was drawn to the imperfections of electoral processes in the 2000 U.S. Presidential Elections. Hillsborough County and Miami-Dade County responded to the demands for change in Florida and planned their transitions to electronic voting systems with varying degrees of success. Other examples are drawn from the experiences of the Philippines, where the introduction of new technologies is just getting underway after an unfortunate false start in an earlier attempt.

The Republic of the Philippines had been considering automating their voting system for quite some time. An initial law for the introduction of modern technologies was enacted in December of 1997. However, the Act was seriously flawed in a number of ways. Not only did it preclude the Philippine Commission on Elections (COMELEC) from considering alternative technologies, it contained detailed specifications that seemed to refer to the equipment of one specific manufacturer. Additionally, violations of Republic's purchasing guidelines combined with administrative deficiencies resulted in the collapse of the initial attempts to use optical scan voting technologies during the 1998 elections. The use of newly purchased equipment was ultimately abandoned after a Supreme Court ruling mandated that the equipment be sealed, stored and not used again. Since September 2005, IFES has provided a number of consultancy services to COMELEC related to its fresh start in its pursuit of modernization, including reviewing and commenting on proposed legislation. Amendments to the law have been developed that (1) provide appropriate authority to the COMELEC to modernize the election process through the proper acquisition and introduction of the modern technologies, (2) remove obstacles that impeded prior attempts to modernize, and (3) define foundation principles and guidelines for implementation that will improve the likelihood of success.

The positive experiences and lessons learned in these jurisdictions serve as useful reference points in this discussion of some of the challenges and pitfalls faced by EMBs as they modernize their electoral processes.

Election officials know first hand that no election system is perfect and that often the success or failure of the system rests in the details. This is certainly true when it comes to planning for the introduction of new technologies in the election process. There are some common pitfalls that hinder the successful implementation of the plan and appropriate installation of new technologies. They include omissions or misjudgments related to:

- identification of actual needs and the most suitable technological solutions to meet them;
- the political, public and physical environment in which they will be introduced;
- the assessments of short- and long-term costs and the continued political will to fund them;
- establishment of a realistic time frame required for implementation;
- the articulation of definitive specifications for the solicitation of proposals from prospective vendors for equipment, programming or services;
- the negotiation of contracts with vendors that adequately secure the state's interests; and,
- the institutional implications and commitments over the long term.

V. Defining Needs and Suitable Technological Solutions

In the face of growing pressure to embrace new technologies, lawmakers and EMBs can sometimes have difficulty clearly defining the actual need to be served and the most suitable technological solution to satisfy that need. In some instances the introduction of new technologies is envisioned as part of a long-range plan for improving overall efficiency and communications, streamlining program delivery, integrating various systems and sub-systems, lowering costs of operation, and minimizing manpower requirements. However, in some circumstances modernization and automation is spurred by a sense of urgency to overcome a specific problem.

Failure to assess the cause of the problem accurately can lead to a premature rush toward modernization, result in overextension of fiscal and human resources, and generate stress on existing institutional capacities. In light of the criticism of punch-card voting systems in Florida, for example, the push to enact new federal and state legislation prompted the abandonment of punch-card balloting altogether. What followed was a rush to purchase electronic voting machines, with insufficient time for EMBs to fully understand all of the consequences. EMBs, lawmakers and political parties alike generally failed to recognize the implications of electronic voting with respect to the options they allowed for traditional recounts in response to election challenges. Within months U.S. states were mired in controversy when the new systems were criticized for not providing a voter verifiable paper audit trail. New federal legislation that would require that DREs used in federal elections generate a printed representation of each voter's ballot is pending. Similar legislation is being debated in several state capitals as well. Unless their DRE units can be upgraded, states that moved quickly to abandon their punch card and lever voting systems (in favor of what was then "state of the art" equipment) could find they have to purchase all new equipment should any of these legislative bills pass into law.

In some instances less dramatic solutions might be more suitable as a prelude to the institution of a long-term plan for a more comprehensive overhaul of the system. For example, the introduction of electronic voting machines in the Philippines is being viewed as a means of solving major problems related to perceived inaccuracy and delay in the reporting of election results. The Philippines has a quarter of a million polling stations. Votes are hand counted at the polling stations after the close of the polls, and tabulation is accomplished manually throughout the country. The likelihood of human error at any stage in this process cannot be dismissed. The accumulation of manually tabulated results from polling stations at the municipal, provincial, district and national levels, and the absence of a credible audit process, has raised serious distrust among political participants and voters with respect to the legitimacy of the results reported at the national level. While automation is seen as the solution, current plans call for only pilot testing to be conducted in the first elections following enactment of the new law. In the first roll out, automated voting systems are to be used in two highly urbanized cities as well as in two provinces in each of three specified districts. Nationwide implementation is to follow by 2010.

In the meantime the root causes of distrust among political participants and the general public still need to be addressed. Based on further investigation of the current counting and tabulation systems, IFES suggested that, in the interim, other reforms could be implemented that would have an immediate positive affect on the accuracy and timeliness of the reporting of results, even in paper ballot jurisdictions where counting will continue to be done manually. Ballots are currently printed without the names of candidates in the various races; each voter refers to a posted list of candidates and handwrites his or her choice on the ballot. By virtue of its design, the current ballot style combined with the manual tabulation process not only creates a fertile environment for purposeful manipulation and fraud should individuals or groups chose to pursue such endeavors; it also provides the perfect environment for an even more likely and insidious threat that can be just as injurious to a credible election: human error. From the minute a single voter is given a ballot to mark the field is set for a chain of human errors that, in the worst case, can remain hidden indefinitely. Including the candidates' names on the ballots and developing a system for data entry and electronic transmission of results would go a long way toward achieving the desired ends, even in polling stations where paper ballots might still be used and counting is done manually. Earlier Philippine House and Senate bills did not included such provisions. However, as of 6

December 2006, they were included in the compromise bill that emerged from the conference committee. It is yet to be seen how soon these provisions will actually be executed nationwide.

VI. Understanding the Political, Public and Physical Environment

Planning the introduction of new technologies also requires an understanding of the political, public and physical environment in which the technologies will operate. EMBs may be very enthusiastic about prospects for modernization of the electoral process; however, if they have failed to take into account attitudes of political players or have made no effort to identify interested and supportive legislators in advance, they may find their proposals fall on deaf ears. Insensitivity to the public's apprehension or distrust of change may make implementation a hard sell, especially if the media generates negative publicity that is not preempted or adequately answered.

Another major pitfall is failing to systematically assess the physical institutional environment in which new technologies are to be introduced. Such an assessment should be made relative to both the public and private sectors, especially at the local level. Realistic planning should involve such tasks as taking inventory of the state's existing policies and practices regarding the use of technologies and, in particular, whether or not there are already similar types of programs, databases, internal networks, or electronic data transfer systems used by other departments. The technologies being introduced should not be so far out of step with current policies and capacities so as to doom them from the start. Another major part of the task is to realistically gauge the readiness of election staff and their current familiarity with basic office systems, including their comfort level with computers, software and use of the Internet. The EMB must assess its need to offer specialized training to bring the staff up to speed. Likewise it may be necessary to augment its personnel with information technology specialists or determine the feasibility of seeking such support from other suitable government agencies.

Where there are significant differences in the infrastructures of urban and rural areas, a one-size-fits-all solution may not be feasible. An interactive, online, real-time voter registration program that succeeds in an urban area would not be particularly suited to a remote area where electricity and phone service is unreliable or non-existent or where there is no access to technical support. Such conditions may also impact decisions related to the introduction of electronic or optical scan voting and counting systems, the use of electronic voter lists or poll books at the polling stations, or plans for the electronic transmission of results. Under such circumstances, lawmakers and EMBs should be prepared to consider the co-existence of different systems and the procedural implications involved. Once motivated, lawmakers and EMBs are sometimes so focused on modernizing that they fail to consider the implications for remote areas of their jurisdiction. Previously, the Philippines had not contemplated the use of mixed technologies. However, the Philippines is a country with a very diverse mix of environments across its many islands. During its consultancy, IFES raised this issue and the subsequent draft of the compromise bill includes language allowing the use of different systems, including electronic and paper-based systems, in the same election in different provinces as the COMELEC deems appropriate and practical.

VII. Underestimating the Time Frame for Implementation

In the face of outside pressures and with the promise of major advancements in the process just around the corner, it is easy to underestimate the time it takes to actually put new technologies in place. The standard rule of thumb is that it takes about 18 months to two years to introduce and implement new technologies, depending on the type of program being modernized and the magnitude of the change. A lot has to happen in that time frame.

A. Assessment of Needs and Solutions

The EMB must complete a thorough assessment of the needs for which technological solutions are being pursued. Research must be accomplished to determine what options are available. Where possible, they should draw on technical experts from the public and private sectors, appropriate

nongovernmental organizations and academia for support. In the Philippines, an Advisory Council has been legally established to assist in the assessment and evaluation process and to make recommendations to the EMB regarding the most appropriate, secure, applicable and cost effective technology to be applied. The Council includes members from the Commission on Information and Communications, the Department of Science and Technology, academic institutions, information and communications professional organizations, nongovernmental electoral reform organizations and a member with specific experience managing or implementing large-scale information technology projects. In addition to providing input on optimum technologies, members of the Council also participate as non-voting members on the EMB Steering Committee, which is tasked with implementation. In this capacity, they are expected to offer advice in the planning, inception, development, testing and evaluation stages.

