



---

# MEMORANDUM

---

Date: October 19, 2007

To: The Honorable Chairman and Members  
Pima County Board of Supervisors

From: C.H. Huckelberry  
County Administrator

A handwritten signature in black ink, appearing to be "C.H. Huckelberry", is written over the typed name and title.

Re: Election Security

## Background

On May 17, 2007, after learning that allegations of potential election fraud had been made regarding the Regional Transportation Authority funding election, I asked the County Attorney to request an appropriate investigation of this matter by the Attorney General. The Attorney General then undertook a criminal investigation of these allegations. The County and our employees have fully cooperated with this criminal investigation. We understand the difficulty and complexity of the investigation and are pleased it has been concluded with no findings of criminal wrongdoing on the part of County Election employees or the County Division of Elections.

We are also pleased with the findings of the Attorney General that the Regional Transportation Authority Excise Tax Election shows no evidence of tampering, alteration or election fraud. We also concur with and acknowledge the difficult and complex issues associated with election security highlighted by the investigation of the Attorney General. These security issues are faced by every state and local election authority.

Pima County has been and will continue to be diligent in our efforts to ensure election security. To enhance our security measures while providing complete and full transparency of election functions, we have, in the recent past, completed substantial modifications to our physical facilities and election processes. Additionally, we believe that recent changes in state law requiring hand count verification of electronic vote tabulation results is a positive step to ensure the integrity of election results and ensure voter confidence in those results. While Pima County's election security systems are among the best in the state, more can, and should, be done regarding election security, particularly in the area of electronic vote tabulation. The following pages contain my recommendations regarding the conduct of future elections.

## Increasing Security Concerns Related to Election Results

We clearly understand the principle that every vote counts, and that every vote must be counted and reported accurately. As technological advances have been implemented, the

ability to ensure fair, accurate and secure elections has dramatically increased. Ironically, and despite these advances, there have been, and continue to be, heightened concerns across the United States regarding election security and the validity of election results.

With the advent of electronic touchscreen voting devices, new concerns have been raised regarding election security and, hence, election outcomes. These concerns are valid and require carefully crafted policies and procedures, independent checks and balances, and, importantly, the impeccable integrity of all individuals involved in the election process. Locally, the political parties, and the Democratic Party in particular, have been concerned about election integrity. In response to the concerns of the parties and the concerns of others, the County made significant modifications to the conduct of the 2006 general election. Presently there is ongoing civil litigation regarding access to certain computer files for this and prior elections. While we may disagree with the Plaintiff in this litigation, we do not disagree with the principle of election security. In fact, it is precisely because of our concerns for election security that we have opposed the release of electronic information databases on the grounds that such information is not only made confidential by law, but also because such release would make future elections more vulnerable to electronic attack.

#### **New Election Security Measures Established Prior to the 2006 General Election**

Prior to the 2006 election process, a number of measures were implemented to improve security and enhance transparency of the election process, particularly with respect to activities at the technical center where the election results are tabulated and summarized. This center is also the receiving station for all precinct level vote tabulation devices and contains the computer equipment for tabulating all election results, both absentee or early ballots, verified conditional ballots, and Election Day ballot data transmitted from the polling places. The modifications made in 2006 can be classified as facility modifications, process modifications, electronic countermeasures, vote device counting measures, or as training and staffing improvements. Each of these are identified below to provide an understanding of the additional level of security improvements that went into the 2006 election and that will carry forward as we now prepare for the 2008 elections.

##### **1. Facility Modifications**

- Removal of all network cabling in the Counting Room from within the walls to be openly and separately displayed in ladder racks suspended from the ceilings. Each cable is a different color and can easily be traced from the equipment to the actual Ethernet Switch. Server connections are also color specific and allow for isolation of the servers between counting sessions as described later. The green ground cable is clearly defined. No outside data wiring is connected to the GEMS counting systems.

- Installation of an electronic access control system that secures the entire counting facility. This system checks both ingress and egress by a RFID card assigned to each of the staff as well as three cards for Sheriff's deputies. A limited number of cards allow access into and out of the Counting Room. For those entering the room without a card, the use of a manual sign-in and sign-out log with times and purpose of the visit is required.
- Installation of a video surveillance system consisting of 16 color cameras, with infrared capability when bright daylight is not available. These cameras are connected to a recording system that is triggered by motion detection in the camera. Cameras cover all doors and areas where ballots or equipment will be handled or processed. Cameras also show the top/back of the locked computer cabinet as well as the area where the computer and console reside and the front of the cabinet--but are not focused so sharply as to divulge entry of a password on the keyboard. The feed from four cameras is displayed on a 42-inch flat panel monitor that is visible from the public viewing area in the lobby of the center as well as the observation area inside the Counting Room. These four images show the computer area and the operations area and where seals are checked on election night.
- A second console monitor was relocated to allow full view of the flat panel monitor and is in the west edge of the lobby viewing window, so visitors can see console operations as they occur. A third console monitor was added to the wall adjacent to the console desk for the Observers' view. The Party Observer area in the Counting Room has been extended to allow Observers to view the computer and console area directly.
- Secured the power disconnect boxes to the building with standard keyed padlocks to prevent intentional or accidental drop of power during the vote counting process.
- Secured the metal siding that was added to the building with epoxy to insure against inappropriate access via removal of those panels.
- Improved the door structures for the front and back doors to be secure.
- Extensive lighting has been added to illuminate the parking lot, as there is a great deal of foot traffic in and out during Early Counting as well as on election night.

## 2. Process Modifications

- An agreement was reached with the official Observers of the Democratic Party to produce a series of control reports--before counting any early votes, at the end of each counting day, at the beginning of each subsequent counting day, and after the final counts--to determine continuity of numbers being added. It should be noted that these reports do not contain details related to any specific race, so it is impossible to use these reports to alert parties of possible outcomes.

- An agreement was reached with the official Observers of the Democratic Party to produce a printed and electronic version of the Windows Event Log to be used to identify the installation of any new software, enabling or disabling any specific hardware, or other nonstandard modification of the system. This will occur prior to the beginning of the counting of early ballots, and again following the completion of the count of all votes.
- An agreement was reached with the official Observers of the Democratic Party to provide them, and the other parties, with snapshot copies of the GEMS Audit Log prior to the beginning of counting of early ballots, and again following the completion of the count of all votes.
- Agreement was reached with all of the official Party Observers at the Party Logic and Accuracy Test on October 21, 2006 as to the schedule for the processing of early ballots, the disconnection of the servers from their Ethernet Switch and securing of the computer cabinet following the day's activities, and the process of opening the cabinet, reconnecting the servers and running the agreed upon control reports.
- Agreement was reached with all Party Observers to modify the flow of the equipment received on election night. The Elections Board that inspects the seals and validates status of equipment will be located in the warehouse--just outside the pass-through window so only those machines requiring activity will be passed into the room for processing once the Board has approved them.
- Agreement was reached with the Democratic Party as to the number of races (4) to be audited in the precincts included in the post election validation audit process. The 2007 amendments to the hand count statutes have changed and clarified the law, negating the need for continuation of this particular agreement.

3. Electronic Countermeasures

- Using two different election scanning devices, Building 27 and the TSx machines awaiting placement in the field were swept to determine the presence of any wireless transmissions that could impact the equipment. The same scanning devices were used on Election Day to scan for wireless activity at random precincts selected by the political parties, and to scan incoming devices and the Technical Center on election night.
- Hash Totals of the processing software were generated from copies taken at the beginning of the counting of Early Ballots and on election night, and finally after all votes had been counted. These copies were processed by the County Information Technology Department to create Hash Totals. The resulting Hash Totals were compared against the Hash Total for the certified version of the GEMS software

that is available from the National Software Reference Library. This process verifies that the software actually running on the GEMS counting computers is exactly the same as that certified at the national level. Increased use of Hash Totals will be identified in a later section.

4. Vote Device Tampering Countermeasures

- An additional tamper evident seal was added to the side opposite the doors on the TSx device to prevent anyone from taking the screws out of the case and gaining access to the logic boards inside "clamshell" style.

5. Staffing and Training

- As many as 12 additional troubleshooters made up of technical staff from a number of County departments will be available to precincts to troubleshoot or assist in setting up the TSx equipment.
- Additional training was conducted for over 2050 workers to improve their knowledge of the TSx systems.

As set forth above, there have been a large number of modifications made to the election process in 2006 that significantly added to election security and integrity. The balance of this report will address those additional measures that will now be taken to enhance security for future elections.

Electronic Voting Security Review Findings

Because of the complexity of reconstructing and performing forensic analyses on electronic databases and software, the Attorney General employed the services of an expert in computer fraud analysis. This firm, iBeta of Aurora, Colorado, is one of the federal Voting System Testing Laboratories accredited by the United States Election Assistance Commission to test voting systems for federal certification. iBeta produced a report for the Attorney General regarding its investigation of allegations relating to the 2006 RTA election. The report is included as Attachment 1 to this memorandum. In summary, the iBeta report stated that there was no evidence of manipulation of the RTA Bond Election data files as alleged by the Democratic Party. A date error was discovered, but was attributed to human error that occurred when a file was being saved. Furthermore, iBeta stated that its testing revealed that the GEMS software exhibited "fundamental security flaws that make definitive validation of data impossible due to the ease of data and log manipulation." It is this finding that further strengthens our commitment to ongoing improved physical security as well as the implementation of more checks and balances.

To assist both the Attorney General and iBeta in their electronic forensic analysis of the RTA election process and results, I directed that Dr. John Moffatt, Office of Strategic Technology Planning, be available to assist the County Attorney, Attorney General and iBeta by providing information regarding the County's computer systems, particularly related to elections. Such assistance was appropriate as there was a need for local technical knowledge of the operation of the Counting Center to supplement information obtained through the forensic processes employed by the Attorney General and Department of Public Safety. In addition, Dr. Moffatt reports only to me and is completely independent of the Division of Elections or any other agency involved in the elections process.

#### Election Procedure Error

In addition to the findings of iBeta, the Attorney General focused attention on the allegation that an employee of the Division of Elections ran a vote tabulation summary report on early election vote results, and that this constituted a violation of law. Running the vote summary report on early election results by an Elections employee is not a violation of law. Only disclosing the results to affect the outcome of an election is a violation. This allegation was one of several presented to the Attorney General by the Democratic Party. Following an extensive investigation, the Attorney General did not comment on or recommend changes based upon this activity.

Running a summary report has been a past practice of Elections staff. The primary objective of Elections staff in running such a report is simply to validate how the actual physical number of ballots counted by the computer compares to the number of ballots submitted by the Recorder's Office. This is an important verification process to determine that ballots were not skipped or counted twice in the tabulation process. On our existing system, two computer-generated reports can verify this information. One is the Summary Report and one is the Cards Cast Report. The Summary Report produces the number of ballots tabulated at the top of the first page of the report.

The Cards Cast Report produces the same result, but the total number of transactions processed is displayed at the very end of the report, which is typically as long as 16 to 20 pages. For time and convenience purposes, Elections staff has utilized the shortcut of viewing the top of the first page of the Summary Report to track and verify the number of ballots processed to that point. While this practice has been convenient, it has obviously left the Elections staff open to criticism and to the charge that they may have somehow used this information to the advantage of a candidate or a particular ballot measure. The investigation of the Attorney General indicates that no such use occurred. Nevertheless, use of the Summary Report to track processing counts has been discontinued. In the future, the only report that will be run to track progress and validate ballots processed will be the Cards Cast Report.

It should be noted that there is an appropriate time and place to run the Summary Report during an election. Summary Reports must, by law, be run immediately prior to and following the processing of an "audit batch" for the required hand count audit of election results. As required by the Secretary of State's Election Procedures Manual, the Summary Reports for selected races and precincts are printed face down at the beginning of the batch selection and at the end of the batch selection. Without being viewed, these reports are placed directly into the box with the ballots from the audit batch. The box is then immediately sealed and signed by Elections staff and Party Observers in attendance. The Party Observers are present during the entire batch selection process, including the running of the Summary Reports.

#### Lack of Thorough Documentation Related to Vote Tabulation Activities

Vote tabulation activities are conducted over a series of days, not just on election night. Early ballots are counted prior to and, if necessary, after Election Day. Precinct TSx machines are brought into the counting center to download the vote data. Verified conditional ballots and duplicated ballots are counted after Election Day. Each time a tabulation activity takes place, the GEMS system is utilized to tally the vote totals. In addition, appropriate computer duplication and backup activities occur on a regular basis. Based upon our review of vote tabulation processes and results of the iBeta review, it would be prudent to require more extensive written standards, documentation and verification of computer tabulation activities. In the case of the RTA vote tabulation, such documentation did not occur. However, I wish to emphasize that such extensive documentation was not and is not required either by statute or by the Secretary of State's Election Procedures Manual. In fact, until the Democratic Party referred its allegation of illegal activity to the Attorney General, the integrity of our staff and their actions during the tabulation of votes had never been challenged. Indeed, representatives of the Secretary of State have affirmatively acknowledged the professionalism of Elections Division staff. This lack of documentation, while in itself it is not an error in the conduct of the election, made the County vulnerable to questions regarding computer tabulation activities. Therefore, we will document every computer action from log-on to log-off in all future vote tabulation computer activities. This documentation is simply the extension of good business practices to the conduct of elections. All documentation will be reflected in a chronologic log appropriately witnessed and verified by a third party.

#### Electronic Vote Tabulation Security Measures to Prevent Electronic Election Fraud

Based on the investigation of the Attorney General, the iBeta report, and the analysis by Elections staff regarding election security, the following actions will be implemented to improve election security and integrity.

1. Election Software and Hardware Administration - Previously, Elections personnel had "Administrative Rights" over the servers which house the GEMS software. These Administrator Rights allow the user full management access to the server, including loading software, adding hardware and performing security-oriented tasks related to users and the operating system. To add an additional safeguard for election security

and to provide a layer of separation between the Elections staff and the management of the counting systems, Administrator Rights will not be available to Elections personnel. System administration will be transferred to a pair of independent system administrators within the Information Technology Department. If the need arises for capability beyond that of a "superuser" on the servers, access to these systems will only be obtained through the independent third party system administrator in the Information Technology Department, and then only after the problem and/or issue has been identified with Party Observers if during an election, or with the involvement of the Elections Director if during a period outside the processing of an election. Note that the dual password capability (described below) shall apply to the System Administrator password as well, so at least two people from the Information Technology Department would be needed to make any changes.

