Doing Things Differently This Time Around
Perspective from an Elections Administrator
By Dana DeBeauvoir, Travis County Clerk, Austin, Texas

A second chance to get something right is a rare luxury in the world of elections, yet, less than ten years after the 2000 presidential election recount in Florida and the subsequent Help America Vote Act (HAVA), we are on the cusp of a new generation of voting systems and requirements. Slowly but steadily, we are moving away from an all-electronic voting environment toward paper ballots with an electronic count. As we define how this new hybrid world will look and operate, it is important that we learn from recent rocky years and find different and more constructive strategies of working together.

Although the added benefit of a paper record provides a more reliable means of performing audits and recounts, all election administrators (except for the smallest of entities) will still rely heavily on computers to tabulate results—and perhaps also to generate paper ballots at polling sites or to capture the vote of the disabled. So while some may assume that reintroducing a paper element resolves security concerns, those of us close to the process know differently. In fact, you could argue that security responsibilities will actually double, since both the paper and electronic elements of these systems must now be managed.

Ten years ago, electronic voting was still a novelty and only a handful of entities had adopted it. Discussions were largely isolated to transitional issues: how would voters adapt? What kind of training and logistics were needed for election workers? How would these systems be set up and made operational by the time the polls closed? The prospects of software attackers, computer viruses, and the world of advanced cryptography seemed more like science fiction than major topics in the election world. Wouldn't it have been great if everyone had known then what we know now? Wouldn't at least some things have been done differently?

Today, we find ourselves again facing issues similar to those in 2000. There is a public stigma that electronic voting systems cannot be trusted and communities are either already moving to new types of voting systems or are planning to do so. Meanwhile, the relationships among all of the parties involved in elections are still governed by last decade's formulas— formulas that have a lot of negatives.

As an example, consider this somewhat oversimplified description from the perspective of a frustrated election administrator (EA) during this past decade:

In 2000, after the weaknesses of old punch card systems were dramatically exposed—in film clips of perplexed election workers examining ballots with magnifying glasses and in the endless news reporting that made "hanging" and "pregnant" chads household terms—the electoral change movement was thrown into high gear. A variety of certified election equipment became newly available for state and local (typically county) governments. (In Texas during this time, ADA court rulings temporarily made DRE's the only acceptable equipment certified for use.) In 2004, the Help America Vote Act set new federal standards for voting systems. Entities that needed to replace or upgrade their systems were required to purchase systems meeting the new

specifications and convert to them by 2006. Both state and local governments were covered by the new regulations, and a great deal of federal funding was provided to facilitate the transition.

After these sweeping changes and as information regarding computer security filtered out, election administrators began to discover and apply practical testing methods and security to make the new systems less vulnerable to errors and threats. Despite these efforts, election administrators were effectively forced into no-win situations. For example:

- Elections Administrators were the main force in developing safety protocols for the new systems, even though they had not participated in their design, and they had little or no say in the requirements used for their certification. They turned to physical security methods, testing procedures, and auditing practices because they had (and still have) virtually no means of demanding any software improvements or standards.

- EAs had minimal assistance from vendors and few options since only a handful of vendors serve all of the election entities in the United States. Vendors implored the public and administrators to trust them while at the same time withholding their software code as proprietary. Vendors, in turn, were in the unenviable situation of needing to keep upgrades to a bare minimum, since even the smallest change required an exhaustive recertification process. The identification and airing of problems and remedies, as well as overall security improvements, were discouraged because of the sluggish and costly recertification process.

- EAs had to hunt down, sort, and analyze a myriad of information, from anecdotal evidence to actual research, that appeared from widely scattered sources. Academic papers and Internet rumors were often given equal weight in the public discourse, and no relevant information was ever formally reviewed for accuracy or applicability by the certification authorities who, under a screen of confidentiality, reviewed the software and certified the systems. As a result, accusations against the election systems, whether valid or invented, continued to stand uncontested by any independent authority.

- EAs were vilified by electronic voting critics who made broad, sweeping statements that condemned all electronic voting systems and the people who administered them.

- EAs often ended up working alone to find ways to make voting safer because vendors, certifying agencies, academicians, and other critics devoted their energies primarily to their own agendas, either absolutely attacking or absolutely defending electronic voting without providing intermediate, practical analyses and solutions.

As stated earlier, this is a simplified description of the position of election administrators, intended to help readers understand their level of frustration. Its purpose is not to inflame hard feeling among the groups involved, nor is it to, as an election administrator, cry "woe is me!" There can be no question that academicians and electronic voting critics, vendors, certifying agencies, and others felt just as much frustration with the situation as did EAs. Academicians communicated much of their expertise and findings after the certification process was finished, and to them it must have felt like they were hollering into a dark well. Vendors felt hamstrung

by the certification process and found themselves stuck in a low-profit business riddled with endless red tape, and, on top of this, they became the go-to targets and scapegoats of anyone and everyone with an agenda. Community activists felt worn out, their concerns seemingly brushed aside under a carpet of secrecy, and were left to wonder how a democracy that boasted of being a government of the people could even be trusted to count the people's votes. As an election administrator, I also know that election administrators were not perfect during this time. In the face of accusations we felt were false, we became defensive. We could have done more sooner but were resistant to having to make even more changes. And, we were just plain grumpy about the whole situation. The point here is not to assign blame but to illustrate how no one benefited from an approach that was ridiculously flawed from the start.