B. Designing Specifications and Selecting a Vendor

Once the objectives are identified through such an assessment, detailed specifications must be developed so that requests for proposals can be solicited from competent vendors. Sufficient time must be allowed for vendors to develop their submissions. Criteria must be developed by which proposals will be evaluated and a vendor will be selected.

One of the subtle traps that EMBs and lawmakers can fall prey to is the "help" offered by vendors. To better understand the various kinds of technologies that are available, election officials often seek out information from various vendors and suppliers. Unfortunately, what starts out as pre-solicitation research can develop into a vendor-driven acquisition process in which requests for proposals are designed in a way that leans toward a particular vendor. It can sometimes be difficult, but EMBs and lawmakers need to be mindful of maintaining some distance and objectivity to promote genuine competition and to ensure that the best interests of the political participants and the voters are being served. In addition, anytime the legitimacy of the solicitation process becomes tainted by real or perceived favoritism, the likelihood for appeals and legal challenges by aggrieved competitors increases. Such challenges can significantly delay the award of a contract and generate negative publicity that erodes public confidence.

Another issue that needs to be considered very carefully is whether a single vendor should be selected or whether multiple vendors should be considered. This consideration is particularly recommended when new technologies are being implemented simultaneously for the automation of voting and registration systems. There are vendors who provide services in each of these areas and offer maintenance, technical support and commodities as well. While there are certainly advantages in "one-stop-shopping," it can also become a serious problem if that vendor is overextended and cannot provide timely and reliable service, or the company collapses.

EMBs are at a serious disadvantage if purchasing rules preclude them from being on the evaluation team. In some jurisdictions, only designated administrative staff members from the procurement office participate. Wherever possible, it is critical that EMB staff be involved; it can also be very helpful if end-users, such as clerks and/or local-level officials, are part of the evaluation team. As practitioners involved in day-to-day operations, they often have insights that escape the notice of senior management.

Hillsborough County in Florida also chose to involve the public in the evaluation process. As part of its criteria, each vendor was required to provide its DRE model for public familiarization purposes. The various units were set up in shopping malls, schools and other public places where people could try them. Evaluation forms were provided so that members of the public could indicate which unit they liked best. These events provided great opportunities for media coverage. Ultimately, these evaluations proved invaluable in the selection process. Based on the pre-established evaluation criteria, the evaluation committee selected a vendor whose product exceeded their budget limit. It turned out that it was the unit also most preferred by the public. Armed with this information, the EMB was able to get approval for the increased expenditure from the County's Board of Supervisors. Where the Board might not have been sympathetic to the EMB's request for a budget increase, they were more responsive to the voice of their constituents. Ultimately, observers noted that the equipment selected by Hillsborough County worked very well on election day in 2002.

C. Contracting and Delivery

Once a vendor is selected, negotiation of the contract also takes time. It is likely that attorneys of both parties will review the legal technicalities. Great thought must be invested in refining the description of deliverables and terms of payment. It is also important to clearly define the terms for the ongoing relationship in terms of warranties, including replacement and repair, maintenance and ongoing system and commodity support.

Actual delivery of the final product may also take considerable time. If the project involves program development for computerizing the voter registration process, for example, it could take six months to a year to develop and pilot test the software, accomplish the complete conversion of existing records, and test and debug the system. When the new technologies adopted involve the purchase of equipment such as DREs, it should ideally be certified by an independent agency. Such certifications are also time-consuming. Depending on the number of units required, it could also take considerable time for the vendor to produce, customize and deliver the equipment. Time should also be put aside for acceptance testing, which is usually undertaken when equipment is first delivered to verify that it functions as promised and that it has been configured according to specifications. This exercise should never be based on a random sampling; each and every piece of equipment should be tested individually.

D. Establishing Deadlines for Implementation

Key to any plan's success is establishing a time table that provides a firm deadline by which preparations, testing, debugging and installation must be accomplished prior to the election in which it is to be utilized for the first time. In its first use of DRE machines, Miami-Dade County made a crucial error in judgment by deciding to introduce a change to their configuration right before election day. While it might have been well intended, the addition of another language to the system at the last minute left little time for recovery when errors were encountered that jeopardized the performance of the DREs in the days immediately prior to election day. As a result, some units had to be pulled from service.

E. Preparing the Public and Training Election Workers

The introduction of new technologies requires that time be invested in preparing the public. The development of public information campaigns is critical to gaining the public's acceptance of and confidence in the new systems. In addition, sufficient time must be allotted to train permanent staff as well as temporary election workers and polling board members.

When Miami-Dade County in Florida introduced its electronic voting systems for the first time during the 2002 Primary Election, the county encountered as many problems as they had when they were using punch cards in the controversial 2000 Presidential Election. Polling stations opened late, voting machines didn't work, and voters were once again frustrated at the polls. The transition to DREs did not solve those residual problems. Ultimately, a determination was made that many of the serious election problems were not due to the failure of the equipment alone, but were due to the inexperience and inadequate training of the poll workers, inadequate training materials provided by the EMB and/or the vendor, the lack of technical support, and errors in judgment. It was only in preparation for the 2002 General Election that improvements were realized. The turn around was achieved when extraordinary measures were taken to involve the police department in strategic planning, communications and logistics. Professional specialists from several other county government departments were called in to supervise the development and conduct of poll worker training and the public outreach campaign. IT specialists from virtually every government department were assigned to be on hand at polling stations, and other technicians were hired to be on call to respond to requests from poll workers for technical support throughout the period of in-person advance voting and on election day.

In contrast, Hillsborough County went to great lengths during the first roll-out of its new electronic voting machines to prepare the public and the poll workers before the election. Their planning calendar allotted time for the scheduling of a mock election about three months before the actual

election in which the DREs were to be used for the first time. Every polling station was opened and through a widely publicized ad campaign voters were encouraged to participate. Forty thousand voters turned up at the polls for the mock election. Not only was it a great way to get the voters involved, it gave poll workers the opportunity to test their skills and build their confidence in the set up, use and close out of the new machines. These exercises greatly contributed to the smooth operation of the polls and to voter satisfaction on election day.

While it may not be possible for other jurisdictions to budget for such a sweeping exercise, it should be possible to dedicate a certain number of units for voter outreach purposes. They can be made available in public places so that people can see them and get a chance to try them. They can also be demonstrated at public gatherings such as meetings of civic organizations, culture centers serving specific national and ethnic minorities, and schools where polling stations are commonly located. A timely media campaign can advise the public as to where they will be on display on different days in the pre-election period.

F. Establishing the Legal Framework

Another major issue that is often overlooked is the time it takes for legislative bodies to introduce and pass appropriate legislation. Depending on the deadlines by which proposed legislation must be introduced, and taking into consideration the length of each legislative session, gaining consensus prior to the passage of appropriate laws could take months. Work on the election automation bill in the Philippines took over a year to finalize. Should there be an election scheduled in the interim in which a new parliamentary body is elected, the entire process most likely will have to begin anew.

As the experts in administering the existing process, election officials are well positioned to provide technical assistance to legislators, their aides and legislative drafters in defining what new provisions should cover and in identifying those provisions that need to be repealed altogether or amended. A thorough review of proposed legislation is only part of the process. Just as importantly, it is critical that the existing election law as well as any other companion laws be reviewed to determine where conforming amendments are also needed. The introduction of automated systems often requires significant changes to the procedural details, whether they are articulated in law or defined in administrative regulations or guidelines adopted by the EMB. In many jurisdictions, the adoption of administrative regulations involves adherence to a legal calendar that involves various levels of administrative, legal and legislative review, official notice and a public comment period.

Depending on the standard methodologies by which new legislation is introduced in the lawmaking body, however, election administrators may have greater or lesser opportunities to directly influence its formulation. The optimal scenario is when election officials and legislators can develop a positive and constructive partnership in developing a legislative framework for the introduction and implementation of new technologies in the electoral process. In some contexts, protocol limits election officials' direct access or communications with lawmakers. Nonetheless, it is critical that election officials stay on top of every bill that is introduced and are prompt in providing their assessments of each version. The job does not just involve supporting positive developments, but also stopping legislation that jeopardizes the orderly conduct of the process or that introduces requirements that cannot be administered. Often, in an attempt to solve a legitimate problem, lawmakers propose unrealistic legal remedies because they simply are not aware of how processes actually work. What sounds like a good idea on paper may actually scuttle the process in practice.

An example can be drawn from the Philippines experience. Lawmakers explored ways to increase transparency related to the reporting of polling station results in order to overcome suspicions that final results were not the same as those originally reported by poll workers. One of the proposed bills included requirements that each polling board digitally photograph the protocol as soon as it was completed and upload it onto the Internet from the polling station, so that anyone could compare the image with the polling station's reported final results. First, it is very unlikely that such capacity would be available at most polling stations. In addition to the extra equipment costs and the additional burden it would place on poll workers, such a plan would be doomed to failure

with one quarter of a million polling sites trying to upload their images at the same time. Over the course of the revision process, this provision was eventually deleted.