2. Dual Passwords - No single Elections staff individual or administrator will have knowledge of the entire password required to gain access to the computer equipment or the tabulation program. Individuals will be given only a portion of a password meaning that computer access cannot be obtained without the knowledge of at least two individuals and therefore, no single individual within the Division of Elections (or, as noted above, within the Information Technology Department) will be able to gain access to the central tabulating computer or its programs.
3. Discontinuation of Precinct Level Results Modem Transmittal - Because election results at the precinct level are transmitted via modem over telephone lines to the central tabulating computer, one vulnerability of the electronic tabulation systems that has been identified is commonly known as the "man in the middle" possibility. In this scenario, it might be possible to intercept the modem transmission and substitute fraudulent results which would be transmitted to the central tabulating computer. Despite the substantial efforts that have been made to provide security for the modem transmission of votes, this practice will be discontinued for future elections. This simply means that the sealed precinct-level vote scanning and touchscreen devices will have to be transported to the central counting station before election tabulation results therein are downloaded to the main computer at the central counting center. The physical transportation of the precinct machines rather than the transmission of results via modem will delay the release of election results significantly. Rather than election results usually being known before midnight on Election Day, it is possible that the election results will now not be known for one or more days after the election.
4. Ballot Accountability - Accountability for every ballot is a requirement of the electoral process. With an increasing number of voters choosing to vote early, controls have been established at every step to insure that no early ballots are omitted from the count. There will be extensive logging and more time consuming counts as ballots move from one processing station to the next. Every ballot will be accounted for, even those that cannot be processed due to any extraneous markings or physical damage that prevents reproduction by the Duplication Board.

5. Chain of Custody Records - Because portions of the ballot processing stages have, of necessity, been decentralized, there will be increased controls with respect to the transport of ballots from the Recorder's Office to the various County buildings where processing takes place to the Counting Center. The number of ballots will be recorded and chain of custody logs will be kept for the various types of ballots. These records will be available for Party Observers. During periods when Party Observers are present, they will be asked to witness and initial the logs. In areas where Party Observers are not present, logs and seals will be initialed by staff with different party affiliations.
6. Records Retention - Records retention and destruction procedures will be reviewed by the Clerk of the Board's Office to insure compliance with State record keeping regulations and to establish processes to facilitate timely destruction of materials remaining after each election. Detailed logging of materials submitted to the Secretary of State will be initiated and retained as appropriate based upon State approved retention schedules. (Pursuant to legislative changes, the Secretary of State will no longer return election programs to the County.)
7. Video Retention - Archiving of electronic images captured from the video surveillance system installed at the Technical Center as well as the data files retained by the access control systems has been completed by the Information Technology Department. Retention rules have been established in accordance with normal election record retention standards promulgated by the State Department of Library and Archives. The Information Technology Department has the responsibility for destruction of the images and access control records on the appropriate destruction date.
8. Change Control - Over time, changes to the Election Servers will be required. In order to appropriately track authorized changes, the Change Control procedures utilized in the Information Technology Department will be adopted for these servers. This process incorporates review, testing, publication and approval procedures to be completed before any modification can be made to the systems. The Change Control Logs will be made available to the Party Observers and Secretary of State's staff upon their subsequent visits for Logic and Accuracy Tests.

### Electronic Counter Measures

Hash Totals – The use of Hash Totals is an internationally recognized process by which two electronic files can be compared and determined to be exactly the same.

Due to concerns raised about the possibility that files containing votes that are stored on the Election system could be tampered with during the absence of Party Observers, a new process will be initiated to create a Hash Total on the backup files created upon the completion of any processing cycle, before the departure of the Party Observers. A copy of

the resulting Hash Code will be provided to each observer as well as locked up and sealed for safekeeping in the computer cabinet at the Counting Center. The next time votes are to be counted, the files will again be processed through the Hash Total algorithm, prior to their being loaded for subsequent use. The Hash Code generated must match the code given to the Observers and saved at the Counting Center as a precursor to proceeding with vote tabulation. This will insure the entire vote processing system is the same as it was when last observed.

In 2006, Pima County tested the GEMS executable program against a Hash Total calculated from the information used at the federal level to certify the GEMS system. There are other components of the GEMS system database that are used to create ballots and control the systems that process votes in an election. Those components should not change once an election is "SET" and the Secretary of State performs its Logic and Accuracy Test on the Central Count computer as well as on the Optical Scanning and Touchscreen voting equipment. A process is being developed to extract the critical components of the GEMS system database into a specific file structure that can then be compared throughout an election cycle using Hash Total technology to insure the same programmatic controls and parameters exist from the Logic and Accuracy Test, through Early Ballot Processing, on Election Day, during subsequent processing of absentee and other exception ballots following Election Day, and finally, just prior to submission of the Election results to the Board for the Canvass process.

Under current Secretary of State standards, Election Servers must be used to program and process ballots using the same hardware and software configuration as certified at the State level. In order to be able to optimally process the Hash Total tests described above, Pima County will ask the Secretary of State to add the Hash Total Routine used in the Federal certification process as a standard component of the certified system. This will enable processing the Hash Totals on the servers during the election process with the data files in place--avoiding copying or exposure of the files to any removable media while using a well established and recognized tool. Hash Total calculations are a very effective tool to insure consistency of file content and are invaluable in discovering modifications to critical files. If it is determined that the proposed solution is prohibited or introduces an additional risk of release of critical data, this approach will be abandoned.

Wireless Surveillance - As wireless networking becomes more effective and proliferates through more devices offered throughout the industry, the potential for intrusion grows. In addition to using multiple scanners with widely ranging capabilities to scan equipment, and scan for connectivity possibilities in party recommended (and randomly selected) precincts, the Counting Center will become a wireless-free zone where laptops or any other portable data devices capable of transmitting data in a networking environment must be turned off. With the increased handling of Smart Cards that contain votes to be processed on election night, wireless and video surveillance will be applied to insure no opportunity for tampering.

Additional Testing Computer in the Counting Center - One of the recommendations arising out of the iBeta investigation was the inclusion of another (third) computer to retain snapshots of the GEMS System for testing purposes during the processing of an election. This third computer would be separate (not networked) from the official Election Servers and data would only be transferred to this system via CD or DVD media. Since it is inappropriate to introduce any non-certified software or data files onto the official Election Servers, this third computer would include the Hash Total routines discussed earlier and remain a repository of the backup files that would be deposited at the end of every processing cycle. The same separation of Systems Administration capability and user logins as described for the Election Servers would be consistently applied. Elections Department users would not have delete rights to any directory. Information Technology Department system administrators will have the capability to delete files upon direction of the Elections Director, but will not do so until the Election Canvass is complete.

This Test Computer would provide a place to perform the technical testing described earlier in this document, without compromising the official election servers and insuring that the files to be tested remain in a secure environment. No data will be taken from this computer for any purpose and the files loaded for testing will be deleted once the election is canvassed. This system will not have the ability to write any removable media--only read them. Hash Code testing software will be documented and disclosed to the observation teams during the Party Logic and Accuracy Test process. All file transfers and Hash Code testing will be performed in the presence of Party Observers. A separate printer will be connected only to this Test Computer in order to print the results of the testing. File contents will not be printed, only the results of the Hash Code tests.

The sole purpose for this computer would be to provide an even more secure, transparent testing environment without compromising the official Election Servers nor implying that the information contained is anything other than a collection of work files to facilitate the testing process. The presence of this computer in the Counting Center and the procedures described above will be submitted for approval as a part of our increased emphasis on transparency and cross verification of data during the election process. If it is determined that the proposed solution is prohibited or introduces an additional risk of release of critical data, this approach will be abandoned.

It is very important that this proposed process receive Secretary of State approval as well as Federal election certification. Therefore, it may not be approved in sufficient time for the 2008 election cycle.

#### Increased Public Transparency of the Election Process

With increased transparency of the election process comes increased security. There will be more eyes observing the process. To further improve transparency, during all future elections

the public will be able to observe the processing of ballots through the security cameras installed at the Division of Elections in the counting center. Beginning in 2008, and actually operational for elections now occurring for other jurisdictions, Pima County will broadcast, via the worldwide web, streaming video of all proceedings in the counting center as ballots are being counted. This will allow anyone with a computer and Internet access to observe the tabulation and counting process. Video will also be transmitted to the Secretary of State's Office pursuant to the 2007 revision to the election laws.

Today, Elections staff, present and new, undergo and clear a criminal background check in order to work within the Elections Division. Due to the security within the vote tabulation facility, the County will request that Party Observers, particularly those who have access to the Counting Rooms, provide appropriate identification sufficient to ensure that they are the persons appointed by the parties to act as observers.

These items will all improve the public transparency of the election process and hence improve election security.

#### **Hand Count Verification of Electronic Tabulation Results**

In the 2006 General Election, to comply with new State law, the election results were verified by a hand count that was conducted and observed by Elections staff and appointees of the various political parties. The votes cast in selected races in nine precincts were counted by hand and 2,863 ballots were counted for the races audited. It should be noted that the result of the hand count for each of these races was essentially identical to the computer tabulated results in all nine precincts.

When the hand counting process was first discussed by the Legislature, it was feared that the requirements would be overly burdensome and cause delay in election results. The last hand count process in November 2006 took approximately 19 hours to complete. Therefore, the hand count did not interfere with the timely reporting of election results. This process is a valid and safe check of electronic vote tabulation devices and provides the best safeguard against vote fraud.

Finally, there has been a great deal of controversy over the touchscreen voting devices. This concern needs to be put into perspective. The voting machines used by Pima County for elections tabulate results from paper ballots, with the exception of the touchscreen voting devices required by Federal law. The touchscreen devices do produce a printed audit trail of votes cast (and cancelled). It should be noted that in the last election wherein 284,935 ballots were cast, only 505 were cast on touchscreen voting devices. Thus, less than 0.0001 percent of voters who appeared at the polls or cast a ballot through early voting used a touchscreen voting device.

### Public Review and Comment on Proposed Security Measures for Elections

Contained within this memorandum are a number of actions that will require the Division of Elections to prepare a security plan for conducting the 2008 election. This draft plan is attached as Attachment 2, and implements the security recommendations and/or modifications for improved security stated in this memorandum. It would be appropriate to ask for public review and comment on these proposals. Therefore, I have directed the Division of Elections to hold four public meetings throughout the County to receive comments and suggestions regarding this elections security plan. In addition, I have provided copies of this memorandum and report to all of the immediate past Party Observers involved in the election tabulation and vote counting process--Republican, Democrat, Libertarian, and Green parties--for their review and comment.

### Replacement of Election Equipment

The present election equipment, the optical scanning devices purchased from Global Elections nearly 12 years ago in the County's transition from punch card voting to paper ballot optical scanning, is old and will need replacement after the 2008 election. This provides the County, as well as any interested party, an opportunity to determine the best and most secure voting system to be employed in future County elections. Any system selected will need to have been certified by both the Federal government and the Arizona Secretary of State. It is likely that the cost of replacing this election equipment will exceed \$5 million. In addition, a more secure election facility is needed in the future. Today our election operations are divided between two locations, and completely separated from the Voter Registration Program of the Recorder's Office where early and conditional ballots must be verified prior to being counted. A new elections center, to be located on Mission Road, should also begin to be planned. I will ask the Bond Advisory Committee to consider the purchase of a new election system and replacement building in a future bond election. For planning purposes, approximately \$10 million should be set aside for this purpose: \$5 million for election systems and equipment, and \$5 million for a secure election building. After the 2008 election, I will ask the Board to appoint a committee to recommend voting equipment and system replacement. The committee will consist of accredited election parties, technical experts, the Recorder, the Registrar of Voters, and the Elections Director.

### Summary

We are pleased with the findings of the Attorney General regarding no criminal wrongdoing on the part of County employees, and no evidence of tampering or altering election results related to the Regional Transportation Authority. Based on the stated concerns of the Attorney General regarding electronic election vulnerability, we will provide him with our proposed policy and procedure revisions regarding our election methodologies in Pima County to ensure the integrity and security of election results. We will also ask the Secretary of State of Arizona to review our new policies and procedures and, as necessary, have said policies and procedures approved by the United States Department of Justice.

The Honorable Chairman and Members, Pima County Board of Supervisors  
**Election Security**  
October 19, 2007  
Page 14

To date, the RTA election ballots remain secure (see Attachment 3). Based on the conclusion of the Attorney General's investigation, the County Attorney will consult with him on ballot destruction pursuant to statute and give notice of such action to allow any party to object to same through appropriate legal proceedings.

Finally, I am attaching, for your information, a recent paper by the Information Technology Innovation Foundation regarding secure electronic voting (Attachment 4).

**Recommendation**

It is recommended the Board accept this report and the proposed modifications to our elections process to improve and enhance security. After appropriate public review and comment on said procedures and policies by the parties and the public, I will schedule this matter for Board direction. All comments received during the public review process will be compiled and provided to the Board, as well as any additional or modified security procedures resulting from this public review.

CHH/jj

Attachments

- c: Brad Nelson, Elections Director  
Dr. John Moffatt, Office of Strategic Technology Planning  
Chris Straub, Chief Civil Deputy County Attorney

# Attachment 1

## Pima County Final Report

**Created For:**

Program Name	PIMA
Final Version	N/A
Client	Pima County, Arizona
Project Lead	Kathleen Kempley

**Created By:**

Project Lead	William Miller
Test Lead	William Miller
Date	July 2007

**Table of Contents:**

Table of Contents:..... 3  
Executive Summary ..... 4  
Summary of Testing..... 8  
    Setup & Planning ..... 8  
    Test Execution ..... 8  
    Test Specifics ..... 10

## Executive Summary

iBeta was approached to perform a quantitative investigation for Pima County, Arizona of a specific Diebold GEMS electronic voting system version and associated hard drive data with regard to alleged vote tampering.

The investigation took place at iBeta's certified testing facility in Aurora Colorado.

iBeta received a sealed Seagate Barracuda 7200, ST3250820A, 250 gigabyte hard drive (s/n 6QEoNTQZ) from Pima County which contained four drive images in Symantec Ghost format.

iBeta staged the images for investigation and analysis using an external IDE to firewire converter. Of these images it was discovered that only two, "Item 1" and "Item 2" contained useable data and "Item 1" was 10.2 gigabytes in size while the "Item 2" image was 204 gigabytes in size.

The target file of the investigation was a Diebold GEMS database backup file called "pima consolidated 051606 EARLY DAY1.gbf" which, according to the audit log of the GEMS software was initially created 05/10/06 at 12:27:27, and then overwritten 05/11/06 at 09:56:30.

The focus of the investigation was to determine the validity of the target file and to look for evidence of tampering. The investigation consisted of several tests:

1. R-Studio scans of the two hard drive images "Item 1" and "Item 2" to look for partial, ghost, or deleted evidence of a different version of the DAY1 file, which came back negative.
2. Date and timestamp checks on all of the available copies of the DAY1 file. This showed some irregularities, but these were later explained away by the troublesome installation and backup of the new GEMS systems on July 20th 2006 and the normal copy and cleanup process on July 27, 2006 in preparation for the next election.
3. CRC comparisons on the five available copies of the DAY1 file, which showed all of the files to be identical across the two systems.
4. CRC comparisons of the Preference tables in the 051606 databases which show that the programming was not altered from the initial "L and A" run for the 051606 event.
5. Backing out the deck data in the DAY1 database to uncover any discrepancies in votes coming in and votes total which would pinpoint the addition of votes. This showed no variation in vote totals.