So today, at this important transitional moment, we need to come up with a new way of doing business around the next generation of voting systems, and we have only a small window of time to make this change. The new cycle has already begun. Two of the election equipment vendors have announced that they are already back at the drawing board to develop new voting systems. Before this process gets too far down the road, we must reclaim our proper roles and work toward our strengths. The previous backward process—in which voting security problems with no viable solutions come to the forefront *after* the passage of reform legislation, the enforcement of ADA standards, the certification of systems, the purchase of new equipment by state and local entities, and the conduct of elections—caused everyone to torque into ill-contrived positions. This does *not* have to happen again. Following is a draft of ideas of how we can return to our core responsibilities so that we can function in more natural and productive roles. Please know that some possibly controversial items have been included in order to spur thought and conversation.

Roles of Election Administrators

- Administrators must focus on taking care of voters and competently conducting elections so that communities can trust the democratic process.
- Administrators must actively participate with certifying authorities in a requirements process that directs vendors to meet their needs. This would be unlike the current situation where Administrators are forced to pick what just a few vendors have independently designed.
- Administrators must keep abreast of all types of security risks received from all sources; however they must also be able to rely heavily on assessments from sources (possibly the certifying agencies) that routinely receive and analyze anecdotal and research-backed information regarding potential risks and then issue recommendations for physical or procedural changes that can help mitigate these problems until a vendor solution can be implemented.
- Administrators must receive more training specific to computer security and encourage comment and fact-finding by computer security experts.
- Administrators must demand that their national organizations provide educational classes on voting system design and software security and make them a mandatory part of any professional certification program.
- Administrators must consider election academicians one of their best resources and encourage opportunities for these researchers to have access to the whole election process in real-life situations so that everyone can learn new ways to improve.

- Administrators must have better and more uniform methods of mitigating risks and detecting if a system attack has occurred. The evidence that these mitigation procedures are being followed should be open for review, criticism, and monitoring.
- Administrators must fully document unusual situations or substantiate anecdotal concerns, and these reports should be sent to a certifying or monitoring agency. This may sometimes mean revealing one's own errors for the benefit of everyone.
- Administrators must always listen to concerns from citizens who have suggestions or criticisms of voting systems and offer anyone the opportunity to see any part of the process.

Roles of Vendors

- Vendors must solicit more input from election administrators, election security experts, the disability community, voters, and the certifying and monitoring agencies during every stage of product development.
- The engineers who design the systems must go into the field to observe real-life election scenarios, both before and after designing a system.
- Vendors must have the ability to expend resources for research and development instead of finding ways to minimize changes to avoid the lengthy and expensive certification process.
- Vendors must consider the real-world and current need to provide better and more cost-efficient products instead of protecting or minimizing changes to an outdated or inappropriate system.
- Vendors must be required to prove in a public setting that their systems have high levels of security and performance, perhaps using open peer reviews.
- Vendors must establish a code of high ethical standards that includes the promise that the corporation and its top executives will not make political contributions to individuals or political action committees.

Roles for Academicians and Computer Security Experts

- Academicians and experts must continue their efforts to find flaws or holes in election security.
- Academicians and experts must place more focus on and give greater value to developing practical solutions and safeguards to problems that have been shown to exist or to potential future problems.
- Academicians and experts must create more equity between the goal of finding problems and the goal of finding solutions.
- Academicians and experts must help determine whether claims that surface through variously reported problems or through Internet chatter are real or exaggerated.
- Academicians and experts must work in close partnership with election administrators to find solutions. (An example of a positive outcome would be a computer expert who, having identified a vulnerability, was able to work with the election administrator to develop a procedural method for mitigating the risk until additional software protection could be implemented and certified.)

- Academicians and experts must improve communication and working relationships with vendors and certifying or monitoring agencies, perhaps by participating in open peer reviews of software.
- Academicians and experts must work with election administrator organizations to provide classes that teach the basic technical aspects of computer security, and they must regularly update these organizations on new information.

Roles for Certifying or Monitoring Agencies

(In this section for ease of discussion, I am grouping all federal and state agencies with election responsibilities together and calling them "Agencies." I am not trying to put forth a specific design for an organization.)