Another challenge for lawmakers and EMBs alike is finding the right balance between the articulation of general guidelines and explicit administrative details in the law. Ideally, the law will provide clear language regarding mandatory requirements and standards, while also delegating sufficient regulatory authority to the EMB to enable it to clarify procedural details.

VIII. Common Failures in Designing Specifications

In order to get thorough and responsible proposals from vendors, it is important that the specifications be as detailed as possible. Too often deficiencies in the responsiveness of vendors, contractual disagreements, cost overruns and unsatisfactory relationships are the direct results of errors and omissions in the specifications and language of the requests for proposals themselves.

The most common deficiencies relate to omissions regarding the full disclosure of legal and functional requirements, the use of vague or unclear language and lack of specificity regarding the client's expectations. In seeking proposals for development of a computerized voter registration program, for example, every effort should be made to ensure the language is clear, not only about the compilation and maintenance of the registration database but also about any sub-systems the database is to support. Such sub-systems might include applications related to early voting and absentee voting programs. Or, in those jurisdictions that provide provisional voting opportunities, they might include the post-polling day verification of provisional ballots. In another example, specifications for electronic or optical scan voting and counting units should include specific details about the number of jurisdictions, precincts and split-precincts involved, the number of races they need to accommodate, and the number of ballot styles or combinations that will be involved. Likewise, language options and requirements related to the use of the machines by people with disabilities should be covered, as should specifications as to the manner in which results are to be reported or transmitted. Every detail that is omitted creates an opportunity for dissatisfaction for both parties.

EMBs should also ensure that the specifications include terms and conditions related to vendor failure in timely delivery or product quality. Of key importance to the EMB is specificity in the terms related to warranties, ongoing maintenance and technical support.

IX. Understanding Long-Term Institutional Implications

Modernization or the introduction of computerized data systems, electronic voting equipment, electronic transmission of results or other technologies should never be thought of as a single event or a one-time purchase. Once on that path, it is like a marriage for which there is no annulment. Sometimes lawmakers and EMBs are blindsided by the long-term implications that they had not anticipated.

- Modernization has a significant effect on the costs of elections due to both initial and residual costs and on investment value relative to the potential obsolescence of systems and equipment over time. The "new best thing" is always on the horizon.
- Modernization and high-tech options often challenge the capacities of some localities' infrastructures and bring additional burdens to local officials. The need for new, more suitable office space frequently emerges. Logistics planning requires additional attention to issues like transport, storage, maintenance and contingency, communications and emergency strategies. Warehousing and transport issues are likely to arise relative to new voting equipment and its safekeeping between elections.
- Skill sets required of election officials may have to change. Likewise, this may be a significant issue with respect to the recruitment and training of poll workers if part of the modernization effort calls for the introduction of electronic voting equipment or electronic poll books. Training and education of officials, political participants, and the media as well

as outreach to voters will require extra time and resources to prepare them to use the new technologies.

- The design and institution of back-up systems and the implementation of contingency plans in the event of system failure will have to become a regular part of the election preparation regimen. If DRE voting equipment is used, for example, part of a contingency plan might include arrangements for a team of support technicians to be on call or procedures for the transfer of equipment from one site to another if there is a malfunction. If voting is interrupted because of power failure, provisions might call for a formally authorized extension of polling hours. If electronic voter registers are introduced for use at the polling stations, it might be advisable to also provide paper copies of the voter lists, or to provide for the creation of supplemental lists to which voters can be added so that voting doesn't have to stop if there is a power failure. EMBs have to become experts at anticipating what could go wrong and being ready to respond when it does.
- Depending on the technology selected, transparency, auditability and data security issues are likely to raise new challenges that will have to be fully addressed to maintain public and political confidence in the integrity of the system. Ongoing maintenance—including functionality, logic and accuracy testing on voting equipment between, prior to and after elections—is a critical requirement. The institution of appropriate security measures and controls against unauthorized intrusion or manipulation remains a constant concern. The use of advanced technologies also brings with it concerns for the protection of individual privacy.
- Regardless of the system selected, EMBs must be ready to make every effort to ensure its integrity and to alleviate, to the maximum degree possible, opportunities for unauthorized access, intrusion, manipulation, vandalism or loss. These issues are often at the heart of the criticisms lodged against new technologies and litigation filed in the aftermath of an election. Sometimes the only defense available to the EMB is its ability to demonstrate that all due diligence has been exercised, including administrative, physical and technical security.

  Administrative security routines might include, for example, conduct of comprehensive security risk assessments, security awareness and training for all staff, security incident handling, security monitoring and audit controls, and access management. Documented physical security might include such measures as physical access controls, inventory documentation, secured storage and chain of custody documentation during transport, and routine maintenance. Technical security is perhaps the most challenging. Measures for maintaining technical security should be addressed in two ways: through "preventive" controls in terms of preventing unauthorized intrusion or manipulation in the first place; and, through "detective" controls that ensure that an intrusion or manipulation can be detected should it occur. Preventive controls are designed to be preemptive. Detective controls are designed to neutralize an occurrence and to contain the damage. Of utmost importance will be systematic and consistent implementation of technological and procedural routines that protect the hardware, firmware and software components of the system from unauthorized or undocumented change or modification. Every "patch," alteration or upgrade should be formally documented. The main concern for EMBs is determining how best to "prove" that systems are secure and that they are functioning accurately.

X. In a Nutshell

When they are thoughtfully chosen, well-designed and competently implemented, the positive benefits of new technologies can far outweigh the downsides. The serious challenges surrounding the introduction of registration technologies and electronic voting systems should not lead to a reflexive decision to "junk" automation, but rather to ensure that automation is used mindfully. Ultimately, the basic questions that any EMB considering new technologies should focus on are the following:

- Will modernization offer a significant improvement over the system that currently exists?

- What types of new technologies being considered make the most sense in terms of cost, capacity, and infrastructure?
- Is there sufficient political will to see the process through with realistic expectations, adequate funding and enduring institutional support?
- Can sufficient protections be put in place to ensure against system failure or, in such an event, can an adequate and reliable recovery plan can be fully implemented?
- Can sufficient safeguards can be designed and maintained with due diligence to protect the new system from unauthorized intrusion or manipulation that would jeopardize its integrity and public confidence in the results?
- Can the new automated systems put in place be sustained over time?
- Will the new technologies serve the public interest in keeping with the fundamental principles of democracy?

Administration of elections has always been a complex business. EMBs need only to remember that modernization never alters the fundamental principles they've always upheld in delivering a free, fair and transparent election process; rather it only alters the manner in which those principles are achieved. As long as vision is tempered with practicality and the important details don't get lost in the big picture, the successful introduction of new technologies is not only achievable, but it can also be an exciting and rewarding journey.

Perspectives on Electronic Voting

Douglas W. Jones[*]

I. Introduction

Election managers must consider a number of factors when considering a move to electronic voting technologies. The legislative bodies that oversee the election managers should be aware of these considerations as they craft the laws guiding the shift to new technology. Partisan and independent election observers also need to be aware of these considerations as they observe both the crafting of election laws and the reduction of those laws to practice.

Our focus here is on technologies that stand between the voter and the results of the election. This includes machinery that directly or indirectly attempts to interpret voter intent. Examples of such technologies include:

- Mechanical voting machines, as first developed over century ago.
- Direct recording electronic voting machines, as deployed in some countries since the 1970s.
- Punch-card vote tabulators, such as the Votomatic that was the center of controversy in Florida after the 2000 general election in the United States.
- Optical mark-sense ballot tabulators that scan and tabulate votes from paper ballots marked by the voter.

This section will address two questions that jurisdictions must answer when considering election automation:

- Why pursue voting technologies?
- How to manage the acquisition, evaluation and use of voting technologies?

The very first issue a jurisdiction faces as it moves toward election automation is the fundamental question: why do this? This question needs to be answered before any decisions about election technology are made.

The next issue that must be faced is how to manage the acquisition, evaluation and use of new voting technology. Each technology poses its own problems, but all technologies, from the simplest to the most complex, pose many of the same (or at least similar) problems. These problems can be looked at from a number of viewpoints. Each of these viewpoints brings out different aspects of the problem. Among the most valuable viewpoints are those centering on the election equipment life cycle, the election cycle, the flow of data through the election system, and the chain of custody that carries a vote from voter to the final canvass of the election.

There are many other issues involved in adopting voting technology, including choosing machines, dealing with vendors, working with donor and or legislative expectations, and maintaining public confidence in the election process. However, in this section, the focus is on the decisions of why to adopt voting technology, and how to bring that technology into operation. As a result, this paper discusses election technology without focusing on the specifics of any one technology. Thus, questions about the distinctions between, for example, optical mark-sense voting systems and direct recording electronic voting systems are not at issue.

[*]This material is based, in part, upon work supported by the National Science Foundation under Grant No. CNS-052431 (ACCURATE). Any opinions expressed here are those of the author and are not endorsed by the National Science Foundation or by the University of Iowa.

II. Why Automate Voting

Votes have been counted for thousands of years without the aid of technology. Ancient Greek democracy, Roman democracy and Swiss democracy did not rest on any technology more complex than shows of hands, stone and metal ballots, or pen and paper. These simple techniques serve to this day in many contexts, so it is useful to ask what drives election authorities to adopt more complex technologies.