During testing it was discovered that the GEMS software exhibits fundamental security flaws that make definitive validation of data impossible due to the ease of data and log manipulation from outside the GEMS software itself.

Ultimately, it is the determination of iBeta that the overwriting of the target file can be attributed to human error. iBeta arrives at the "human error" conclusion for two reasons:

- iBeta was unable to detect any manipulation of the 051606 event data across the multiple copies of the data discovered.
- The basis of the investigation is that there are log entries that point to tampering - but it is far easier to remove evidence of tampering from the logs than to actually tamper with the vote totals in the Microsoft Access database that the GEMS software uses. So it does not follow that someone with the knowledge to manipulate the GEMS data would neglect to alter the log file to remove the evidence of the manipulation.

## Summary of Testing

### **Setup & Planning**

The focus of the investigation was to determine the validity of the target file and to look for evidence of tampering.

### **Test Execution**

The investigation consisted of several tests:

1. R-Studio scans of the two hard drive images “Item 1” and “Item 2” to look for partial, ghost, or deleted evidence of a different version of the DAY1 file, which came back negative.
2. Date and timestamp checks on all of the available copies of the DAY1 file. This showed some irregularities, but these were later explained away by the troublesome installation and backup of the new GEMS systems on July 20th 2006.
3. CRC comparisons on the five available copies of the DAY1 file, which showed all of the files to be identical across the two systems.
4. CRC comparisons of the Preference tables in the 051606 databases which show that the programming was not altered from the initial “L and A” run for the 051606 event.
5. Backing out the deck data in the DAY1 database to uncover any discrepancies in votes coming in and votes total which would pinpoint the addition of votes. This showed no variation in vote totals.

## Test Specifics

Test 1 – R-Studio was used to perform a drive-wide scan for deleted, partial, and ghost copy data. While R-Studio did find and recover a great deal of interesting data, none of it was relevant to the investigation at hand.

- This test can be defeated by repeated loading, deleting, and defragmentation of the hard drive, which repeatedly overwrites the deleted data with parts of other files and makes recovery very difficult. Based on iBeta’s observations of the drive images this defeat was not performed.

Test 2 – The date and time stamp checks of the files did turn up what appeared to be evidence of tampering as the files pertinent to the investigation showed a pattern of irregularities in either the date/time created or modified. John Moffatt did some investigation on his end and discovered that there were some issues in the backup, installation, and recovery of data during a July 20<sup>th</sup> 2006 GEMS system update followed by the normal copy and cleanup process on July 27th. This explained the oddities discovered in the file timestamps.

- This test can be defeated by altering the date/time stamp data for the files. There are utilities which will do this, but it appears that this was not done because the files still exhibit non-uniform dates/times. It is unlikely that that defeat was performed because if one of these utilities would have been used, there would have been no alert as all of the date/time stamps would have been sequential to the event - leaving no clue that the files had been altered or replaced.

Test 3 – Ultimately five copies of the target file were discovered or recovered. These five versions were run through a CRC32 process which is used to determine file changes at a bit level. The CRC check returned that all five of the files were identical. The CRC32 value of the target files was “FAD8C70E”.

- It is possible to defeat this test by replacing all of the copies of the target file with a prepared version. It is unlikely that the defeat was employed due to the various modification date/time stamps on the target file – if this defeat had been deployed all of the replacements would have the same create/modify timestamp. Additionally the file residing in multiple locations on multiple computers makes this defeat very difficult as access to the various machines and knowledge of the locations would be required.

Test 4 – John Moffatt proposed a test to determine if the programming used in the 051606 event which compared the “preference” table of the initial L and A test to the various saves of the 051606 event. The compare showed that the programming never changed from the initial L and A event.

- It is possible to defeat this test by way of replacing the preference table in all of the 051606 event data sets after the event was over. This defeat being used is unlikely due to the modify date/time stamps of the original L and A data being from the day preceding the event and every copy of the L and A data exhibiting the same date time stamp. A blanket replace of the entire 051606 event dataset would have had to take place to defeat this test, which encounters the same issues as Test 3.

Test 5 – John Moffatt also proposed a test to determine if any votes were added to the vote totals from an external source. This test used the GEMS software to list the decks for each segment of the 051606 event and when backing those decks out, a total of zero votes remained. This means that all of the votes seen came from the central count scanners or precinct voting machines and not some other source.

- As with other tests it is possible to defeat this test by ensuring that any vote modification keeps the vote totals the same. This means that if you add 1000 votes to one candidate, you subtract a total of 1000 votes from one or more other candidates. This defeat has a low probability of being deployed based on the fact that it only works for the total number of votes. Any report run that shows the votes at a precinct level, when compared to a total votes report, will show the data modification.

## Attachment 2



# Pima County Division of Elections

## Security Plan

September 2007

# Table of Contents

<b>Introduction</b>	3
<b>Guiding Laws, Procedures and Policies</b>	4
Open and Transparent Election Environment	6
Physical and Personnel Security	7
- Physical	
- Personnel	
Legal and Procedural Security	9
- Ballot Programming and Election Administration	
- Logic and Accuracy Test	
- Two Person Rule	
- Security of Voting Equipment to/from the Polls	
- Early Ballot Tabulation	
- Post Election Audits	
- Two Person Rule	
Technical and System Security	11
- General	
- Network	
- GEMS specific	
<b>Responsibilities</b>	15
<b>Summary</b>	16

## Introduction

Security of the voting process is paramount to ensuring the public's confidence in elections. The Pima County Division of Elections Security Plan is intended to provide a general overview of tasks as well as roles and responsibilities of selected offices and agencies in maintaining the security of the voting process.

In general, election systems are almost universally composed of two (2) major independent systems that provide functionally for election tabulation and voter registration. In Pima County, the responsibility for maintaining the voter registration system belongs to the County Recorder. The responsibility for election tabulation rests with the Pima County Division of Elections. This security plan will only address the election tabulation function. The system used in Pima County to conduct ballot tabulation is the Global Election Management System (GEMS).

The Pima County Division of Elections Director has the responsibility to ensure that all employees working in elections are working in a secure environment. In addition, it is crucial that every eligible ballot is counted and that the voting process is secure. The Elections Director or their designee is responsible for the overall coordination of security concerns during elections. That position will be clearly identified to all employees as the primary point of coordination of security issues.

Effective security does not depend nor rely on a single process, feature, or policy. Effective security requires a number of interrelated processes, systems, and policies that compliment and build on each other. The systems, processes and policies that comprise the layers of security for Pima County Elections are represented on page 5 in figure 1.

These multiple layers of security systems, processes, and/or procedures ensure that elections are not inappropriately influenced. Involving external stakeholders such as the media, political party observers, the Arizona Secretary of State and the public provides transparency and is integral to the detection of problems with the elections process. The physical and personnel security measures which have been implemented ensure that only authorized individuals are allowed to access critical election spaces, materials, technical systems and ballots. Elections staff and seasonal employees are trained in elections processes and procedures designed to ensure the security and integrity of the election process. These elections processes are audited and reviewed throughout with many checkpoints for accuracy. This layered approach ensures that if one or even two layers are compromised, bypassed or proven ineffective the security and integrity of the election process is still preserved.

The contents of this Plan are structured to parallel the layers of the security shown in figure 1: open and transparent election environment, physical and

personnel security, legal and procedural security and technical and systems security.

This Plan is a dynamic, living document that will be reviewed and updated as significant security issues arise or situations change. After every election, Pima County Elections Staff review the lessons learned from that election and make adjustments to the processes, procedures and systems to improve the effectiveness of operations and security. The Pima County Elections Staff also monitors the experiences in other jurisdictions and scrutinizes studies and reviews by third parties. They then adjust policies and procedures in order to avoid weaknesses experienced or identified by others.

All employees who work in elections or who have a role in elections security share a responsibility to ensure that our elections remain secure and that they are conducted with the utmost integrity. To this end, all new employees are required to read and become familiar with the Security Plan as well as any implementation procedures that are relevant to their work areas. All employees will be briefed periodically with the key aspects of this plan. All employees, not just supervisors, are encouraged to suggest ways to improve the security of the election process. Pima County Elections also welcomes suggestions from political parties, and other observers on ways to enhance system security.

## **Guiding Laws, Procedures, Policies and Studies**

Laws, procedures, policies and studies that apply to elections include:

- Help America Vote Act of 2002 (HAVA): 42 U.S.C. 15301 to 15545
- Arizona Revised Statutes Title 16
- Arizona Electronic Voting System Instructions and Procedures Manual
- Pima County Administrative Procedure 13-17
- Quick Start Management Guide for Voting System Security, United States Election Assistance Commission
- California Secretary of State - University of California Red Team Report 2007
- Florida State University Software Review and Security Analysis of the Diebold Voting Machine Software, August 2007
- Brennan Center for Justice Report, "The Machinery of Democracy: Protecting Elections in an Electronic World" 2006

# Layers of Election Security

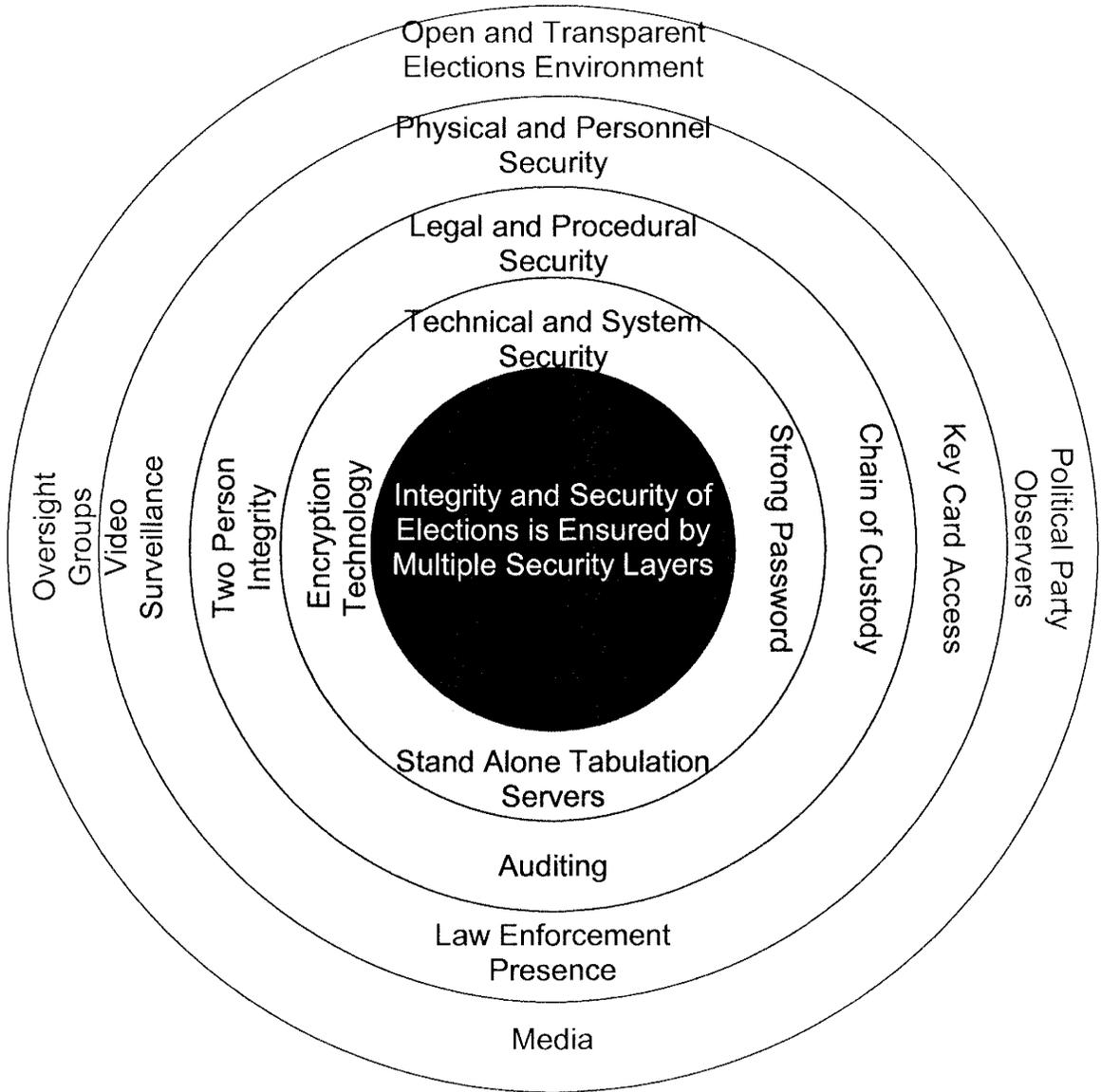


Figure 1

## Open and Transparent Election Environment

Administering elections is a monumental responsibility and one which openness and transparency are essential to gaining and retaining public trust in government. It is the process by which citizens of a democratic republic choose their political leaders, and in the State of Arizona, it is a system in which the electorate through the process of initiative and referenda can directly make law. In any other system or process, it would likely be considered contradictory to require openness and transparency around a set of processes while at the same time restricting access and ensuring strong security, but this is exactly what election administrators across the nation must accomplish. This involves a variety of concepts that combine accountability, transparency, security and accuracy, to enable access, foster openness, and preserve the integrity of the process. In Pima County, this is achieved through:

- Building Infrastructure Design and Access

Open floor plans, viewing windows, public monitors, exposed and color coded network cabling, surveillance cameras and optimized viewing areas are all design elements that facilitate transparency. Additionally, starting in 2008, Pima County will provide streaming video, via the World Wide Web, of proceedings in the tabulation center as ballots are being counted.

- Public/Political Party Observers

The ability for observation of the tabulation process is grounded in State law. The responsibility for providing political party observers is with the Chair of the county political parties. Any other observers are public observers and are covered under a separate law. It is the responsibility of the Pima County Elections Director to designate where the observers are to be stationed and to approve the assignment of the observers.

- Public disclosure of records

- Media access

- Video broadcast of ballot tabulation on the web

## Physical and Personnel Security

The first line of defense against unauthorized access, tampering with election results, or other illicit activity is physical and personnel security. If unauthorized individuals cannot get to areas or systems where election activity takes place, they are unable to tamper with or affect the process. Ensuring that Elections personnel do not inappropriately influence or tamper results starts with selecting highly trustworthy individuals and through additional layers of checks and balances to ensure they do not have the opportunity or inclination to create harm to the process.

### Physical

Access Control: Access to the election office and work areas is limited. The physical layout of the administrative office is such that people entering the office pass through a motion detection device that sets off an audible alarm. Staff then greets visitors to the office and escort authorized personnel into restricted areas.

At the Election Technical Center, located at the Mission Road complex, sixteen (16) video surveillance cameras are set up at strategic locations to provide staff with the ability to observe restricted areas inside and outside of the facility. Select doors can only be opened with electronic key cards that provide a log of who gained access to restricted areas and the date and time of the action. These same doors are equipped with switches that sound an alarm if the door is held open. All video is recorded 24/7 and archived for up to 24 months for post-event review.