- Agencies must have leadership that includes computer security expertise, election administration, and disability services.
- Agencies must provide a central reporting, monitoring, and research division that investigates and serves as a clearinghouse for anecdotal information and reported events. After investigating incidents, agencies should publicly comment on the findings. It is vital to get correct information on the record. Initial news reports that misinform the public and create unnecessary distrust cannot be allowed to stand.
- Agencies must actively seek out information from and involvement by academicians who are either directly studying elections or indirectly researching related fields such as cryptography.
- Agencies must take an active role in providing assistance to election administrators regarding the latest recommendations for detecting problems, mitigating risks, and identifying computer attacks. This information must be continuously updated and disseminated.
- Agencies must provide sufficient numbers of qualified staff to operate a streamlined process that can move vendor products more quickly and less expensively through certification.
- Agencies must regularly compile a list of suggested software upgrades, hardware changes, etc. that would make voting safer. This information should be made public so that vendors, computer security experts, and other interested parties can comment and discuss these changes.
- Agencies must set a deadline for vendors to comply with these upgrades and have a process where recertification can occur quickly and less expensively.
- Agencies must help develop standards of ethics and conduct for businesses offering to provide independent audits of results or processes; these standards should be similar to those used by financial auditors. (For example, guidelines could be set to determine if it is appropriate for a person or business paid to participate in the certification of a system to later be hired as an independent auditor to report on the performance of that system in an actual election environment.)
- Agencies must promote a fair and open marketplace for election system vendors that demands competition and innovation.

Given the task of considering these suggestions, it is natural to ask, "Where do we begin?" The first step is for each group to spend less time talking to its own membership about just its own viewpoints. Instead, we need to claim our proper roles and work actively with individuals in the other groups. We need to look outside our own boundaries so that we can understand and utilize the knowledge and perspectives these other groups have gained. We need to build relationships based on trust, respect, and shared purpose. The development of joint solutions should be given paramount value, and the process of finding flaws always paired with the obligation of finding practical remedies. Meetings should be held as soon as possible with representatives of the academic community, computer security experts, election administrators, and other election agencies and groups. A means of hearing comments and concerns from members of the public with concerns and ideas should be incorporated. These discussion should not dwell on the past, but focus on how we can best work together to improve the voting process now and in the future. Below are a few example discussion questions.

1. How can computer scientists/academics fulfill their role to critique? How will peer review occur? Specifically, how are we going to define open software or open source code? How can the election administrator make use of these types of reviews? How will they affect the operations of the election administrator?
2. Are adequate security standards and procedures in place for precinct ballot counters, VVPAT equipment, and systems that produce individual ballots at the polling place?
3. What new methods of proof should be required of vendors to show that their systems meet the EAC Voluntary Voting System Guidelines 2005 (VVSG) level of security standards or higher?
4. What new methods for testing or physical security should administrators be considering? Are there pilot projects that would be helpful for election administers to try?
5. How will appropriate pre-election testing and post-election audits be developed and standardized for the new voting technologies?
6. Many jurisdictions want independence from the vendor in ballot design, lock-down, and operation of the voting system; other jurisdictions want, and perhaps need, vendor technical assistance. If the vendor is involved, what methods should be followed to ensure that no tampering occurs and conflict-of-interest questions are addressed?
7. How can we create an atmosphere that promotes greater competition, forces more innovation, and keeps purchase and maintenance costs at more reasonable levels?
8. What clear messages can be sent to vendors regarding future standards for security and reliability of operation? Is the EAC the proper messenger?
9. How can the certification processes be improved, done at more frequent or regular intervals, and at a lower cost?
10. What types of documentation can states require from election administrators to ensure that proper testing procedures are occurring?
11. What type of system can be put into place to keep information on computer security up-to-date and disseminated?
12. What new ideas for voting systems need a chance to be heard? Do we need to give vendors a description of what we want the new voting systems to look like?
13. How can we make certain that members of the public or citizen organizations with concerns about voting have an opportunity to voice their opinions and ideas? How can we make certain that those thoughts are broadly communicated to all election

administrators, vendors, academicians and security experts, certifying agencies, and other decision makers?

14. How can we improve the way in which we vote and the appearance of the ballot to make it easier for voters to use?
15. What requirements can we incorporate to make voting systems environmentally friendly? How can we reduce paper usage and lower electricity demands? How can we make certain that the materials and processes used to build equipment have minimal effects on our limited resources? How can we make certain that proper options are available for out-of-use equipment that must be discarded and for salvaging and recycling parts?
16. No matter what kind of voting system – whether current or new – an effort to improve sustainability is an ongoing challenge we have yet to address. How do we sustain systems, protect them from pre-mature obsolescence, and guard against paying a premium for parts and repairs?

My goal in presenting this paper is to focus attention on the need for all of us to adopt and speak from our proper roles and to work together toward a united purpose for the voters of our great country. I want to take this lump of steel while it is still hot and malleable and have us all participate in pounding it into a strong and workable tool. I am seeking input and support from everyone in the elections community so that we can devise better ways to communicate and be accountable to one another. We can achieve something incredible if we act now. I look forward to hearing your comments and ideas.

Respectfully submitted,

Dana DeBeauvoir
Travis County Clerk
dana.debeauvoir@co.travis.tx.us
512-854-3996
January 2010