Looking through the history of voting technology, there are at least five distinct reasons that, singly or in combination, have driven electoral authorities to adopt complex election technologies:

- To centralize control over the conduct of elections.
- To deal with the complexity of voting rules.
- To increase access to the polls.
- To reduce costs.
- To satisfy a desire for modernization.

The final reasons above are questionable. Whether it is political leaders or the international community, the hope to save money and the desire to show that the election authorities are thoroughly modern tend to lead to decisions that are less likely to be informed by technical and practical realities.

A. Centralized Control

In general, complex technological mechanisms require significant expertise to manipulate. Around the world, election authorities have used this fact to take control of elections away from local election workers and centralize it in the hands of authorities, or rather, the technical staff of the authorities. Election technology can offer significant benefits in jurisdictions where there is widespread fraud at the polling places, for example, where local election workers have routinely engaged in ballot-box stuffing or forgery of election results. On the other hand, centralization creates a risk of centralized fraud if the authorities or their technical staff are less than honest.

There are estimates that close to 30 percent of the ballots cast in some jurisdictions in the United States were fraudulent in the 1880s.[1] Many early developers of voting machines in the United States saw their machines as a defense against such fraud,[2] and reform advocates frequently saw the adoption of mechanical voting machines as an effective defense against fraud.[3]

One can easily infer a similar motivation for the adoption of computerized voting systems in Kazakhstan. Observers in the 2005 presidential election in that country reported widespread problems. While electronic voting would not have prevented reported abuses such as family or group voting, it would have prevented the incidents of ballot box stuffing or the numerous incidents of irregular ballot counting. In polling places where electronic voting was used, the opportunity for some of these abuses was eliminated.[4]

However, it is unfortunately easy for election administrators to overestimate the security they gain by using advanced technology to conduct elections. In 2006, the United States had about 500,000 computer programmers, 800,000 software engineers, and 500,000 computer systems analysts,

[1]Worth Robert Miller, "Harrison County Methods: Election Fraud in Late Nineteenth Century Texas," *Locus: Regional and Local History,* 7:2 (Spring 1995): 111-28. Available at http://clio.missouristate.edu/wrmiller/Populism/texts/harrison_county_methods.htm.
[2]Douglas Jones, "Technologists as Political Reformers: Lessons from the Early History of Voting Machines," presented at the Society for the History of Technology Annual Meeting, Las Vegas, October 13, 2006. http://www.cs.uiowa.edu/~jones/voting/SHOTpaper.pdf
[3]Joseph Harris, *Election Administration in the United States* (Brookings Institution, 1934). See particularly page 60. Available at http://vote.nist.gov/election_admin.htm.
[4]*Final report on the presidential election in Kazakhstan, 4 December 2005*, Organization for Security and Cooperation in Europe, Office for Democratic Institutions and Human Rights, February 21, 2006. See section XIV. Available at http://www.osce.org/item/18133.html.

i.e., a total of around 1.8 million people with significant knowledge of computer programming.[5] The United States has no monopoly on such knowledge, so it is reasonable to double this number to account for professional programmers elsewhere in the world, and to double it again to account for people who can program but do not do so as their primary job. In sum, we can safely guess that there are over seven million people in the world who have the skills needed to carry out technologically sophisticated attacks on computerized systems. Furthermore, some electronic voting machines appear to be vulnerable to surprisingly low-tech manipulation. For example, there are allegations from the spring 2006 municipal elections in the Netherlands that one polling place election official manipulated the controls on an electronic voting machine to fool elderly voters into thinking that they had voted when in fact, they had not.[6]

Centralized control, of course, poses significant risks. Centralization that takes control from corrupt local election officials and puts it in the hands of honest central authorities is good, but the central authorities are not always honest. The history of vote fraud in the United States is dominated by stories of corrupt political machines that controlled counties or occasionally entire states.[7] Decentralization is frequently a strong weapon for dealing with corrupt authority.

B. Complex Voting Rules

When ballots are simple, with a single race on each ballot and only a few candidates in the race, hand counting paper ballots can be fast and accurate. An example of a recommended practice is to divide the ballots into stacks, one stack for each candidate plus one stack for blank or ambiguous ballots. This should be done without access to any pens or pencils in the presence of observers. At least two people representing opposing parties should examine and agree on the interpretation of each ballot, and disputed ballots should be displayed to all interested observers to demonstrate that they indeed contain no legal vote. Once this is done, the count can be completed by simply counting all of the ballots in each stack.

Such relatively simple counting rules do not work where there are many different races on one ballot, as in a typical general election in the United States. Or where there are hundreds of candidates in a single race, as in a parliamentary election in the Netherlands. The more complex the counting rules, the more likely people are to make errors in carrying them out.

Machines, whether mechanical or electronic, do not make clerical errors. They do, however, make other types of errors, and the people who administer machines make clerical errors. Yet as election rules grow more complex, the sheer volume of work involved in counting the ballots can make technology desirable despite these problems.

C. Increased Access to the Polls

Conventional elections require that all voters present themselves at a polling place during a limited time period. Many potential voters may not be able to travel to a polling place during the designated interval. Postal voting, voting by fax machine and Internet voting all offer the opportunity for increased access to the polls. However, each of these poses significant security problems! How can the election authority determine that a ballot received by post, by fax or over the Internet came from a legitimate voter? Numerous technologies have been proposed to accomplish this, some of which do not solve the problem at all (forgery of a photocopy of an ID document is far easier than forgery of the document itself). Other solutions compromise a voter's

---

[5]Occupational Outlook Handbook, United States Bureau of Labor Statistics, 2006-07 Edition. Available at http://www.bls.gov/oco/

[6]Onderzoek naar stemfraude in Zeeland (Investigation of vote fraud in Zeeland), *Brabants Dagblad*, March 21, 2006. Available at http://www.brabantsdagblad.nl/brabant/article188558.ece.
NFI: niet geknoeid met stemmachine Landerd (Netherlands Forensic Institute: no tampering with Landerd voting machine), *Brabants Dagblad*, August 23, 2006. Available at http://www.brabantsdagblad.nl/regios/udenveghel/article594020.ece.
Strafklacht stemfraude in Landerd (Indictment for vote fraud in Landerd), Brabants Dagblad, August 31, 2006. Available at http://www.brabantsdagblad.nl/gemeenteraadsverkiezingen/article613419.ece.

[7]Andrew Gumbel, *Steal This Vote* (Nation Books, 2005).

right to a secret ballot. This is currently a very active area of research.

The problem of reaching a polling place during the voting period is most severe for expatriate voters. The problems of expatriate voters, particularly those in areas with poor postal service, deserve particularly close attention. Many jurisdictions have explored Internet voting to serve the needs of these voters.[8] [9] [10] In many of these cases, it takes one or more postal transactions to obtain the right to cast an Internet ballot. It is reasonable to ask whether it might be more secure to use the Internet to deliver a postal ballot instead of using a postal transaction to deliver authorization to cast an Internet ballot.

In addition, voting on conventional paper ballots at the polling place requires that voters be able to handle a pen or pencil and that they be able to read the ballot. Blind voters, illiterate voters and physically disabled voters are at a clear disadvantage in such a context. There are very low-technology approaches to ballot access for the disabled and illiterate, most notably the tactile ballot.[11] Despite this, today most attention is focused on use of electronic voting machines for this purpose. A new class of devices, known generically as accessible ballot marking devices, is only beginning to emerge.[12] [13] The latter are, without doubt, as technologically complex as electronic voting machines, but instead of recording or tabulating votes, they merely assist the voter in marking a ballot.

D. The Cost of Elections

Elections are expensive. Among the costs to consider are the following items and processes:

- Salaries for polling place election officials, polling place technicians, polling place security officers, security officers at the storage facilities, and technicians required to maintain, test and set up voting equipment (among others).
- Training polling place election officials and polling place technicians.
- Special transportation for voting equipment.
- Printing paper ballots.
- Secure facilities to store paper ballots and voting equipment.
- Climate-controlled storage for electronic voting equipment.

In the United States, it is quite common to find that the total number of election officials exceeds 1 percent of the turnout in a general election. In addition, many election jurisdictions assign law-enforcement officers to protect ballots, technicians to provide support at polling places, truck-drivers to transport ballots, and many other temporary job assignments, so that the total number of people needed to carry out an election approaches 2 percent of the turnout. Every one of these workers must be paid, if not directly, then indirectly through the costs of their lost labor elsewhere in the economy.