Because of its use in the tabulation of election results, GEMS at the Election Technical Center receives extra security. GEMS tabulation servers are housed in a secured, locked environment, which can only be accessed using electronic key cards by an authorized entrant. This secured, locked room serves as the location where the election database is prepared and where ballot layout and design assurance is performed. Only authorized election personnel are permitted to enter the secured server room unless escorted by an authorized entrant. GEMS server room access is given only to qualified and authorized personnel. All persons entering the secured room must sign a manual log stating time in and out and the purpose of their visit.

Uniformed Security Presence: Commissioned law enforcement officers in uniform are assigned to the Election Technical Center and stationed at key locations to protect entry and exit points as well as acting as additional observers of the processes, staff, observers and visitors on Election Day.

Accessible Voting Units and Optical Scan Voting Devices: Accessible voting units and precinct county optical scan voting equipment are stored in a secured limited access warehouse facility. Voter access, supervisor and administrator cards for

the accessible voting units in addition to memory cards for each unit are secured in a locked room with limited access. The outer case of each of these units is sealed with a minimum of two uniquely numbered, tamper-evident seals. Each of the units, in addition to the associated components is tracked with an electronic inventory system to maintain a documented chain of custody.

These measures enable it to be detected if a unit has been tampered with by either a poll worker, voter or election staff member at anytime. By maintaining a documented chain of custody, we can detect who may have tampered with a device or when it would have likely occurred.

Servers and Electronic Media: All sensitive equipment and supplies are secured in locked cabinets and/or fire proof safes contained in a controlled access room, under 24/7 video surveillance.

Locking rack mount cabinets for all GEMS servers have been installed. When not in use, the color coded network cables for the servers are disconnected and the keyboard and mouse are locked and sealed within the cabinet. A log is maintained to record seal numbers and access to the interior of the cabinet. USB ports on the servers have been disabled. Security cameras continuously monitor the front and rear of the server cabinet to record any access, or attempted access. On Election Day testing for the presence of wireless connectivity is performed at randomly selected precincts and at the Technical Center. These security features deter any attempt to “plug” into the system, or to maliciously shut the system down.

### **Personnel**

Employee and observers who work during elections must practice a high level of security. Only authorized personnel with a specific need for access are to be allowed in sensitive areas. Others will be accompanied by an escort in sensitive areas at all times.

Upon the implementation of this plan, criminal background checks will be required for all employees and observers who work in areas of heightened security. Heightened security areas will be designated by the Elections Director.

All personnel, observers and visitors are required to wear visible credentials at all times.

# **Legal and Procedural Security**

## **Ballot Programming and Election Administration**

Members of Pima County Elections Staff are responsible for ballot layout and the programming of all elections administered by Pima County (no vendors). The process of ballot layout and programming takes place in county election offices under camera surveillance with controlled and tracked access.

The “live election database” used for tabulating results and certifying the election is created by and under the control of elections staff at all times. Contents of the databases related to programming, ballot design and report formatting are repeatedly subjected Hash Total comparison beginning with the Official Logic and Accuracy Test through canvass of election in order to detect any alterations.

## **Logic and Accuracy Tests**

Before every election, the entire vote tabulation system, including each voting unit, undergoes rigorous logic and accuracy testing. The process checks that each machine properly records, counts and tabulates results correctly. The tabulation system and each voting machine must pass logic and accuracy testing before it is “set” for the election. Then the memory card for each unit is sealed in the unit to prevent tampering. An extensive audit trail is maintained of this process, including detailed checklists.

In the past, Pima County has invited the political parties to actively participate in the logic and accuracy test of the equipment prior to partisan elections. These “party tests” have provided the ability for the parties to receive and mark test ballots (from precincts of their choosing) and subsequently process the ballots through Pima County’s tabulation equipment.

(Pima County is the only county in Arizona that provides this level of political party involvement in the logic and accuracy test process).

## **Two Person Rule**

To ensure against the possibility of the illegal manipulation of voted ballots, any time voted ballots are not in a sealed container in a secured area during the election process, they shall be in the presence of no fewer than two observers who shall not be of the same political party. Ballot processing shall not be curtailed if the requested observers have not been provided. The Pima County Elections Director, or their designee, may assign pairs of observers at times other than as prescribed above when in the Director’s opinion, it is warranted.

## **Security of Voting Equipment and Ballots to and from the Polls**

Pima County utilizes numbered tamper-evident seals on all voting equipment and ballot storage devices. Dual tamper-evident numbered seals are to be affixed across the seam at which two halves of the exterior case of the voting unit joins. The slots/doors for the flash memory cards are also sealed over each door/slot. The sealed voting devices are then locked and sealed into individual steel cages for transport to the polls. All seals shall be verified by at least two election officials at the polls prior to the start of voting. Pima County shall maintain a written log that records each seal number that is assigned to each voting unit. Any breach of control over a sealed item shall require the immediate notification of Pima County Elections.

After the polls close, the poll workers, one from each party, shall return all voting equipment and voted ballots in sealed/numbered containers to a receiving center. At each receiving center, the numbered seals shall once again be checked and a receipt is issued to the poll workers.

From the receiving centers the equipment is returned to the Election Division where the seals shall be checked again, under political party observation.

## **Early Ballot Tabulation**

The tabulation of early ballots can begin no sooner than seven days prior to Election Day. Early ballots are tabulated under public and/or political party observation. During the administration of partisan elections, political party representatives designate batches of early ballots subject to hand count audit prior to official canvass of the election. Political parties will be notified as to the date and time of early ballot processing. Political parties providing observers for the early ballot process must provide the names of the observers in time for a background check to be performed. Unless approved by the Elections Director or their designee, only one observer from each political party is allowed in the counting room at any time. By law, summary reports are generated for each batch of ballots selected by the political parties. The generation of summary reports, other than those prescribed by law, is prohibited.

## **Post Election Audits**

Arizona State Law requires a hand count/audit of randomly selected precinct ballots and randomly selected early ballots for the presidential preference election, primary and general elections. Random audits are done to catch fraud or mistakes in the vote totals. By law, the audited ballots and contests are randomly selected by the political parties and the entire auditing process is open to political party observation.

**Post Election Audits (continued)**

State law does not provide for the hand count/audits for countywide nonpartisan elections. Nor does State law provide for political party observation of countywide nonpartisan elections. However, Pima County intends to perform hand count/audits for countywide nonpartisan elections in the future. The political parties and civic groups will be encouraged to participate in and observe the process.

## **Technical and System Security**

The technical security features include the computer security components necessary to ensure data integrity and security of technical systems, as well as prevent unauthorized access into election systems through the use of best practice tools, processes, procedures and policies. Proper management of the technical security environment for the system is critical to prevent any unauthorized access to elections systems and data, even if an unauthorized individual has circumvented other layers of security. Technical security is the last barrier to someone intent on malicious action, though the other layers of security would facilitate detection (e.g. armed Sheriff's deputy security, camera surveillance, and key card access records.)

### **Split passwords**

Pima County Election Staff members responsible for election programming cannot access the tabulation program without a proper password. To better ensure election integrity, no staff member has knowledge of the complete password. A maximum of two staff members know the first part of the two part password. A maximum of two staff members know the second part of the password. The complete password shall be at least sixteen characters long and comprised of a mix of case sensitive letters, numbers and symbols.

Once staff members gain access to the election program they must enter an additional split password. A maximum of two staff members know the first part of the two part password. A maximum of two staff members know the second part of the password. The complete password shall be at least eight characters long and comprised of a mix of case sensitive letters, numbers and symbols.

Passwords are changed at least once a year.

### **Hash Codes**

Before installing or upgrading any software on any system involved with collecting and tabulating votes, Pima County Elections will verify the software received is the same as that certified at the Federal level through the use of hash code testing. In addition to testing software on receipt, Pima County Elections will work towards periodic hash code testing of a percentage of randomly selected devices for each election to verify that software installed is the certified version and has not been tampered with. Pima County Elections is instituting the practice of hash code testing the GEMS application at the start of each day to prove that the application software is the certified version and it has not been tampered with. Additionally, the database will be hash code tested at the conclusion of each day's operations and again at the start of the following day's operations to prove that the database has not been tampered with. The database will also be hash code tested upon the official canvass of the election so that any future

reporting from the database can be certified to have come from the final official election database.

Hash code testing validates that the ballot tabulation software is exactly the same as the software tested and analyzed in the federal and state certification process, and provides election administrators and observers in Pima County with the assurances needed to be certain that no changes to applications or other critical files have occurred.

(A hash code is a large number computed using a standard algorithm from the entire string of bits that form the file. The hash code is computed in such a way that if one bit in the file is changed, a completely different hash code is produced).

### **Restrictions**

There are no wireless devices used within the tabulation system or with any voting device. Pima County has, and will continue to employ, wireless sniffers to detect signals at the Counting Center and at randomly selected polling places on Election Day.

To further ensure security, the following devices are prohibited in the Counting Room:

Any USB storage key - "jump drive"

Laptop or tablet computer

Laptop or tablet computer with a wireless transmission capability turned on in adjacent rooms.

#### **Specific GEMS restrictions:**

GEMS is a comprehensive system used to design and build ballots, tabulate central count ballots, accumulate results from the polls and early voting and report election results.

GEMS is administered solely by Pima County Division of Elections personnel.

GEMS is installed on two servers (one primary and one back up). Neither of these servers is connected to an external network and is prohibited from being so. Any sharing of data files (to the website or Secretary of State) is done using portable media, such as a CD. A network internal to the Counting Room exists to connect printers, AccuVote ballot scanners and TSx touch screens as well as the two servers. The use of wireless networking devices on any GEMS server is strictly prohibited.

To ensure the security and integrity of tabulated results, several additional steps are taken when ceasing daily operations and when resuming operations on a subsequent day or after a break in processing. A Cards

Cast report will be produced when ceasing operations as well as resuming operations. The two reports will be reviewed by Election Staff and political observers to ensure the cards cast when resuming is the same as when operations ceased. Party observers will date and sign this report attesting to the fact that there was no change. This step will be taken any time there is an interruption in operations such as for lunch, breaks, to back up / restore the database, etc. At the cessation of daily activities, the GEMS database will be backed up to at least two new shrink wrapped CDs – one for on-site storage and one for off-site storage. The CDs will be sealed and initialed by observers. Before resuming operations on a subsequent day, the database residing on the server will be hashed once again. The hash code from the previous CD and the hash from the live database will be compared by Election Staff and party observers to ensure no change. Matching hash codes indicates that there was no change to the database.

#### Audit Logs

Before the Logic and Accuracy Test, the Window's audit log for the tabulation server will be cleared. During the tabulation process, these logs will not be cleared. After the election is officially canvassed, the logs will be printed and kept with other election records for 6 to 24 months depending on the type of election administered.

#### Power Supply

The GEMS server is served by an uninterruptible power supply (UPS) to facilitate an orderly shutdown and securing of the GEMS database including procedures for Cards Cast Reports, hash coding and backup to CD. The UPS will be tested at least two times per year.

#### Time Synchronization

The clock(s) on the GEMS servers will be set and synchronized prior to each election.

The GEMS tabulation system and tabulation database is the most secured system in use by Pima County Elections because of its use in tabulating and reporting election results. The hardened physical security measures significantly restrict unauthorized access, and since the tabulation hardware is not networked to any other system, physical access to the server would be required in order to attempt any unauthorized access.

## RESPONSIBILITIES

Elections require participation and responsibility at all levels of government. A list of responsibilities below is not intended to be exhaustive but does provide an overview for various aspects of the election process.

US Government – Provides certification of voting tabulation systems

Arizona Office of Secretary of State – provides procedures and advisories; provides state certification of voting tabulation systems

Pima County Government – Oversees federal, state and local elections for Pima County.

Pima County Recorder

Maintains the Pima County List of Registered Voters and administers Early Voting

Pima County Elections

On behalf of the Pima County Board of Supervisors, administers all federal, state and local elections in Pima County.

Pima County Sheriffs Office

Provides security at Pima County Election Facilities and provides deputies to act as couriers for election material(s) on Election Night.

Pima County Facilities Management

Provides security enhancements for Pima County facilities used for election tabulation.

Pima County Information Technology

Assists with Hash Code Check(s), Assists with Video Surveillance, provides Touch Screen Voting Equipment Troubleshooters on Election Day and provides cyber security by operating wireless sniffers on Election Day at the Counting Center and selected polling places.

Pima County Attorney

Provides legal counsel

## SUMMARY

Effective security does not rely on a single process, feature or policy. Effective security requires a number of interrelated processes, systems and policies to compliment and build on each other. The systems, processes and policies that comprise layers of security for Pima County Elections are represented in detail throughout this plan, and illustrated graphically on page 5, Figure 1.

These multiple layers of security systems and processes and/or procedures ensure that elections are not inappropriately influenced. External stakeholders such as the media, candidates, political parties, the Arizona Secretary of State and members of the public provide transparency and are integral to the detection of problems with the election process. The physical and personnel security measures which have been implemented ensure that only authorized individuals are allowed access to the critical election spaces, materials technical systems and ballots. Election staff members are trained in election processes and procedures designed to ensure the security and integrity of the election process. The elections processes are audited and reviewed throughout with many check points for accuracy. The layered approach ensures that if one or two layers are comprised, bypassed or proven ineffective, the security and integrity of the election process is still preserved.

This Security Plan details many safeguards in place to protect elections in Pima County. Many of the safeguards are not unique to Pima County Elections; they are deployed throughout election agencies across the state and country. Although many of the safeguards in place today were implemented before they became recognized best practices or recommendations by outside stakeholders, they are nonetheless based on lessons learned internally, through observation of others, or were existing legal requirements.

The security of elections in Pima County is also the result of a genuine commitment by election officials to cooperate with outside stakeholders. Local stakeholder recommendations for improvement have proved beneficial and many have been implemented. The Elections Division continues to be receptive to recommendations made by all interested parties in so much as they positively contribute to election security, election integrity, public trust, openness, transparency and accountability.

## Attachment 3



---

# MEMORANDUM

---

Date: May 18, 2007

To: Brad Nelson  
Elections Director

From: C.H. Huckelberry  
County Administrator

A handwritten signature in black ink, appearing to read "CHH", is written over the printed name "C.H. Huckelberry".

Re: Allegations of Election Fraud

I was advised via e-mail (attached) last evening that the attorney representing the Democratic Party, Mr. Bill Risner, has made very specific allegations of election fraud against the Division of Elections as it relates to the Regional Transportation Half Cent Sales Tax Election. In essence, Mr. Risner, in a conversation with Deputy County Attorney Karen Friar, indicated that "Bryan Crane flipped the RTA election," simply meaning that Mr. Crane electronically manipulated the vote results of the election. This is a very serious allegation and requires investigation. I have asked the County Attorney to request an outside and independent investigation of this allegation.

In addition, we need to protect, secure and seal any information related to Division of Elections actions regarding not only the November 2006 election, but also the May 2006 RTA election. Even though the ballots/returns for the RTA election are eligible for destruction pursuant to A.R.S. 16-624, please ensure that all ballot and election returns for this election now stored at our contract records management facility are retained, with specific instructions not to destroy these documents. Further, since the allegations are against an official of the Division of Elections, it would be appropriate to ensure that there are very specific instructions approved by the County Attorney to the contract records management firm that Division of Elections personnel, including you as the Director, and myself as your immediate supervisor, are not granted any independent access to said records without independent oversight and supervision. This will ensure that County Administration and the Division of Elections cannot be accused of having independent access to the ballots and altering same.

In addition, there should be appropriate duplicate information obtained from the Elections tabulation computers and other electronic records copied and again placed with an independent third party. We need to take action to ensure that all documentation, ballots, electronic files and other information sources are secured so they cannot be altered, tampered with or destroyed as I am sure an accurate and independent review of this material will verify that the allegations made by Mr. Risner are absolutely untrue.

CHH/jj  
Attachment

c: Dr. John Moffatt, Office of Strategic Technology Planning  
Christopher Straub, Chief Civil Deputy County Attorney  
Karen Friar, Deputy County Attorney, Civil Division

## Julie Johnson

**From:** John Moffatt  
**Sent:** Thursday, May 17, 2007 9:23 PM  
**To:** Chuck Huckelberry  
**Subject:** Risner

I just spoke with Karen Friar. In her discussions with Bill Risner today, he alleged that they have proof that the RTA Election was "Flipped by a County staff member." They will discuss this with you at your normal meeting tomorrow. I have to meet Gilbert Ramos at 8:00 but that should take only a few minutes, then I will be in to discuss this prior to 9:00 and/or will attend the 9:00 meeting if you wish.

I have repeatedly told Risner that if he had allegations of impropriety that I would gladly place him directly in touch with you or that if there was illegal activity, that the investigation should immediately be turned over to Law Enforcement. I offered to involve them as soon as the Democratic Party felt that there was such a problem. Until today, they have never made this allegation to the best of my knowledge.

Karen and I discussed involving the Attorney General immediately. They will review this with you at the meeting.

We also discussed placing the information they are requesting in Escrow with the Court being the only one to order its release to anyone. Given the allegation that has surfaced, it is appropriate to get a copy of the information off of the Election Tabulation computers and placed in the hands of an independent agency. As I am also accused of covering this up, we need to get someone like Bill Allaire, or even an independent third party like the Attorney General's staff to oversee the extraction of this information.

See you tomorrow!

*John Moffatt*

John H. Moffatt, Ph.D.  
Office of Strategic Technical Planning  
520-740-8463  
john.moffatt@pima.gov

## Attachment 4

# Stop the Presses: How Paper Trails Fail to Secure e-Voting

BY DANIEL CASTRO<sup>1</sup> | SEPTEMBER, 2007

*A federal mandate to require voter-verified paper audit trails for all electronic voting machines would prevent the use of innovative voting technology that offers more security, transparency, and reliability than paper-based audit trails alone.*

Americans trust computers to run critical applications in fields such as banking, medicine, and aviation, but a growing technophobic movement believes that no computer can be trusted for electronic voting. Members of this movement claim that in order to have secure elections, Americans must revert to paper ballots. Such claims are not only incorrect but attack the very foundation of our digital society, which is based on the knowledge that information can be reasonably secured. Clearly, no system with a human element—including electronic and non-electronic voting machines—is error-proof, and specific versions of certain voting machines have security weaknesses. Neither of these facts, however, should be taken as a universal indictment of e-voting.

Direct recording electronic (DRE) voting machines are electronic machines, similar to ATMs, that let voters view ballots on a screen and make choices using an input device such as buttons or a touchscreen. Some opponents of electronic voting are lobbying for legislation that would require so-called “voter-verified paper audit trails” for all DRE voting machines. The purpose of the paper audit trails would be to provide proof that the DRE voting machines functioned correctly. Unfortunately, as discussed in this report, paper audit trails for DRE voting machines have several shortcomings. They do

not provide complete security to voters and they increase costs and risks. Furthermore, requiring voter-verified paper audit trails would prevent the use of innovative voting technology that offers voters more security, transparency, and reliability than can be delivered with paper audit trails alone.

Congress is now considering legislation that would mandate that all DRE voting machines have voter-verified paper audit trails, and many states will vote on similar legislation this year. We believe it is time for the debate on e-voting technology to move beyond a discussion of

paper audit trails. To restore voter confidence and promote secure election technology in the United States by ensuring that states can continue to improve their voting systems, we recommend the following:

- Congress and the states should allow the use of fully electronic ballots, not restrict electronic voting systems to those that create paper ballots.
- Congress and the states should require that future voting machines have verifiable audit trails, not require machines that create verifiable paper audit trails.
- Congress should provide funding for the U.S. Election Assistance Commission to issue grants for developing secure cryptographic voting protocols and for pilot testing of new voting technology.

#### ELECTIONS IN THE UNITED STATES

Voting machines used in U.S. elections must satisfy many requirements. First, virtually every state requires a secret (or Australian) ballot, so the machines must allow secret ballots. In the late 1800s, election officials in the United States introduced the secret ballot as an improvement to voice votes and party tickets.<sup>2</sup> A secret ballot has the following properties: it must contain the names of all candidates and the text of all propositions; it must be distributed only at the polls; and it must be marked in secret.<sup>3</sup> Maintaining the confidentiality of voters' selections helps election officials limit voter coercion and vote selling. Second, elections must be secure, so the integrity of the voting machines and ballots must be maintained at all times, and voters must be permitted to vote only once and only in the elections in which they are eligible. Third, elections must be auditable so that election officials can verify that the results of the election are accurate.<sup>4</sup>

One difficulty with administering secure and confidential elections in the United States is that there is no trusted third party. A trusted third party is an entity that facilitates transactions between two entities. If the two entities trust a third party, they can use this trust to secure their own interactions. Thus, for example, a notary public provides third-party verification for authenticating and verifying a signature. In theory, election administrators are trusted third parties; in fact,

however, many of these individuals are either elected officials or political appointees, so they have a conflict of interest. In the 1920s, one of the primary reasons for moving from paper ballots to mechanized voting was to eliminate the reliance on human participants.<sup>5</sup>

---

*The integrity of a paper ballot still depends on physical security controls. Historically, failed security controls have led to modified, spoiled, and stolen ballots, as well as to stuffed ballot boxes.*

---

Voting machines used in U.S. elections must also adhere to a number of usability requirements. First, a number of federal laws, including the Americans with Disabilities Act, the Voting Rights Act of 1965 (as amended in 1982), the Voting Accessibility for the Elderly and Handicapped Act of 1984, and the Help America Vote Act of 2002, guarantee the right of disabled individuals to participate in elections. Second, in many precincts, election material must be available in multiple languages.<sup>6</sup> Third, many states require that voters be allowed to include write-in votes. Fourth, states are required to allow a voter to cast a provisional ballot even if the voter appears to be ineligible to vote. Fifth, some states require ballot rotation so that a candidate cannot gain an advantage from the placement of his or her name on the ballot. Finally, some elections use preferential voting, where voters rank their chosen candidates to avoid the need for a runoff election.

#### THE PROBLEM WITH PAPER BALLOTS

Voting technology has evolved and improved over time as a result of several technical advances. Before the mechanization of the industrial revolution, voters relied on paper ballots. In the early 1900s, election officials overwhelmingly decided to use mechanical voting machines after witnessing years of fraud and error with paper ballots.<sup>7</sup> Advertisements proclaimed that mechanical lever machines were completely secure because they did not rely on humans to hand count each vote. When voters pulled the lever, their vote was immediately cast and tallied. Voters no longer had to wonder if their ballot would be lost, misinterpreted, or considered a spoiled ballot.<sup>8</sup>

In the late 1950s, as mainframe computers were developed, computerized vote processing was introduced as a more efficient means of vote tallying. By 1982, more than half of the American electorate was using punch-card voting machines, which had replaced lever machines as the dominant voting technology. These machines used the punch-card paper ballots made infamous during the controversial 2000 U.S. presidential election.<sup>9</sup>

As history has repeatedly shown, traditional paper ballots are not a secure form of voting. Although some current legislation calls for “durable paper ballots,” the term durable is misleading because such ballots are required to withstand only basic handling.<sup>10</sup> The integrity of a paper ballot still depends on physical secu-

rity controls. Historically, failed security controls have led to modified, spoiled, and stolen ballots, as well as to stuffed ballot boxes. The story of how Lyndon B. Johnson used paper ballots to commit fraud demonstrates the weaknesses of paper ballots.

Another problem with paper ballots is that voters may add extraneous marks to identify their ballot to a third party. If their ballot can be identified by a third party, such as an election official, then voters can engage in vote selling. A common countermeasure to this tactic is to consider any ballot with extraneous marks as a spoiled ballot. The downside to this countermeasure is that it is easy for election officials to spoil a ballot, especially during a manual recount.

### BOX 1: HOW LBJ USED PAPER BALLOTS TO STEAL AN ELECTION<sup>11</sup>

The story of Lyndon Johnson's election in 1948 to the U.S. Senate illustrates how paper ballots enabled fraud and corruption in American elections. Johnson first ran for the U.S. Senate in 1941, when Texas held a special election to fill the seat of a recently deceased senator. Johnson was a 32-year-old congressman at the time, and many thought he would soon become the youngest senator in the country. As Election Day approached, all of the polls showed Johnson in the lead against his opponent Governor Pappy O'Daniel.

Confident that he would win, Johnson told the precinct bosses he controlled that they could report their results immediately. This decision proved to be a critical mistake. Conventional wisdom at the time said that candidates should always wait until the last minute to report the totals in the precincts they controlled. This prevented their opponents from learning how many votes they needed to add to win the election. When Johnson allowed his men to call in their totals early, he gave O'Daniel all the advantage he needed. While Johnson celebrated what he thought was a certain victory, O'Daniel's campaign quickly had their own men add more votes to their tallies.

The next day Johnson was shocked when he discovered that he had lost the first election of his life. He would not forget this defeat or the means by which he lost. Seven years later, in his second run for the Senate, Johnson faced the popular former governor Coke Stevenson in the Texas Democratic state primary. Johnson waged an aggressive and expensive campaign against his opponent, but Stevenson won a plurality and beat Johnson by 70,000 votes. He did not win a majority, so a runoff election was scheduled.

Although Johnson slowly narrowed the gap in the polls between Stevenson and himself, as the runoff election date grew closer, Johnson's campaign aides realized Stevenson still maintained a solid lead. Unable to obtain the remaining votes through conventional methods, Johnson's campaign directed their funds to the political machines that controlled the minority voting blocs along the border and in San Antonio. These investments paid off. For example, in the notoriously corrupt Duval County controlled by George B. Parr, not only did Johnson receive an overwhelming 99 percent of the vote, but the county recorded a 99.6 percent turnout of all registered voters, a record level of civic participation. Unfortunately for Johnson, on election night, Stevenson still led by 854 votes.

Stevenson would not remain in the lead for long. Johnson and his campaign aides worked the phones over the next few days to persuade local leaders to “find” a few more votes for Johnson. In many counties this was impossible. In

*(continued)*

### VOTING MACHINE REFORM AFTER THE 2000 PRESIDENTIAL ELECTION

After the controversial 2000 U.S. presidential election, many voters decried the inaccurate and inconsistent voting systems used throughout the country and demanded change. Congress responded with the Help America Vote Act (HAVA) of 2002, which was intended to help states modernize their aging electromechanical voting systems.<sup>13</sup> HAVA includes the following provisions:

- establish the U.S. Election Assistance Commission (EAC), an independent federal agency tasked with creating voluntary voting system guidelines and minimum election administration standards for states and local government
- provide nearly \$4 billion in funding for states to replace their lever and punch-card voting machines with more modern and more accessible voting systems<sup>14</sup>
- require states to implement a single, uniform, state-wide, computerized voter registration database
- mandate that in the event a voter appears to be ineligible to vote, the voter may still cast a provisional ballot if he or she believes this ineligibility to be a mistake
- mandate that voters who register to vote by mail or who have never voted before in a federal election must provide either photo identification or other documented proof of their name and address

#### BOX 1 (continued)

San Antonio, Johnson had been able to buy almost 10,000 votes, but since the city voted by machine, once the mechanical tallies were certified, additional votes could not be added. Over the next few days, as precincts checked their votes, however, the tally slowly changed, and Stevenson's lead dropped to a handful of votes. Finally, around noon on the sixth day after the election, the Democratic Executive Committee of Jim Wells County called the Election Bureau to report an amended return. The south Texas county, under the domain of the Parr political machine, claimed that they had misreported the figure for Johnson as 765 votes when the correct total was 965 votes. After all the dust settled, Johnson had won the election by a margin of 87 votes.

Vote buying had long been a part of Texas politics, but Stevenson declared that these additional 200 votes represented "the first time that the manipulators of the voting in these counties were not content with all-out bloc voting, but re-opened the boxes in secret long after the election had closed and stuffed them with a directed number of ballots."<sup>12</sup> Furious at the audacity of Johnson's vote stealing, Stevenson decided to prove his allegations of ballot stuffing and headed to Alice, the county seat of Jim Wells County, with Frank Hamer, the legendary Texas Ranger best known for tracking down and killing Bonnie and Clyde.

With the most feared lawman in the Lone Star State at his side, Stevenson marched past George Parr's armed gunmen and demanded to see the poll list held in the safe of the Texas State Bank of Alice. The poll list contained the names of every voter as they signed in to vote. Here Stevenson found the evidence he was seeking: the last 200 names on the poll list been added in a different color ink, in a single handwriting and in alphabetical order.

His lawyers spent the next weeks rounding up these voters who later testified under oath in federal court that they had not voted in the election. Armed with this evidence, along with evidence of voter fraud throughout the state, Stevenson tried desperately to block the state from certifying Johnson as the Democratic Party's nominee. He eventually took the dispute all the way to the U.S. Supreme Court, but after all copies of the poll list disappeared, the federal court ruled it did not have jurisdiction.

In the end, Johnson prevailed and eventually headed to the U.S. Senate with the sobriquet "Landslide Lyndon."

Although HAVA provided nearly \$4 billion in funding for states to upgrade their voting systems, it did not mandate that the states use a specific voting technology. States could choose any voting technology, including DRE, optical scan, and lever voting machines, that met certain specified functional requirements (e.g., voting machines must be accessible for individuals with disabilities and have an audit capacity).