Where paper ballots are used, the usual rules call for the number of ballots printed to exceed the expected turnout by a significant safety margin. It seems a pity to print ballots knowing that many of them are destined to be discarded unused. After the election, the law generally requires the

[8]Robert Hensler, "The Geneva Internet voting system, République et Canton de Genève Chancellerie d'Etat" (January 15, 2003). Available at http://www.geneve.ch/chancellerie/E-Government/doc/pre_projet_eVoting_eng.pdf.
[9]David Jefferson, Aviel D. Rubin, Barbara Simons, and David Wagner, "Analyzing Internet voting security," *Communications of the ACM* 47:10 (2004), 59-64. Available at http://portal.acm.org/citation.cfm?id=1022594.1022624.
[10]Organization for Security and Cooperation in Europe, Office for Democratic Institutions and Human Rights (OSCE/ODIHR), *Final Report on the 22 November 2006 Parliamentary Elections in the Netherlands* (March 12, 2007). See section IV.C. Available at http://www.osce.org/item/23602.html.
[11]American Council of the Blind, *Independent, Secret and Verifiable: A Guide to Making Voting an Independent and Accessible Process for People Who Are Blind and Visually Impaired* (2002). Available at http://www.acb.org/resources/votingbook1.html.
[12]The Automark ballot marking device is made by Automark Technical Systems (www.automarkts.com).
[13]Douglas Jones, *System for handicapped access to voting ballots*, U. S. Patent 7134597. Available at http://www.freepatentsonline.com/7134597.html.

storage of all ballots and other records of the election for some time. Paper records are bulky and expensive to store, and in warm moist climates, they may deteriorate quite rapidly.

For more than a century, advocates of election technology have hoped that mechanical and later electronic voting systems would reduce these costs. With respect to personnel costs, fast mechanical or electronic counting can indeed greatly reduce the amount of labor hours required after the polls close. With respect to printing and storage costs, paperless mechanical or electronic voting systems do eliminate the need for printing excess ballots before the election and storing voted ballots afterwards. Unfortunately, starting with the analysis done by Joseph Harris in the early 1930s, it has been clear that these savings can be elusive.[14]

The fundamental problem is that voting technology has costs that are quite different from the costs of low-tech elections conducted with simple paper ballots. Voting machinery must be stored securely between elections, generally in climate-controlled storage. Furthermore, voting machines require skilled technicians for maintenance and trained election workers for operation.

Some voting technologies are indeed inexpensive. The Votomatic and its descendants use mechanical ballot marking templates (the Votomatic machine), inexpensive ballot boxes, and only a single central computer system for ballot tabulation. In contrast, it may be necessary to purchase and store one direct recording electronic voting machine per 50 voters for a general election in the United States, or one per 1,000 voters for a Dutch parliamentary election. The difference in the number of voters a voting machines can handle is largely a function of how long it takes an average voter to work through the ballot, and this, in turn, depends on the complexity of the ballot.

E. The Appearance of Modernity

The electronic voting machines of the late 20th century and the mechanical voting machines of the late 19th century were all close to the limits of what was technologically possible at the time of their introduction. Some people clearly feel that the need to be modern is sufficient justification for using a technology. A typical advertisement for an election technology product promises that it "delivers the promise of the future of voting today!"[15] or "Internet voter registration and voting could be the most compelling issue facing e-government today and could also reinvigorate democracy like nothing before."[16]

However, modernity for its own sake is nothing more than a matter of fashion. Being modern may excite some voters, but the hope that it will reinvigorate democracy is, at best, speculation. As such, arguments for voting technology based on this kind of rhetoric should be discounted. When such arguments dominate the drive toward electronic voting, hard questions need to be asked.

III. Four Views of Voting Technology Management

As mentioned above, four views of the election process will be discussed, and steps related to the use of voting technology will be illustrated through each view.

A. The Voting System Life Cycle View

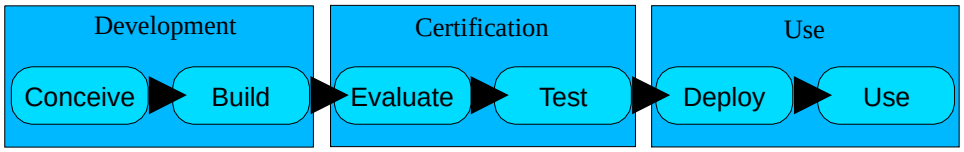
Typically, it takes several years for a voting system to move from conception to use. The cycle may be accelerated for incremental changes to an already deployed system, but even then, it is rare to upgrade a system in less than six months. More rapid system deployment can only be done at the risk of shoddy development, incomplete testing and inadequate training.

---

[14] Harris, p. 61.
[15] Quoted from Toolsmith Consulting, Liberty Election Suite, available at http://www.tool-smith.com/ToolsmithWeb/?t=products/liberty.
[16] Robert S. Done, *Internet Voting: Bringing Elections to the Desktop* (The PricewaterhouseCoopers Endowment for The Business of Government, February 2002). Available at http://www.businessofgovernment.org/pdfs/Done_Report.pdf.

The life cycle of a voting system, from its initial conception to its eventual abandonment, involves three major stages that can be subdivided into several minor stages. These stages bear strong similarities to the stages in the life cycle of safety critical systems such as avionics software or medical devices. The process begins with system development, followed by certification or qualification. Once systems are certified, they may be deployed and used.

Figure 1: The voting system life cycle



Voting system development begins with the conception of the new system. In the case of entirely new systems, this is frequently done by either an election official or an independent inventor. Where the system is an incremental upgrade of an existing system, the conception usually rests on observations of some inadequacy in the existing system.

Once conceived, the voting system must be built. This generally involves considerable labor, so someone must provide the capital needed to fund this work. Some voting systems have been developed at government expense, for example, the Sailau system in Kazakhstan or the SERVE system in the United States.[17] [18] Other systems have been developed with private funds, as with most voting systems sold in the United States. In some developing democracies, donor funds have been used to develop voting systems; in such cases, there is a real risk of disconnect between the actual needs of the developing democracy and the expectations of the donor.

Regardless of who funded the development of the voting system, it is essential that the system be subject to evaluation to ensure that the system, as developed, meets the requirements that have been set for it. A very common model has emerged around the world for such evaluation. Governments designate independent testing authorities (ITAs) to which voting systems are submitted for evaluation. The ITAs then evaluate the voting systems against voting system standards set by the government. This model is old, originating with independent steam engine and boiler testing agencies in the 19th century. Since then, it has spread to many other domains. In 1990, the United States adopted this model for testing voting systems.[19] Kazakhstan and the Netherlands use much the same model.[20] [21]

The need for the testing authority to be independent of the voting system developer or vendor is fairly obvious. It is equally important that the testing authority be independent of the government. When a government has spent large sums on a voting system or has committed itself to installing that system by a particular date, it is very natural for the government to attempt to pressure the testing authority to approve that system regardless of its actual adequacy. This kind of pressure threatens the integrity of the entire approval process.

Typically, the independent testing authority has two distinct functions, design review and testing. Design review involves a study of the design of the voting system, determining whether the system, as designed, meets the requirements set by the voting system standards. Such review applies equally to hardware mechanisms and software. Testing compares the system, as built,

[17]OSCE/ODIHR, *Final report on the presidential election in Kazakhstan, 4 December 2005* (February 21, 2006). See page 9. Available at http://www.osce.org/documents/odihr/2006/02/18133_en.pdf.
[18]Jefferson et al., 59-64.
[19]United States Federal Election Commission, *Performance and Test Standards for Punchcard, Marksense, and Direct Recording Electronic Voting Systems* (January 1990). Available at http://josephhall.org/fec_vss_1990_pdf/
[20]OSCE/ODIHR, *Final report on the presidential election in Kazakhstan*. See section VI.
[21]OSCE/ODIHR, *Final Report on the 22 November 2006 Parliamentary Elections in the Netherlands* (March 12, 2007). See section B. Available at http://www.osce.org/documents/odihr/2007/03/23602_en.pdf.

with both the design and the standards. Black-box testing focuses on functionality, focusing on user manuals and the external behavior of the system. White-box or glass-box testing examines the internal mechanisms of the machinery. Red-team testing involves deliberate attacks on the system in order to evaluate its response to improper or malicious use.[22]

The biggest problem faced by independent testing authorities is that they can only test to the standards that the government has set. If these standards are inadequate, the tests will be inadequate. Some standards are easy to test. For example, voting machines used in the Netherlands require that the buttons used to select candidates be no smaller than 10 millimeters and function when depressed from 0 to no more than 6 millimeters with a force of no more than 4 newtons. Additionally, they must operate on 187 to 242 volts at 49 to 51 hertz.[23] Other standards can be quite difficult to test. For example, voting machines used in the Netherlands must present information that is relevant, clear and clearly perceptible, and they must prevent or limit accidental or incorrect use, so far as is reasonable and technically possible.[24] Such problems are not confined to the Netherlands. Similar complaints have long been made about the voting system standards in the United States.[25]

Once a voting system has been approved as adequate, deployment may begin. At this point, training materials are finalized and training programs begin for election administrators. While preliminary training may have begun during the certification process, certification may require significant changes, and allowances must be made for these in the preparation of training materials. The highest training priority is for election administrators and the technical staff at election equipment warehouses.

Training typically involves using examples of the new voting system, but only a few such examples are needed initially. Large-scale manufacturing of the approved system can typically begin during training, because no large-scale deliveries should be made until trained staff are prepared to accept delivery.

On receipt of voting equipment, it is necessary to conduct an acceptance test to see that the machines, as delivered, are functional and match the designs that were approved. As with any purchase, acceptance testing must be conducted by the customer. A responsible vendor will, of course, conduct quality control tests in order to avoid liability for delivering broken or incorrect equipment, but if the customer does not test, there is no way to know if the vendor is being responsible.