HAVA also mandated that EAC provide grants for pilot programs to test new technology in voting systems and grants for research and development “to improve the quality, reliability, accuracy, accessibility, affordability, and security of voting equipment, election systems, and voting technology.”<sup>15</sup> HAVA authorized EAC to provide \$10 million for pilot programs and \$20 million for improving voting technology. Since 2002, Congress has failed to appropriate the \$30 million to fund these grants authorized by HAVA.<sup>16</sup> Recently proposed legislation would provide approximately \$1 billion in additional funding for states to procure new DRE voting machines with printers but would not first appropriate funds to develop and pilot test new voting technology. This legislation, if adopted, would force many states to discard their existing equipment if their current DRE voting machines cannot be upgraded to include a printer.

---

*HAVA authorized EAC to provide \$10 million for pilot programs and \$20 million for improving voting technology.*

*Since 2002, Congress has failed to appropriate the \$30 million to fund these grants authorized by HAVA.<sup>16</sup>*

---

Many of the reforms introduced by HAVA have strengthened the U.S. election system. The provisional ballot requirement has helped prevent many citizens from being denied the right to vote at the polls. In the 2004 elections, for example, 1.9 million voters nationwide cast provisional ballots; approximately 1.2 million (64.5 percent) of those provisional ballots were counted.<sup>17</sup> In addition, HAVA has increased the integrity of our elections by strengthening statewide voter registration databases.

HAVA authorized EAC to develop a national program to accredit voting system testing laboratories and national standards to test the voting systems. In 2005, EAC adopted the Voluntary Voting System Guidelines for states on voting equipment and election technologies. These guidelines, which will become effective in December 2007, provide “a set of specifications and requirements against which voting systems can be tested to determine if the systems provide all the basic functionality, accessibility, and security capabilities required of these systems.”<sup>18</sup>

HAVA’s requirements have helped speed the adoption of electronic voting machines as replacements for lever and punch-card voting machines. In 2000, just 10 percent of the counties in the United States (containing 13 percent of registered voters) used DRE voting machines, while 41 percent of counties (containing 29 percent of registered voters) used optical scan ballots.<sup>19</sup> In 2006, 36 percent of the counties in the United States (containing 38 percent of registered voters) used DRE voting machines,<sup>20</sup> and 56 percent (containing 49 percent of registered voters) used optical scan ballots.<sup>21</sup>

#### **BENEFITS OF E-VOTING**

Digital electronic voting solves a number of voting problems associated with electromechanical voting technology. In the 2000 U.S. presidential election, for example, punch-card voting machines created ballots with half-punched ballots. When election officials could not determine voter intent, they had to discard these ballots. DRE voting machines eliminate this problem, because in the binary world of computers, “dimpled chads” do not exist. In addition, when completing a paper ballot, voters can easily mistakenly overvote or undervote and render their ballot invalid. DRE voting machines help eliminate these problems by preventing voters from casting invalid ballots, thereby ensuring that more ballots count.

Electronic voting also has the potential to revolutionize the voting process for blind, disabled, or illiterate voters. With paper ballots, many of these voters could vote only with the assistance of poll workers, which compromised both the confidentiality and the integrity of their ballots. Audio-based electronic voting

machines enable blind and illiterate voters to vote privately and independently. DRE voting machines also can have more user-friendly interfaces to make voting simpler. For example, DRE voting machines can show voters a summary of their ballot, allowing them easily to verify that they have not made an error.

Finally, many states allow early voting at central polling locations throughout the state in the days prior to Election Day. Early voting helps make voting more accessible to people who might otherwise be unable to vote on the day of the election. Early voting with paper ballots is impractical and expensive because custom ballots must be made available for each precinct, often in multiple languages. Thus, for example, in Riverside County, California, election officials switched to DRE voting machines after they discovered that they wasted over half a million dollars in unused paper ballots in one election because of low voter turnout.<sup>22</sup> DRE voting machines can host ballots for every precinct, so election officials can more easily provide early voting. In addition, many DRE voting machines enable multilingual and non-English speaking voters to vote using their preferred language.

#### OPPOSITION TO DRE VOTING MACHINES

Unfortunately, the effort to bring voting machines into the digital age has been politicized by various interest groups, including BlackBoxVoting.org and VerifiedVoting.org. These groups have waged a full-scale assault on DRE voting machines. They decry the technology as inherently insecure while refusing any solution other than a return to paper ballots.

The success of these groups reflects the high degree of polarization and distrust in politics, as well as the emotional investment many people have in elections. Many opponents of electronic voting machines are motivated by a distrust of technology, anger at election results, and conspiracy theories about voting companies. For example, political strategist Bob Shrum has blamed Senator John Kerry's loss in 2004 on the electronic voting machines in Ohio and suggested that election officials intentionally rigged these devices to favor President Bush.<sup>23</sup> Opponents of fully electronic voting machines also rely on the fact that few Americans understand the technology behind electronic

voting, such as cryptography. They scare voters and election officials into demanding something they do understand: paper.

Not surprisingly, some opponents of electronic voting machines have waged their battles in the courts. In Maryland, for instance, Linda Schade, the founder of TrueVoteMD, sued the Maryland State Board of Elections to force the board to decertify the Diebold voting machines and obtain an injunction to force Maryland to use paper ballots in the 2004 election.<sup>24</sup> The courts dismissed her motion and arguments and stated that although no election system could meet a standard of "perfect security," the court was "confident the votes of the Plaintiffs will be counted."<sup>25</sup>

---

*Opponents of fully electronic voting machines also rely on the fact that few Americans understand the technology behind electronic voting, such as cryptography.*

---

The debate on electronic voting was further politicized when Walden O'Dell, the CEO of Diebold, one of the primary manufacturers of e-voting equipment, was found to be a major fundraiser for the Bush re-election campaign in 2004. In addition, O'Dell distributed a fundraising letter in which he stated his commitment "to helping Ohio deliver its electoral votes to the president next year."<sup>26</sup> Since then Diebold, originally known for making ATMs, has been targeted by critics of e-voting for its allegedly insecure voting equipment. Initiatives such as "Hack the Vote" were created, and a monetary prize was offered to anybody who could prove that they could hack into an e-voting system undetected.<sup>27</sup> To date, nobody has claimed the prize money.

At the heart of the argument against e-voting is the notion that a computer cannot be trusted—an idea that flies in the face of our digital culture. In areas from online banking, to health information technology, to aviation, Americans trust computers every day with their lives and livelihood, not because computers are infallible, but because the benefits of technology significantly outweigh the risks. With any voting system

there is a margin of error, from either fraud or error, but e-voting offers the chance to minimize the margin of error by offering complete end-to-end auditing. The claim that “e-voting systems actually provide less accountability, poorer reliability, and greater opportunity for fraud”<sup>28</sup> is false and indefensible. Furthermore, as we discuss later in this report, some e-voting techniques use advanced cryptography that offer voters and election observers an unprecedented level of verifiability not achievable in traditional paper-based voting systems.

#### **Demands for Voter-Verified Paper Audit Trails**

Critics of electronic voting have demanded states add “voter-verified paper audit trails” to all DRE voting machines. If this approach were adopted, a DRE voting machine would print a paper ballot after each voter cast his or her electronic ballot. The individual voter could then verify that the printed paper ballot was correct. Depending on the system, the voter would either manually deposit this paper ballot into a ballot box or the voting machine would mechanically store the paper ballot. Advocates of adding voter-verified paper audit trails to all DRE voting machines have dubbed this approach “verified voting,” because the voter can verify that the voting machine has created an audit trail of his or her vote.

Unfortunately, paper-based auditing trails such as these do not allow the voter to verify that the results of an election are accurate. A DRE voting machine can provide up to three different guarantees to a voter: first, that the vote was cast as intended; second, that the vote was recorded as cast; and third, that the vote was tallied as recorded.<sup>29</sup> The first property, that the vote was cast as intended, simply means that the DRE voting machine understood the voter intent. Such verification is typically provided to the voter when the DRE voting machine shows the voter’s selection on the screen. The second property, that the vote was recorded as cast, means that the DRE voting machine recorded the correct vote for the voter. Paper audit trails are but one way to verify this property. The third property, that the vote was tallied as recorded, is not provided by voter-verified paper audit trails. Without this property, the other two guarantees are of less value. Ultimately, voters want to know that their vote was included in

the final tally. Paper audit trails do not provide this assurance.

One of the most common arguments used by opponents of e-voting is that the DRE voting machine is essentially a “black box,” and its operations are hidden from the voter. For most DRE voting machines, this statement is true. Historically, though, many types of voting machines, including the lever machines that were used for more than 100 years in U.S. elections, have been black boxes whose internal workings have been hidden from voters. There are always some people who mistrust new technology. In the 1960s, for example, people objected to using IBM computers to count punch-card ballots because of fears that the machines might switch votes.<sup>30</sup>

Contrary to the claims of e-voting opponents, though, merely adding paper audit trails to DRE voting machines does not make elections more secure. The problem is not “black box voting” but “black box elections.” Most of the operations of the election, such as ballot collecting, ballot transferring, and ballot tallying are hidden from the voter. The result is that no voter, regardless of the presence or absence of paper audit trails, currently knows whether his or her vote was actually counted.

---

*Ultimately, voters want to know that their vote was included in the final tally. Paper audit trails do not provide this assurance.*

---

Another common argument made by opponents of e-voting is that without paper receipts, an attacker can easily make a voting machine alter ballots without being detected.<sup>31</sup> Opponents of e-voting use fear of the unknown and widespread ignorance about information security to create the illusion that DRE voting machines can easily be hacked. Unfortunately, this argument confuses two issues: attacking a computer versus attacking an election. As we explain later, most voting systems used today rely on both physical security and auditing to prevent election fraud. Opponents of e-voting such as BlackBoxVoting.org claim that they can “hack an election,” but none of their attacks are plausible under real-world election scenarios, particularly

when the voting machines are correctly designed and implemented.<sup>32</sup> Unfortunately, claims that it is possible to “hack an election” are difficult for the average person or elected official to judge, because few Americans are information security experts.

For example, in July 2007, a group commissioned by the California secretary of state to review the state’s voting machines released a report documenting the security vulnerabilities that they found.<sup>33</sup> The report received much press, and critics of e-voting pointed to this report as proof that DRE voting machines can be hacked. While the report serves as a valuable tool to evaluate and improve the security of these machines, the so-called “attacks” detailed in the report are inconsequential. While these attacks may work in the lab, most of these attacks are unrealistic in real-world election conditions. As the authors admit early on in the report, they made no assumptions about the “compensating controls or procedural mitigation measures that vendors, the Secretary of State, or individual counties may have adopted.”<sup>34</sup> Moreover, the authors acknowledge that the “testers did not evaluate the likelihood of any attack being feasible.”<sup>35</sup>

Similarly, the claim that paper receipts are needed for voters to believe that the DRE voting machine has cast the correct ballot reflects a naive view of elections for several reasons. First, as discussed later in this report, paper receipts are not the only form of verification. Second, the DRE voting machines used in elections have been independently tested during the certification process. Independent testing has a crucial role in helping ensure the security of voting machines. EAC has worked with the National Institute of Standards and Technology to develop a National Voluntary Laboratory Accreditation Program to test the functionality, accessibility, and security of voting equipment.<sup>36</sup> Only laboratories that receive this accreditation are authorized to issue a national certification for voting machines, and the vast majority of states require this certification. If independent testers do not find a vulnerability that is later discovered by third-party researchers, then the state should review why the independent testers did not find the vulnerability and work to strengthen the certification process.

Because some people do not understand that voting machines must undergo independent testing, they fear that a voting machine may steal their vote. Independent testers perform quality assurance tests to verify that the machine does not erroneously record voting results. Thus, for example, a DRE voting machine that is preprogrammed to cheat would not be approved by independent testers because it would not give consistent or accurate results.<sup>37</sup> In order to steal votes, the DRE voting machines would have to be compromised after the certification process. The risk of DRE voting machines’ cheating can be further mitigated by conducting election-day auditing of a randomly selected group of voting machines during an election. Such auditing provides a probabilistic guarantee that no voting system can cheat.

Election officials use various physical security controls to prevent attackers from tampering with voting machines. Such controls include securely storing and transferring voting machines, using tamper-resistant hardware, and employing election watchers at the poll site. Critics claim that reliance on physical security controls is a weakness; however, paper-based voting systems also depend on physical security controls to avoid cheating (e.g., election watchers must prevent attackers from destroying or altering ballots).

Using a standard refrain from information technology security, opponents of e-voting also charge that “every system can be hacked.”<sup>38</sup> They argue that no DRE voting machines should ever be used because any computer can be compromised. This charge is unsubstantiated but plays to many Americans’ fears and inexperience with technology.

Once again, the realities of the election process are often ignored. The debate is not whether some machines can be compromised in a laboratory where the attacker has a laptop, tools, and full access to the voting machine, but whether an attacker can alter votes with limited access to the voting machines. Certainly, given enough collusion, time, and access to voting equipment, many attackers could successfully compromise voting machines. However, one of the reasons citizens trust elections is because there is sufficient separation of duties between multiple independent

actors to prevent most types of abuse. Regardless of the voting technology, though, no election is completely secure. To illustrate, “denial of service” attacks can be made against voting machines and poll locations through vandalism or intimidation. Yet the risk from these threats is mitigated by countermeasures, such as the threat of jail. The real threat to elections is from those attacks in which votes can be altered without detection.<sup>39</sup>

#### Requests for Disclosure of Source Code by Manufacturers

The disclosure of source code by e-voting manufacturers is another contentious issue for opponents of e-voting. Although virtually every DRE voting machine vendor discloses the source code of its products during the certification process, opponents of e-voting claim that it is unfair that everybody does not get a chance to see the source code. Many DRE vendors are unwilling to release their source code publicly because they fear copyright infringement. They also fear that individual reviewers will make unsubstantiated claims against their voting systems prior to an election simply to undermine the public’s confidence in the voting systems.

---

*Audit trails are less useful in proving that the voting machines functioned incorrectly. If there is a discrepancy between the audit record and the electronic record, neither voters nor election officials will know which record to trust.*

---

In any event, requiring all e-voting manufacturers to disclose their source code is not the solution. Most computers, including DRE voting machines, rely on third-party software, such as an underlying operating system, hardware drivers, and other related programs. No source code disclosure by a DRE manufacturer will be complete, because DRE manufacturers cannot provide source code for third-party software. Furthermore, attempts to mandate both paper audit trails and source code disclosure miss the fact that if paper audit trails work, there is no need for the source code to be publicly disclosed.

Although Congress should not mandate the disclosure of proprietary source code, states and counties would be wise to show preference to voting system manufacturers that publicly release the source code of their products for review. “Security through obscurity” has long been derided as an ineffective safeguard against attackers. The security of the voting machine should not depend on the confidentiality of the machine source code. Voting systems with publicly released source code will undergo greater scrutiny and testing by security researchers than those that are only tested in government-approved laboratories. Furthermore, voters will have a higher level of confidence in elections conducted on these machines given their greater degree of transparency.

#### WHY PAPER AUDIT TRAILS ARE NOT THE ANSWER

Requiring that voter-verified paper audit trails be added to DRE voting machines to detect error or fraud will not provide complete security in an election because the integrity of the election still depends on the chain-of-custody remaining secure. The real problem with the current generation of DRE voting machines is not that they use computers, but that the integrity of the election depends on maintaining a secure chain-of-custody of the voting machines and the ballots.<sup>40</sup> This problem is not unique to DRE voting machines, because the integrity of the election in a paper ballot system is similarly dependent on a secure chain-of-custody. In either voting system, a ballot can be compromised only if malicious actors are able to insert themselves into the voting process by, for instance, stuffing a ballot box or changing the code in a DRE voting machine. In both types of systems, election officials employ physical security countermeasures such as locked ballot boxes, poll watchers, and police to mitigate these risks.

Requiring that voter-verified paper audit trails be generated by DRE voting machines would increase the cost and complexity of elections. Paper ballots must be properly created, collected, transferred, tracked, stored, and counted. In addition, printers are costly to add and maintain. Printers can fail for a variety of reasons including hardware failure, paper jams, lack of paper, or lack of ink. Voting machines that generate

“reel-to-reel” paper receipts reduce anonymity on voting machines, especially for the last voters. Since poll watchers can track who votes on each voting machine, a chronological record of votes could compromise voter privacy.<sup>41</sup> Finally, opponents of e-voting demand paper ballots and paper audit trails so that they can be used in a manual recount. Yet manual tallying introduces numerous possibilities for fraud and error given the unpredictable human element.

A voter-verified audit trail provides voters a guarantee that an audit record of their vote was created. The audit trail also provides limited post-election assurance to election officials that the voting machines functioned correctly. An audit trail helps prevent anybody from undetectably altering the ballots cast in an election. Unfortunately, these audit trails are less useful in proving that the voting machines functioned incorrectly. If there is a discrepancy between the audit record and the electronic record, neither voters nor election officials will know which record to trust. Ultimately, election law will determine whether the electronic record or the paper record is counted as the true ballot in a disputed election.

---

*Unlike local verifiability, universal verifiability allows voters to be completely confident in the validity of the final election results.*

---

If a paper audit record is the ballot, as advocated by many opponents of e-voting, then any error or fraud in the paper trail will result in incorrect election results. To steal an election, attackers would merely need to alter the paper ballots and then claim the DRE voting machines malfunctioned. The United States moved to electronic ballots precisely to avoid the problems of paper ballots such as stuffed ballot boxes, spoiled ballots, and stolen ballots. The addition of paper audit trails to DRE voting machines would simply convert our elections back to a paper ballot system. Voter-verified paper audit trails can assure voters that a machine has properly understood their votes, but such audit trails offer no assurances that ballots were recorded correctly or included in the final vote. Similarly, voter-verified paper ballots assure individual voters that their ballot was recorded correctly by a machine, but such

ballots do not provide any assurance to voters that their ballot was counted correctly or even included in the final total.

#### ALTERNATIVES TO PAPER AUDIT TRAILS

Not all audit trails for DRE voting machines are paper based. One option that has emerged is audio verification of votes. After making their selections, voters hear an audio playback of their intended votes over headphones. An audio recorder, independent of the DRE voting machine, then records the audio confirmation of voters' selections. A recent study that compared the behavior of voters on DRE voting machines with audio audit trails and paper audit trails found that the paper audit trails had serious usability defects. The DRE voting machines were configured intentionally to introduce errors into the voting record. The study found that voters were 10 times more successful at finding errors when they heard their vote read back to them than when they read a paper receipt.<sup>42</sup>

Another option is to use two machines: one to record the ballot and a second, independent machine to verify the ballot and create a digital audit trail of each vote. The ballot can be stored on either digital media or paper. Thus, for example, voters could go to machine A to record their ballots onto a smartcard, and then go to machine B to verify that the smartcard contained the correct votes. The security of a system such as this would depend on the two machines not colluding. To discourage collusion, states could require separate manufacturers for each device or use open-source code. The fact that both machines would use audio technology would mean that everyone, including people with disabilities, could independently verify the audit trail. In contrast, paper audit trails would not allow blind or illiterate voters to verify their ballots independently.

A similar form of verification for DRE voting machines could also be achieved by using a single-input, dual output voting system. In this scenario, two independent DRE voting machines would connect to a single input, such as a keyboard or touch-screen. The two separate machines would independently capture all voter input and create separate audit trails of all votes. Again, the security of this voting system would depend on the machines' inability to collude.

An alternative to “local verifiability,” where the correctness of each vote is verified by the individual casting the vote is “universal verifiability,” which allows anybody to check that the final tally of votes is correctly computed.<sup>43,44</sup> Unlike local verifiability, universal verifiability allows voters to be completely confident in the validity of the final election results. The simplest example of universal verifiability is a vote taken by a show of hands. Anyone voting or observing the election can confirm that all votes were counted correctly. Obviously, showing hands would not work well in large elections, and it would force voters to give up their privacy. As discussed below, however, several cryptographic procedures have been proposed that provide universally verifiable elections, while also preserving the institution of secret ballots.

#### MOVING BEYOND PAPER TRAILS: THE NEXT GENERATION OF DRE VOTING MACHINES

DRE voting machines that provide universal verifiability offer more security than any voting machine currently used in U.S. elections. Researchers have developed a number of proposals to provide universal verifiability using cryptographic techniques (see Box 2) to secure information. These cryptographic systems provide voters with more security and verifiability than is found in traditional voting systems. To illustrate how cryptography can be used to improve the voting process, two examples of voting systems that offers universal verifiability through innovative cryptographic techniques—VoteHere and Scratch & Vote—are described below.

##### VoteHere

VoteHere, developed by Dategrity Corp., is an example of a voting system that offers universal verifiability through innovative cryptographic techniques. This system gives election administrators a complete end-to-end audit capability and voters the opportunity to verify that their vote is included in the final tally. A simplified version of the voting process includes the following steps:

1. Voters cast an electronic ballot in the voting booth using a DRE voting machine.

2. Voters receive a receipt, which provides them assurance that their ballot was encrypted correctly. The receipt also allows voters to track their ballot on the Internet. This receipt does not provide any information that would allow a voter to prove to anybody else how he or she voted.
3. At the end of the election, election officials post every encrypted ballot on the Internet. Voters can verify that their ballot has been recorded, but they cannot view the details of their ballot. Since the ballots are encrypted, each vote remains private.
4. Voters use the receipt they received after voting to verify that their encrypted ballot was transmitted successfully from the poll site to the central computer and has not been altered.
5. Election officials anonymize the ballots. They use a cryptographic technique called mixnets (described in Box 2) to guarantee that no votes are added or changed.
6. Election officials decrypt and count the anonymous ballots.

Dategrity Corp has published the source code used in the VoteHere system. In addition, it has published a number of white papers that explain, in depth, the details of the cryptography.<sup>47</sup> Although not everyone may understand or want to know the specific mathematics behind this voting system, the availability of the details of this voting protocol provides the opportunity for anybody to verify the security of this system.

##### Scratch & Vote

Scratch & Vote is another voting protocol that illustrates how researchers are developing innovative solutions for integrating advanced cryptography into easy-to-use voting systems. It uses everyday technology such as barcodes and

Candidates	Please select one candidate.
Bob	<input type="checkbox"/>
Carol	<input type="checkbox"/>
Ted	<input type="checkbox"/>
Alice	<input type="checkbox"/>
	
	

a scratch surface (such as that found on a lottery ticket) to provide universal verifiability.<sup>48</sup>

Voters mark their vote on a paper ballot but then cast their vote using a digital image of the Scratch & Vote ballot. This system illustrates how integrating cryptographic voting solutions can create an unprecedented level of security and verifiability for voters.

The Scratch & Vote ballot has two halves, as shown in the accompanying figure. On the left half, the ballot lists the candidates in a random order. The right half of the ballot is a column of corresponding checkboxes. It also includes a bar code, a scratch-off area and a tracking number. The bar code indicates which candidate

corresponds with each checkbox; however, this information is encrypted using a secret key. The secret key is located under the scratch-off area.

The voting process in the Scratch & Vote protocol works as follows:

1. The voter marks the checkbox opposite the name of the candidate of his or her choice.
2. The voter discards the half of the ballot that contains the list of candidate names. Since the names on the ballot are in a different random order on each ballot, without the list of names, nobody can tell from the checkmark position whom a voter selected.

## BOX 2: CRYPTOGRAPHIC TECHNIQUES TO IMPLEMENT VERIFIABLE, SECRET BALLOT ELECTIONS

Some of the most common cryptographic techniques used to implement secure, verifiable voting systems are described below. Although a discussion of the algorithms behind these techniques is outside the scope of this paper, an overview of these common techniques illustrates how cryptographic solutions can improve voting. All of the techniques described can be implemented using public, open cryptographic algorithms that have been peer-reviewed and subjected to scrutiny by the information security community.

**CUT AND CHOOSE.** Cut and choose is a basic building block of several cryptographic protocols. How can a piece of cake be divided fairly between two individuals? One simple solution to this problem is to allow one person to cut the cake and the other person to select a piece. This approach works because the person who cuts the cake cannot cheat since the other person chooses which piece each person receives. A similar cut and choose technique can be used to ensure that a voting machine cannot cheat without being detected. For example, imagine a voting protocol where the voter is asked to submit an encrypted ballot. If the ballot is encrypted, how can the voter trust that the encrypted ballot is correct? One solution is as follows. The voter makes his or her selections and then instructs the computer to print two different encrypted ballots. The voter chooses one ballot to test and one ballot to put in the ballot box. Next the computer proves that the test ballot correctly decrypts and matches the voter's original selection. After confirming that the chosen ballot decrypted correctly, the voter submits the encrypted ballot. Since the computer does not know which ballot the voter will select to test, it has a 50 percent chance of being caught if it ever tries to cheat.<sup>45</sup>

**HOMOMORPHIC ENCRYPTION.** Encryption is the process by which information is encoded to provide confidentiality. Modern encryption schemes have two parts: a public encryption function and a private key. The encrypted information is unintelligible to anyone without the key. Voting protocols use encryption to ensure that ballots remain private. Once ballots are encrypted, they can be made public since they are indecipherable without the key. If election officials make encrypted ballots public, then voters can verify that their encrypted ballot arrived unaltered from the poll site. How can election officials tally the votes if the ballots are encrypted? One possibility is first to decrypt all of the ballots, and then tally the decrypted ballots. The problem with this method is that decrypting ballots compromises voter privacy. A better solution is to use a special type of encryption, called additive homomorphic encryption, to encrypt the ballots. Homomorphic encryption is a special type of cryptography in which the sum of two encrypted values is equal to the encrypted sum of the values. Additive homomorphic encryption has a unique property described by the following equation:

$$\text{Encrypt (A) + Encrypt (B) = Encrypt (A + B)}$$

*(continued)*

3. The voter takes the remaining half of the ballot to a poll worker. The poll worker ensures that the scratch-off area has not been scratched off.
4. The poll worker detaches and throws away the scratch-off area.
5. The voter scans the ballot into a digital repository. The voter can take the paper ballot home, as it does not show who the voter selected and it does not contain the secret key necessary for decrypting the barcode on the voter's ballot.
6. Election officials post all of the scanned ballots on the Internet, which allows the voter to use the tracking number to verify that his or her ballot is posted online and has not been altered.

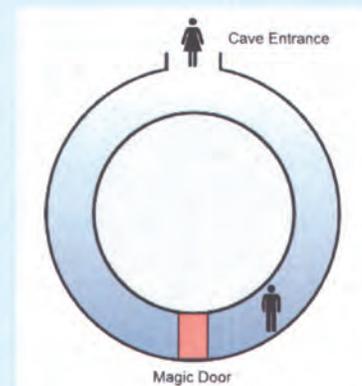
To ensure that no ballots are “rigged,” each voter can request two ballots during the voting process. The voter audits one ballot and votes with the other one. The audit process works as follows. First, the voter scratches off the scratch-off area, which reveals a key. Using this key, the voter can then decrypt the barcode information and confirm that it is correct (i.e., that the information in the barcode accurately reflects the random order of the candidates on this ballot). Finally, the voter discards the test ballot. Election officials do not accept any ballot where the scratch-off area has been removed.

To tally the votes, a computer reads each barcode to reveal the encrypted value that corresponds to the

## BOX 2 (continued)

The sum of two encrypted values is equal to the encrypted sum of the two values. This property allows a voting system to add all of the encrypted ballots into a single encrypted tally without first decrypting the ballots. Election officials can then just decrypt this one encrypted tally. Since nobody decrypts the individual ballots, each ballot stays private but the tally is public. How do the voters know the tally was decrypted correctly? The election officials post a zero knowledge proof (explained below), which any voter can verify.

**ZERO KNOWLEDGE PROOFS.** A zero knowledge proof is a method by which one individual can convince another individual that a statement is true, without revealing anything other than the veracity of the statement. The classic example of a zero knowledge proof involves Pablo the Prover, Violet the Verifier, and a cave with a magic door. As shown in the figure below, the cave is shaped like a circle, with the entrance on one side and the magic door on the other. Only a person who knows the magic word can open the magic door and complete the circle. Pablo wants to prove to Violet that he knows the magic word, but he does not want her to hear the word. Instead, they agree on the following test. Violet stands with her back to the entrance to the cave and Pablo enters either the right or left passage of the cave. Violet then faces the cave and tells Pablo which side of the cave she wants him to exit. If he does not know the magic word, Pablo only has a 50 percent chance of coming out the correct passage. If he knows the magic word, it is easy for him to accomplish. Pablo and Violet repeat this test until Violet is convinced that Pablo must know the magic word. In voting systems, this protocol is useful for confirming that a computer has completed an operation without forcing the computer to reveal information that could compromise voter privacy.



**MIXNETS.** Universal verifiability means that anybody can verify that the final tally is correctly computed from all valid ballots.<sup>46</sup> To provide universal verifiability, voting systems must allow anyone to look at the final ballots. For example, all of the ballots can be posted on the Internet. Unencrypted ballots cannot be posted online if they identify the voter because this would eliminate voter privacy. One solution is to anonymize the ballots before posting them on the Internet to ensure voter privacy. To anonymize a set of ballots, a computer takes the ballots and outputs a random permutation of them. However, voters need assurance that their ballots have not been changed in the process. Mixnets use zero-knowledge proofs (explained above) to prove that the computer has created a permutation of the original votes, without revealing the selections made by each voter. Mixnets allow voting systems to anonymize data without relying on a trusted third party.

checkmark position on the voter's ballot. Each of these encrypted values was created using homomorphic encryption (described in Box 2 above). This property allows the computer to aggregate all of the encrypted values to arrive at one encrypted tally for each race. Since all of the ballots are available online, anyone can perform these same steps to verify that the election officials have correctly tallied the ballots. Finally, a quorum of election officials decrypts the single encrypted counter, and then posts a proof of correctness that any voter can verify.<sup>49</sup>

Although cryptographic voting systems offer many improvements over current optical scan and DRE voting systems, no voting machine can ensure perfect elections. Even the best voting machine cannot prevent elections from being susceptible to poor authentication of voters, corrupt voter registration databases, and voter intimidation. Nor can these voting machines protect against voter fraud or coercion that occurs through absentee voting by mail. For the voters that use these machines, cryptographic voting systems can offer a significantly improved and more secure voting experience than paper-based systems.