Acceptance testing is as important for low-tech voting devices as it is for computerized election machinery. For example, prior to the 2000 general election in Cook County, Illinois, the ballot tabulating machines were tested, but not the mechanically trivial Votomatic vote recording devices. Unfortunately, as post-election analysis would show, these were defective, with holes that were slightly out of alignment. This error probably disenfranchised about three percent of the voters.[26]

Once the new voting system has passed its acceptance tests, it may be employed for one or more election cycles. During these cycles, deficiencies in the voting system will probably come to light, for example, due to inadequate design or improper use. At some point, these inadequacies will invariably lead to the decision to change the voting system, either by replacing it with an entirely new system or by modifying the design of the current system. Either of these cases involves the initiation of a new voting system life cycle, from development to deployment.

---

[22]Brennan Center Task Force on Voting Security (Lawrence D. Norden, Chair), *The Machinery of Democracy: Protecting Elections in an Electronic World* (Acadamy Chicago Publishers, 2007). See Appendix E, Voting Machine Testing.

[23]Netherlands Ministry of the Interior, "Annex: Specifications for voting machines," in *Voting Machines (Conditions and Approval) Regulations* (1997). See items 9.4 and 12.1.

[24]Ibid. See items 2.1 and 8.6.

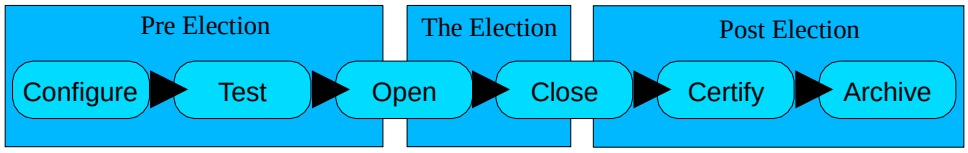
[25]Earl Barr, Matt Bishop, and Mark Gondree, "Viewpoint: Fixing federal e-voting standards," *Communications of the ACM* 50:3 (2007), 19-24. Available at http://portal.acm.org/citation.cfm?id=1226736.1226754.

[26]Michael Hites and Bill Ornt, *Testing of Vote Recorders* (Department of Mechanical, Materials and Aerospace Engineering, Department of Mechanical, Materials and Aerospace Engineering, August 24, 2001).

B. The Election Cycle View

Election cycles are seen quite differently by the public and by election officials, and this difference becomes far more complex when elections are carried out using complex technology. The public sees a political campaign that culminates in an election, followed by a brief flurry of activity as the votes are counted and unofficial results are announced in the press. The election official sees a vastly different cycle that begins with pre-election activities, centers on election day itself, and is then finished with post-election activities that must be completed before the next election cycle begins.

Figure 2: The election cycle.



Pre-election activities include voter and candidate registration, but from the point of view of election technology, the story begins as soon as the lists of candidates and referenda that are to appear on the ballot are finalized. At this point, the process of ballot design begins. This process is remarkably similar whether the ballots are to be printed on paper or presented on an electronic voting system. The complexity of the ballot design problem depends very much on the jurisdiction. Ballots for general elections in the United States or parliamentary elections in Holland may involve hundreds of candidates and may differ significantly from one election district to another.

Where ballots are counted by machine, the machines must be configured to count the ballots. Whether on mechanical voting machines or electronic systems, this involves setting the interlocks on the different voting positions to enforce the rules of each race on the ballot. For example, in the race for president, voters may vote for only one candidate, while in the race for county commission, they may be entitled to vote for five out of the ten candidates, and in the race for city council, they may be allowed to cast a ranked-preference ballot, indicating first, second and third choices.

Ballot layout and voting system configuration are both subject to error, and machines that worked in the previous election may no longer be functional by the time they are used in the next election. Testing provides our primary defense against such problems. There are several types of testing:

- Acceptance testing (discussed above).
- Pre-election testing prior to delivery to the polling places.
- Pre-election testing at the polling places.
- Parallel testing during the election.
- Post-election testing.

Pre-election testing: With paper ballots, pre-election testing may involve little more than careful proofreading of the ballots. With voting machinery, the test should also involve casting test ballots, tabulating them, combining the results from multiple precincts, and verifying that the aggregate result of the test matches the expected result. Such a test involves the entire process of vote tabulation from the voting machinery used by voters to the computers used by the central election authorities.

Pre-election testing may also involve exhaustive testing—that is, complete testing of all system behavior. This is appropriate, but difficult to complete for machinery in election headquarters, including both central computer software and central ballot-tabulating machines. Exhaustive testing is practically impossible for machinery used in polling places. A reasonable scheme involves intensive testing of a random sample of the machines prior to their delivery to the polling

places, with care taken to ensure that every ballot style is tested.[27]

Testing may be conducted by elections office staff, or the public may be involved. In the extreme, pre-election testing becomes indistinguishable from pre-election voter outreach, as in Kazakhstan's 2005 presidential elections, where the public were invited to visit polling places and cast test ballots in the period prior to the election.[28] This was an effective public education measure, and it provided polling-place election officials with useful practice, but such a testing model must be considered an adjunct to, and not a substitute for, carefully designed tests.

As the official election begins, and immediately prior to opening the polls, the polling place election workers have one last chance to perform simple pre-election tests. These must be brief and simple, but they provide important protection to the election process. Failure to do such testing has led to embarrassing problems, as was the case in 2000 in Palm Beach County, Florida, when perfunctory tests were performed without anyone examining the results until a year later. As a result, voters in that election were allowed to vote on a significant number of defective Votomatic voting machines.[29]

During the election itself, the primary challenge posed by technology involves failure. Voting machinery is no different from other machinery, and thus sometimes fails. Provisions for dealing with failure can range from posting technicians at every polling place, as was done in Miami in 2004 and in Kazakhstan in 2005, to equipping every polling place with emergency paper ballots to be used in the event the machinery fails.[30]

Parallel testing: Some jurisdictions do parallel testing, that is, they select random voting machinery from among the machinery deployed to the polling places for testing during the election day. This obviously requires that there be sufficient equipment that taking random equipment for testing will not prevent proper conduct of the election. If properly conducted, parallel testing offers the possibility of detecting widespread rigging of election machinery, for example, by insertion of malicious software or improper ballot configuration files.

To achieve maximum effect, machines should be selected for parallel testing at the last possible moment and the test should be conducted in such a way that the machine cannot reasonably infer from the pattern of test votes that it is a test. Thus, test votes should be cast at realistic times of day, the number of test votes should be typical of the number expected at the polls, and the number of votes for each candidate should be typical. For polling places routinely equipped with multiple voting machines, the most extreme parallel testing model requires that the voting system testers arrive at random polling places just before the polls are opened. The testers then randomly select machines for testing after the machines are turned on and enabled for voting, but before any voters have cast ballots.

Post-election testing: Some jurisdictions require post-election testing. This is typically done with central tabulating equipment in order to verify that, after the official tabulation has been completed, the machinery is still functioning correctly. Post-election testing of direct-recording and precinct-based tabulators is extremely rare, except in cases of contested elections or suspected fraud. For example, extensive post-election tests (mistakenly called parallel tests) were performed after the contested 2006 election in Florida's 13th congressional district.[31]

---

[27]Miami-Dade County Elections Department, *Logic and Accuracy Test, August 32, 2004 Primary Election* (August 13, 2004). Available at http://www.cs.uiowa.edu/~jones/voting/miamihandout.pdf.

[28]"Election officials put final touches on ahead of vote," *Kazakhstan News Bulletin* (November 29, 2005). Available at http://www.kazakhembus.com/112905.html.

[29]Joel Engelhardt and Scott McCabe, "Poll workers ignored flaws in pre-vote machine tests," *Palm Beach Post* (December 9, 2001).

[30]"Temporary use of printed ballots in voting machine precincts," Iowa Administrative Code 721-22.431(52). See also "Counting emergency paper ballots," 721-26.61(49). Available at http://nxtsearch.legis.state.ia.us/NXT/gateway.dll?f=templates&fn=default.htm.

[31]Florida Bureau of Voting Systems Certification, *Parallel Test Summary Report for Sarasota County, FL, November 7, 2006 General Election Using Election Systems and Software, Inc. Unity Version 4.5, Version 2* (December 18, 2006). Available at http://election.dos.state.fl.us/pdf/parallelTestSumReprt12-18-06.pdf.

After the polls close, the concern with failure continues. Errors in the transmission of voting results from polling place to the election headquarters are quite common. Signed voter registers and paper ballots must be physically secured and transmitted, and electronic results must be recorded to physical media for physical transport. Redundancy is an important defense against loss. In Miami-Dade County, Florida, for example, electronic voting results are printed at the polling place immediately after the polls close. The paper copy is sealed in an envelope and sent to the regional election headquarters along with an electronic copy in a removable memory module, and the results are transmitted by modem to the central election headquarters.[32] Similar redundancy was present in the 2005 Kazakh election system.[33]

The canvass of the election usually proceeds through a hierarchy of levels. First, the polling place election officials certify a report of the canvass of the votes at that polling place. Then, once these reports are received by the regional election authorities, they are combined to make the certified regional canvass. Regional canvass reports are then combined to produce a state canvass.