## RECOMMENDATIONS

As the 2008 election approaches, members of Congress and state legislatures have introduced a number of bills to address the security of elections and voting machines. Proposed federal legislation, such as H.R. 811 (Rep. Holt, D-NJ) and H.R. 1381 (Rep. Tubbs Jones, D-OH) in the House and S. 1487 (Sen. Feinstein, D-CA) and S. 804 (Sen. Clinton, D-NY) in the Senate, would require voter-verified paper audit trails on all DRE voting machines. We support verifiable audit trails but we disagree that paper is the best solution or should be mandated to the exclusion of other technology. Other proposed federal legislation, including S. 730 (Sen. Dodd, D-CT), requires a verified audit trail, but permits this to be in the form of a paper, audio, pictorial, or electronic record. Similarly, H.R. 2360 (Rep. Ehlers, R-MI) requires that a voting machine allow the voter to verify his or her ballot before it is cast but it does not mandate a specific technology.

Although paper audit trails do provide local verifiability of votes, they are not the only solution. More

importantly, they are not necessarily the best solution. A key governing principle of the new economy is that policies should be technology neutral.<sup>50</sup> That means that federal legislation should not restrict states to a single voting technology. It is more desirable to have legislation that requires verification rather than a specific means of verification.

To restore voter confidence and promote secure election technology in the United States by ensuring that states can continue to improve their voting systems, we recommend the following:

- **Congress and the states should allow the use of fully electronic ballots, not restrict electronic voting systems to those that create paper ballots.** Although voting systems still can be improved, Congress should not bend to the intense lobbying of those who would ban any voting machine simply because it is fully electronic. As we have shown, paper ballots introduce many weaknesses of their own and are less secure than more advanced cryptographic voting systems.
- **Congress and the states should require that future voting machines have verifiable audit trails, not require machines with verifiable paper audit trails.** Legislation should not dictate what technology is used in voting machines, but instead define the desired characteristics of voting machines. Congress should allow the U.S. Election Assistance Commission and the National Institute of Standards and Technology to define voting machine technical standards, and not mandate or prohibit any specific technology, including paper trails, wireless communication, and Internet access.<sup>51</sup>
- **Congress should provide funding for the U.S. Election Assistance Commission to issue grants for developing secure cryptographic voting protocols and for pilot testing of new voting technology.** Cryptographic voting solutions offer the promise of more secure and reliable elections. Before appropriating another billion dollars to buy printers for DRE voting machines, Congress should fund pilot programs to test and evaluate new voting technology.

## CONCLUSION

Free and open elections are the hallmark of a modern democracy. If the United States wants to continue to be the world's leader in fair, secure, and democratic elections, it must commit to developing improved new voting systems, not go back to the voting technology of the 19<sup>th</sup> century. We believe that by adopting the recommendations outlined in this report, Congress and the states can restore voter confidence and improve security in our elections.

## ENDNOTES

1. The author thanks the following individuals for providing input to this report: ITIF President Robert D. Atkinson and ITIF staff John Anderson, Dan Correa, Julie Hedlund and Torey Liepa.
2. Smithsonian National Museum of American History, "Vote: The Machinery of Democracy," exhibition curated by William L. Bird Jr., Washington, DC, 2004 <americanhistory.si.edu/vote/intro.html>.
3. *The American Heritage Dictionary of the English Language*, 4<sup>th</sup> ed., s.v. "secret ballot" <education.yahoo.com/reference/dictionary/entry/secret+ballot>.
4. Michael Ian Shamos, "Electronic Voting—Evaluating the Threat," *Proceedings of the 3rd ACM Conference on Computers, Freedom & Privacy*, San Francisco, CA, March 1993 <euro.ecom.cmu.edu/people/faculty/mshamos/CFP93.htm>.
5. Automatic Voting Machine Company, "Behind the Freedom Curtain" (industrial film), 1957, available at the Internet Internet Archive <www.archive.org/details/Behindth1957>.
6. *Elective Franchise*, U.S. Code, vol. 42, secs, 1973aa-1a.
7. Smithsonian National Museum of American History, "Vote: The Machinery of Democracy," 2004.
8. Automatic Voting Machine Company, "Behind the Freedom Curtain," 1957.
9. Smithsonian National Museum of American History, "Vote: The Machinery of Democracy," 2004.
10. "For purposes of this Act, paper is 'durable' if it is capable of withstanding multiple counts and recounts by hand without compromising the fundamental integrity of the ballots, and capable of retaining the information marked, printed, or recorded on them for the full duration of a retention and preservation period of 22 months." See *Voter Confidence and Increased Accessibility Act of 2007*, 110th Cong., 1st sess., H.R. 811.
11. For a complete discussion of the election, see Robert A. Caro, *The Years of Lyndon Johnson: Means of Ascent* (New York: Vintage Books, 1990), 209-384; and Merle Miller, *Lyndon: An Oral Biography* (New York: G.P. Putnam's Sons, 1980), 116-137.
12. Robert A. Caro, *The Years of Lyndon Johnson: Means of Ascent* (New York: Vintage Books, 1990), 320.
13. *Help America Vote Act of 2002*, Pub. L. 107-252, 42 U.S.C. 15301 *et seq.*
14. *Help America Vote Act of 2002*.
15. *Help America Vote Act of 2002*.
16. U.S. Election Assistance Commission, *U.S. Election Assistance Commission Fiscal Year 2003 Annual Report* (Washington, DC: 2003) <www.eac.gov/annualreport\_2003.htm>.
17. Wendy R. Weiser, "Are HAVA's Provisional Ballots Working?" Brennan Center for Justice at NYU School of Law, New York, NY, 2006, <www.brennancenter.org/dynamic/subpages/download\_file\_39043.pdf>.
18. U.S. Election Assistance Commission, *U.S. Election Assistance Commission Fiscal Year 2006 Annual Report* (Washington, DC: 2007) <www.eac.gov/docs/EAC%20AR2006.pdf>.
19. Election Data Services, "Voting Equipment Summary by Type as of 11/07/2000," Washington, DC, 2 Feb. 2004 <www.edssurvey.com/images/File/VotingEquipStudies%20/ve2000\_report.pdf>.
20. Election Data Services, "Almost 55 Million, or One-Third of the Nation's Voters, Will Face New Voting Equipment in 2006 Election," press release, 2 Oct. 2006 <www.edssurvey.com/images/File/VotingEquipStudies%20/ve2006\_news.pdf>.
21. Election Data Services, "Almost 55 Million...", 2 Oct. 2006.
22. Farhad Manjoo, "The Case for Electronic Voting" *Wired*, 14 Nov. 2000 <www.wired.com/politics/law/news/2000/11/40141>.

23. Bob Shrum, interview by Stephen Colbert, *The Colbert Report*, Comedy Central, 26 July 2007.
24. *Schade v. Maryland State Board of Elections* (2004), Circuit Court for Anne Arundel County <news.findlaw.com/hdocs/docs/elections/schadevmd90104opn.pdf>.
25. *Schade v. Maryland State Board of Elections* (2004).
26. Melanie Warner "Machine Politics In the Digital Age," *New York Times*, 9 Nov. 2003 <http://query.nytimes.com/gst/abstract.html?res=F70E12FD385D0C7A8CDDA80994DB404482&fta=y&archive:article\_related>.
27. Tom Spring, "Can You Hack The Vote?" *PC World*, 5 Aug. 2004 <www.pcworld.com/article/id,117261-page,1/article.html>.
28. Stuart Miller, "Don't Trust Computers with e-Votes, Warns Expert," *Guardian Unlimited*, 17 Oct. 2002 <www.guardian.co.uk/internetnews/story/0,7369,813223,00.html>.
29. Alan T. Sherman et al., "An Examination of Vote Verification Technologies: Findings and Experiences from the Maryland Study," *Proceedings of the USENIX/Accurate Electronic Voting Technology Workshop 2006*, Vancouver, BC, Canada, 2006 <http://www.usenix.org/events/evt06/tech/>.
30. Tom Zeller Jr., "Why We Fear the Digital Ballot," *New York Times*, 26 Sept. 2004 <www.nytimes.com/2004/09/26/weekinreview/26zell.html>.
31. According to Avi Rubin, "[e-voting] makes the job of a person who wants to cheat a lot easier. If the machines had a paper trail, anyone could inspect the outcome, because the paper would give you the right answer." Source: Stefan Lovgren, "Are Electronic Voting Machines Reliable," *National Geographic News*, 1 Nov. 2004 <news.nationalgeographic.com/news/2004/11/1101\_041101\_election\_voting.html>.
32. Bev Harris, *Black Box Voting: Ballot Tampering in the 21st Century* (Renton, WA: Talion Publishing, 2004) <www.blackboxvoting.org/bbv\_chapter-5.pdf>.
33. California Secretary of State, "Elections and Voter Information: UC Red Team Reports," Sacramento, CA, 2007 <www.sos.ca.gov/elections/elections\_vsr.htm>.
34. Matt Bishop, "Overview of Red Team Reports," Sacramento, CA, 2007 <www.sos.ca.gov/elections/voting\_systems/ttbr/red\_overview.pdf>.
35. Matt Bishop, "Overview of Red Team Reports," 2007.
36. U.S. Election Assistance Commission, *U.S. Election Assistance Commission Fiscal Year 2006 Annual Report*, 2007.
37. Another possibility is for the DRE voting machine to be configured to cheat only after receiving some activation code, such as a sequence of keys. This type of attack should be mediated against by reviewing the source code during the certification process and election-day auditing.
38. Christina Almeida, "Expert Issues e-Voting System Challenge to Hackers," *USA Today*, 30 July 2004 <www.usatoday.com/tech/news/computersecurity/2004-07-30-evote-hack-challenge\_x.htm>.
39. Michael Ian Shamos, "Electronic Voting—Evaluating the Threat," 1993.
40. Ben Adida, *Advances in Cryptographic Voting Systems*, CalTech/MIT Voting Technology Project, VTP Working Paper #51, September 2006 <vote.caltech.edu/media/documents/wps/vtp\_wp51.pdf>.
41. Contemporaneous reel-to-reel paper receipts reduce anonymity for all voters. See Michael Ian Shamos, "Testimony Before the Maryland General Assembly House Ways & Means Committee," 2004 <euro.ecom.cmu.edu/people/faculty/mshamos/WaysMeansTestimony.htm>.
42. Sharon B. Cohen, "Auditing Technology for Electronic Voting Machines," CalTech/MIT Voting Technology Project, VTP Working Paper #46, May 2005 <www.vote.caltech.edu/media/documents/wps/vtp\_wp46.pdf>, 5.

43. Ben Adida, *Advances in Cryptographic Voting Systems*, September 2006.
44. *CyberVote*, "Frequently Asked Questions: 5. What is Universal Verifiability?" n.d. <[www.eucybervote.org/faq\\_security.html#q33](http://www.eucybervote.org/faq_security.html#q33)>.
45. The voter cannot vote with the decrypted ballot because he or she would know the keys used to decrypt it. In most voting protocols, the computer encrypts the final ballot using keys unknown to the voter so that the voter is unable to prove to a third party how he or she voted. This requirement prevents voter intimidation and vote selling.
46. *CyberVote*, "Frequently Asked Questions..."
47. See for example, the following: Andrew Berg, "VHTi Verification as a Scratch Ticket," VoteHere, Inc., Bellevue, WA, 2004 <[www.votehere.net/vhti/documentation/VHTi\\_Cryptography\\_Explanation-detailed-2.0.3638.pdf](http://www.votehere.net/vhti/documentation/VHTi_Cryptography_Explanation-detailed-2.0.3638.pdf)>, C. Andrew Neff, "Verifiable Mixing (Shuffling) of ElGamal Pairs," VoteHere, Inc., Bellevue, WA, 2004 <[www.votehere.net/vhti/documentation/egshuf-2.0.3638.pdf](http://www.votehere.net/vhti/documentation/egshuf-2.0.3638.pdf)>; and C. Andrew Neff, "Practical High Certainty Intent Verification for Encrypted Votes," VoteHere Inc., Bellevue, WA, 2004 <[www.votehere.net/vhti/documentation/vsv-2.0.3638.pdf](http://www.votehere.net/vhti/documentation/vsv-2.0.3638.pdf)>.
48. Ben Adida and Ronald L. Rivest, "Scratch & Vote: Self-Contained Paper-Based Cryptographic Voting," *Proceedings of the 13 ACM Conference on Computer and Communications Security (CCS'06)*, Alexandria, VA, 2006 <[ben.adida.net/research/AdidaRivest-scratch-and-vote.pdf](http://ben.adida.net/research/AdidaRivest-scratch-and-vote.pdf)>.
49. Ben Adida and Ronald L. Rivest, "Scratch & Vote...", 2006.
50. The New Economy Task Force, "Rules of the Road: Governing Principles for the New Economy," Progressive Policy Institute, Washington, DC, 1999 <[www.ppionline.org/ppi\\_ci.cfm?contentid=1268&knlgAreaID=128&subsecid=174](http://www.ppionline.org/ppi_ci.cfm?contentid=1268&knlgAreaID=128&subsecid=174)>.
51. The *Voter Confidence and Increased Accessibility Act of 2007*, 110th Cong., 1st sess., H.R. 811, for example, would prohibit voting machines that allow wireless communications or that have been connected to the Internet.

## **ABOUT THE AUTHOR**

Daniel Castro is a Senior Analyst with ITIF specializing in issues relating to IT and the digital economy. He has experience in the private, non-profit and government sectors. Outside of ITIF, Mr. Castro is a Visiting Scientist at the Software Engineering Institute (SEI) in Pittsburgh, Pennsylvania where he has developed virtual training simulations to provide clients with hands-on training of the latest information security tools. Before joining ITIF, Mr. Castro worked as an IT analyst at the Government Accountability Office (GAO) where he audited IT security and management controls at various government agencies. He has a B.S. in Foreign Service from Georgetown University and an M.S. in Information Security Technology and Management from Carnegie Mellon University.

## **ABOUT THE INFORMATION TECHNOLOGY AND INNOVATION FOUNDATION**

The Information Technology and Innovation Foundation (ITIF) is a nonprofit, non-partisan public policy think tank committed to articulating and advancing a pro-productivity, pro-innovation and pro-technology public policy agenda internationally, in Washington and in the states. Through its research, policy proposals, and commentary, ITIF is working to advance and support public policies that boost innovation, e-transformation and productivity.

For more information contact ITIF at 202-449-1351 or at [mail@itif.org](mailto:mail@itif.org), or go online to [www.innovationpolicy.org](http://www.innovationpolicy.org).  
**ITIF | 1250 I St. N.W. | Suite 200 | Washington, DC 20005**