Jurisdictions differ in the extent to which elections are subject to auditing. Auditing is an important post-election activity.[34] It may take a number of forms:

- Checking redundant information.
- Election recounts.
- Auditing the tabulation process.
- Re-doing the canvass.

All auditing activities may be further subdivided into *hot audits*, that is, those conducted before the certification of the canvass, and *cold audits*, or those conducted later. Hot audits are necessarily limited, since the time available is limited, while it is more difficult to correct erroneous election results with the result of a cold audit. Some jurisdictions have mixed models, involving a preliminary certification of the canvass, after which certain audits may be performed prior to the final certification.

Checking redundant information: All elections produce redundant information. For example, the number of signatures in the poll book and the number of ballots ought to be the same (in a vote-for-one election), the sum of the number of votes for particular candidates plus the number of invalid ballots ought to equal the number of ballots. In addition, with electronic voting machines, as mentioned above, it is common to produce multiple redundant reports of the results from each polling place. The extent to which this redundant information is considered in checking the canvass varies considerably. In Miami, the paper copy of the results and one of the electronic records from every polling place are routinely compared prior to certification of the regional canvass, and then, after the certification of the canvass, the county's audit and management department conducts a cold audit of randomly selected precincts, comparing other electronic and paper records. In contrast, in 2005, only the electronic copies were considered in the Kazakh election.

Election recounts: Recounts are, effectively, audits requested by candidates when they suspect that the official count is inaccurate. Some jurisdictions have automatic recounts for every election where the results are closer than some threshold. Recounts generally involve a complete repeat of the canvassing process, but they vary in the amount of information considered from the ballots themselves. Hand recounts involve actual inspection of all ballots by people, while machine recounts involve re-tabulation of the ballots by machine. The most limited form of recount, the re-canvass, involves no examination of actual ballots.

Auditing the tabulation process: California has long required that, after each election, ballots from polling places representing 1 percent of the vote be recounted by hand in order to check the correct function of the ballot tabulating machinery. This model has since been adopted by many other jurisdictions, with considerable variation in the number of polling places subject to audit,

[32]Miami-Dade County Elections Department, *Logic and Accuracy Test, August 32, 2004 Primary Election*.
[33]OSCE/ODIHR, *Final report on the presidential election in Kazakhstan*. See section VI.
[34]Douglas Jones, "Auditing Elections," *Communications of the ACM,* 47:10 (October 2004), 46-50.

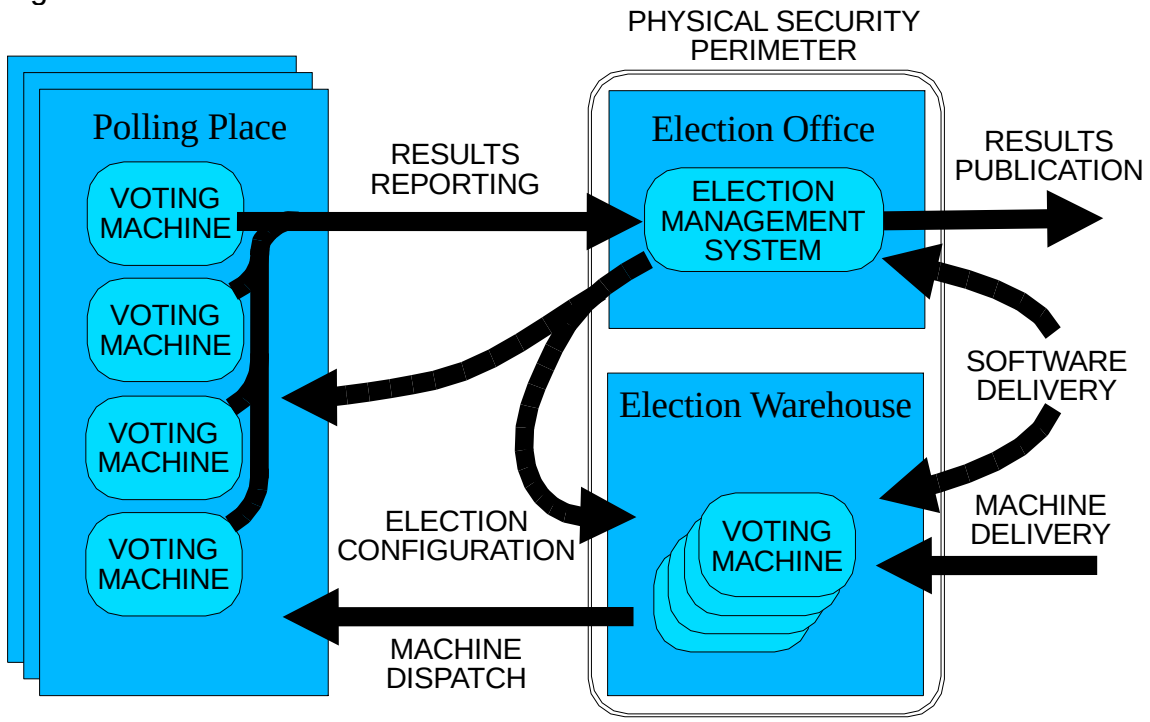
how those polling places are identified and when those polling places are known. The best practice is to determine the identity of the polling places as late as possible, so that there is no way for polling place election officials to know whether their work will be audited until they have completed it. The polling places to be audited should be selected at random, although there are proposals that the candidates should be able to name some of the polling places if they think there were irregularities.

The announcement of the results does not mark the end of the election cycle for the election official! Cold audits may occupy several weeks of effort after the results are finalized, and when this is done, one additional step remains: storing archival copies of the results so that the machinery may be reused in the next election. This archived election data is evidence that may be relevant not only to questions about the legitimacy of the election but also to prosecution of violations of the electoral law at any level. As such, it is prudent to store this information until the expiration of the statute of limitations for prosecution of such crimes and to store it under the same security rules that apply to criminal evidence.

C. The Data Flow View

A security analysis of an election generally begins by isolating all of the data paths through the election system. Once these data paths are identified, the potential attacks on each path can be enumerated. Only after this is done can the defenses be meaningfully evaluated. Figure 3 illustrates these data paths for a jurisdiction using voting machines, but it should be noted that most of these data paths exist regardless of the technology being used.

Figure 3: Election data flow



Machine delivery: As the voting system life cycle begins, machines are delivered to the election warehouse. At this point (as mentioned above), the jurisdiction should conduct acceptance tests to verify that the machines, as received, are functional and are indeed the machines that were ordered. During the lifetime of the hardware, the voting system vendor typically delivers software updates. Each such update should be treated as if it was a new voting system, and again, it is essential to check that the software received was indeed the software certified for use in this jurisdiction.

Machine dispatch: With each election cycle, the machines are moved from the secure warehouse of the election authority to polling places. Typically, the equipment is delivered hours or days before the election, and even if armed guards are present, the authenticity of the machines should again be checked before the polls are opened.

Election configuration: Voting machines, whether electronic or mechanical, must be configured for the election. This configuration has traditionally been done in the warehouse, before dispatching the machines to the polling places, but with modern compact electronic media, it is possible to deliver unconfigured machinery to the polling place and deliver the appropriate configuration files separately.

Wherever voting machinery is joined to election configuration files, it is essential to test that the configurations are authentic and that the machinery, as configured, is fully functional. This can naturally be combined with pre-election testing in the warehouse, or it can be part of testing at the polling place as part of opening the polls. In the latter case, however, the limited expertise available at the polling place poses problems, as does the question of what to do if the configuration is incorrect.

Results reporting: After the voting is complete at a polling place, the results from the various machines used there must be gathered and transmitted to the election management system. As already discussed, this may involve redundant data paths, paper and electronic. These exist, in part, to ensure that the data received from the polling place is indeed the data that was transmitted. Paper records, both physical ballots and paper summary data, provide a simple assurance that is independent of complex technology, while electronic transmission protects against forgery or alteration of the paper records.

For all electronic transmissions, there are technical defenses that can help authenticate the data. This applies to transmissions from the manufacturer to the election authorities, from the election management system to the polling place equipment, and from the polling place to back to the election management system. Broadly speaking, these are generally described as digital signatures or as secure hash codes. These are cryptographic tools for ensuring that a document is authentic and has not been altered.

It is important to emphasize that we are interested in authentication here, not encryption. It is a mistake to require that all election data be encrypted, as is required by the Council of Europe E-voting standards.[35] Encryption, as such, does not prevent or detect alteration, and encryption of information that is publicly known serves no useful purpose.[36] Election results should generally become public records as soon as the polls close, and most of the contents of the election configuration files is public. The only exceptions to this are digital authentication keys for election results transmittal that are included as part of the election configuration. These must, of course, be secured until after the election results have been received and published.

Results publication: The final link in the data flow is from the election management system to the public. Election results must be released. In the days of manual canvassing, it was common for the counting to be conducted in public, with results shown on a blackboard. Anyone could observe the process and copy down the results, and it was trivial for all observers to note that the only ones writing on the blackboard were election officials.

This story changes considerably when computerized election management systems replace the blackboard. With such a system, results from the precincts are entered into a computer, sometimes directly from memory cartridges or by modem, and then the computer declares the result. How can the public be given sufficient access to the election management system that they can observe the election results without granting the public sufficient access to disrupt or alter

[35]Council of Europe, *Recommendation Rec(2004)11 of the Committee of Ministers to member states on legal, operational and technical standards for e-voting*, (September 2004). See item 34. Available at https://wcd.coe.int/ViewDoc.jsp?id=778189&Lang=en.

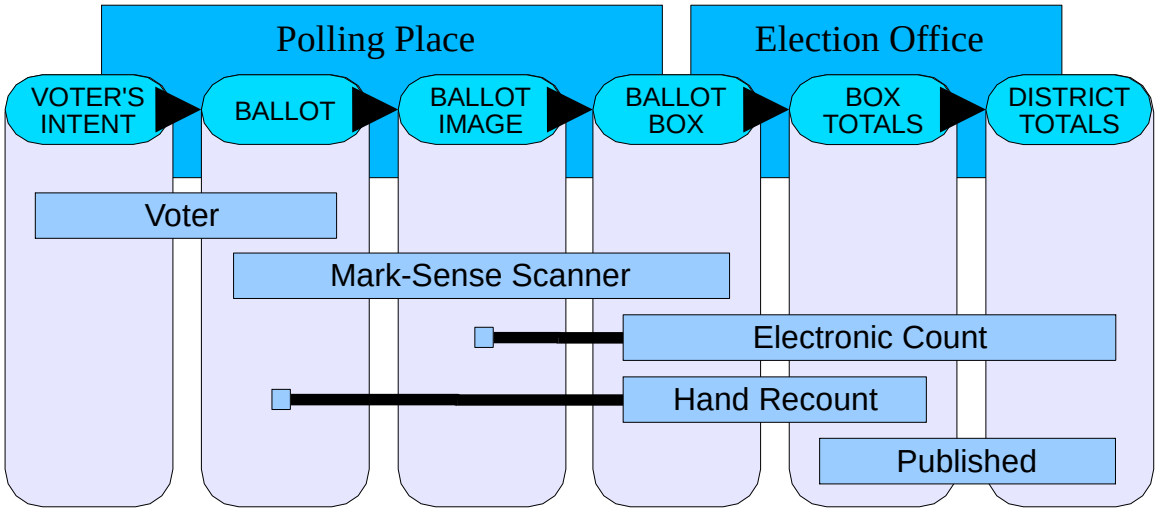
[36]Douglas W. Jones, "Misassessment of Security in Computer Based Election Systems," *Cryptobytes,* 7:2 (Fall 2004), 9-13. Available at http://www.rsasecurity.com/rsalabs/cryptobytes/CryptoBytes_Fall2004.pdf.

those results? Many jurisdictions have directly connected their election management systems to the Internet,[37] a very bad idea. Miami-Dade County recognized the dangers of this and invented a defensive scheme that was simultaneously ingenious, extraordinarily complex and impossible to assess.[38] More appropriate solutions involve easily verified one-way data transmission devices. In the literature, these are known as data diodes.[39]

D. The Chain of Custody View

A final perspective that is useful to consider involves the chain of custody of votes and vote totals as they pass from the voter to the final published election results. The term "chain of custody" comes from the rules of evidence in the United States. Evidence presented with a well documented chain of custody can be trusted, while if there is a weak chain of custody, this raises questions about the authenticity of the evidence. Short chains of custody are easier to trust than long chains. Storing evidence in a secret location known to only one custodian is dangerous if that custodian is not perfectly honest. Storing evidence in the hands of multiple custodians who are subject to public oversight is far safer. Similarly, putting multiple copies of the evidence in the hands of independent custodians offers considerable assurance.

Figure 4: The chain of custody for optical mark-sense voting



The chain of custody illustrated in Figure 4 applies to precinct-count optical mark-sense voting—that is, the voting system where voters mark paper ballots that are then tabulated by a mark-sense scanner in the voter's presence. The scanner drops ballots in a secure physical ballot box as it scans them. The scanner records an electronic ballot image of each ballot as it is scanned, and these are stored in an electronic ballot box. At the close of the polls, both the physical and electronic ballot box are transported to the election office. The votes in the electronic ballot box are then counted to produce the totals for that box, and these are then incorporated into the district-wide vote totals.

At each link in this chain, it is fair to ask who has custody of the data and what proof do we have

[37]Science Applications International Corporation, *Risk Assessment Report – Diebold AccuVote-TS Voting System and Processes* (September 2, 2003). See section 2.2.2. Available at http://www.verifiedvoting.org/downloads/votingsystemreportfinal.pdf.
[38]Douglas W. Jones, *Observations and Recommendations on Pre-election testing in Miami-Dade County* (September 9. 2004). See section 7. Available at http://www.cs.uiowa.edu/~jones/voting/miamitest.pdf.
[39]Douglas W. Jones and Tom C. Bowersox, "Secure Data Export and Auditing Using Data Diodes," *Proceedings of the 2006 USENIX/ACCURATE Electronic Voting Technology Workshop (EVT '06)*, Vancouver, August 1, 2006. Available at http://www.usenix.org/events/evt06/tech/.

that the data correctly reflects the collective intent of the various voters. As the voters mark their ballots, they directly expresses their intent, and election observers can easily observe that the voters themselves place their ballots into the scanner. If the scanner were able to report its interpretation of the ballot to the voter, this would allow the voter to verify not only that the ballot had been scanned, but that it had been scanned correctly. No current scanners do this.

The scanner and ballot box are in the custody of the polling place workers and under observation by the voters and election observers until the polls close. From this point, two distinct chains of custody emerge, one for the electronic data that leads to the district totals, and a second for the ballot boxes and paper ballots.

The electronic records are physically in the custody of the mark-sense scanner software until they are transmitted by modem or extracted to electronic storage media. The notion of software having custody of anything is problematic because the notion of custody usually applies only to people. Nonetheless, the software is able to act independently of its physical custodians, behaving as specified by the programmer or programmers who constructed it and the ballot configuration files that it interprets in order to scan the ballots. This suggests that we must guard secondary chains of custody from the programmers to the machine and from those who prepared the configuration files.

These secondary chains of custody are long and difficult to guard, so many jurisdictions are moving toward a different model based on auditing. In each jurisdiction, after every election, a randomly selected sample of the original paper ballots is subject to a hand count. California pioneered this model in the punch-card voting era.[40] The purpose of this hand count is to verify that the electronic count of those same ballots is accurate. For this hand count to be of any value, we must guard the chain of custody of the paper ballots between the time they are tabulated by the ballot scanner and the time they are subject to hand counting.

In general, the sooner we publish election results, the more difficult it is to fraudulently alter them. If the only published result is the final result, then we must closely guard the chain of custody all the way to the point of publication. If, on the other hand, we publish results earlier, creating multiple copies in the hands of independent witnesses, it becomes far more difficult for later custodians to make alterations without detection. This is one reason why many jurisdictions require that the election results from each polling place be printed in duplicate, with one copy posted for public inspection prior to the transmission of the official copies from the polling place. The procedures for this outlined in Kazakh election law are a good example. This law requires that one copy of the results be posted at the polling place for the public, that additional copies be given to election observers who request them, and that both paper and electronic copies be delivered to the election offices.[41] This early publication allows independent verification of the consolidation of the polling-place results into the final election totals.

IV. Conclusion

Each of the views outlined above serves a different role. The voting equipment life cycle view says more about the voting equipment acquisition process. The election cycle view allows examination of election administration. The data flow view allows evaluation of voting system security, and the chain of custody view helps observers understand the significance of the various pieces of evidence they see. All of these views can play a role in crafting election laws and administrative procedures, and they can play a role in the evaluation of specific voting technologies.

Many of these views reinforce each other. The importance of auditing, for example, emerges clearly in the election cycle, data flow, and chain of custody views. Acceptance testing emerges in

[40]Roy G. Saltman, *Effective Use of Computing Technology in Vote-Tallying* (National Bureau of Standards, March 1975). See page 45. Available at http://csrc.nist.gov/publications/nistpubs/NBS_SP_500-30.pdf.
[41]"On Elections in the Republic of Kazakhstan," *Constitutional Law of the Republic of Kazakhstan* (September 1995). See Chapter 8, Article 43, Section 8. Available at http://www.eurasianet.org/departments/election/kazakhstan/kazelectlaw.html.

both the equipment life cycle and data flow views, while pre-election testing emerges in the election cycle and data flow views. Further examination of these different views can help reveal the nature of the expertise required by the different participants in the process. This is an essential first step that must be undertaken before hiring and training those participants.

The questions raised by the different views of election technology outlined here may appear daunting. Indeed, these issues are daunting. The United States has been using mechanical voting machines for over a century, yet controversies about election technology remain in the headlines today. The Netherlands moved to almost universal use of direct-recording electronic voting machines 20 years ago, yet in their most recent parliamentary elections, controversies about those machines became front-page news. It is clear that these technologies are difficult to administer and that election officials frequently find that they have accepted a burden that is more complex than they are prepared to handle.

IFES
1101 15th Street, N.W. 3rd Floor
Washington, D.C. 20005
Tel: 202.828.8507
Fax: 202.452.0804
www.IFES.org