Recommendations for the Conduct of Elections in Miami-Dade County using the ES&S iVotronic System

(revised)

Douglas W. Jones
Department of Computer Science
University of Iowa
Iowa City, IA 52242
(jones@cs.uiowa.edu)

Revised May 30, 2004
Revised June 7, 2004

Summary

These recommendations are based on a study of various documents, as cited, meetings with Miami-Dade County staff and elected officials on May 13 and 14, 2004, with a followup visit and empirical testing on June 3, and telephone and E-mail contact with ES&S. Some of the recommendations here are already in various stages of implementation by Miami-Dade County, while others may prove to be more difficult. The summary recommendations that follow are each discussed, at length, in the remainder of this report:

These measures should go a long way toward the goal of building confidence in the integrity of the election system. Their effectiveness can be maximized if they are used together, so that knowledgeable members of the public are present to observe all phases of the election process.

The program of public education must include an admission of the known weaknesses of the current system while focusing on moving ahead, conducting the best elections possible using the equipment we have, and building a foundation for responsible equipment purchases in the future.

The following additional sections are included at the end of this report:

Recommendations

1) Build a public-private partnership to encourage civic participation.

The culture of civic participation in Miami clearly needs strengthening. Connie Kaplan has said that she is lucky to find even a few observers for pre-election tests of voting systems, and that it is very difficult to staff polling places on election days. The average age of election workers at the polling place is in the 70's, and a new generation must be recruited into these jobs.

In the wake of election problems in 2000 and 2002, there is a high level of voter anxiety about the integrity of the system of elections. Miami-Dade County has a unique opportunity to exploit this, working to channel this anxiety into constructive action.

Civic groups like the League of Women Voters, the Miami-Dade Election Reform Coalition, the Greater Miami Chamber of Commerce, trade unions, religious groups, and service clubs can all help, as can the political parties, elected officials and the county government. Everyone has an interest in improving the conduct of elections, but isolated and independent campaigns by these groups are unlikely to be as effective as a coordinated effort. It should not take much coordination; certainly, Democrats and Republicans are unlikely to cooperate intensively, but even a little cooperation can have great impact.

It is important to make it clear that this is not just a get-out-the-vote drive, and not just a pollworker recruiting program, but a broad program to encourage citizens to get involved in their community. Political party efforts to recruit doorknockers and partisan polling place workers can also motivate people to vote or work as nonpartisan observers. County efforts to recruit polling place workers can also lead people to volunteer for their parties, and voter registration drives can also lead people to volunteer as polling place workers or observers.

Furthermore, all of these will benefit from pressure on employers to allow leaves of absence on election day or for election-related functions before or after election day. Serving in these functions, whether in voluntary or official roles, is as important a civic obligation as jury duty or military service in time of war, and we should encourage employers to view it in these terms!

Elected officials can play a strong role here, both in encouraging their supporters to volunteer and in encouraging their larger financial contributors to release their employees who wish to serve in voluntary or official roles in the election process.

2) Educate the public about these measures in advance.

If we are to build voter confidence, the voting public must understand what the government is doing to protect their voting rights and to protect the integrity of the election system. The campaign discussed above will be ineffective if voters believe that it is empty propaganda, so it is essential that the measures include a campaign to recruit and educate members of the public to serve as observers of and witnesses to every critical step in the election process. This is why it is so essential that the campaign listed above be conducted as part of this effort.

Furthermore, substantial segments of the public must be informed of the flow of the election, from pre-election testing to the final canvass, and of the potential vulnerabilities in this flow and of the measures taken to guard against exploitation of these vulnerabilities. Simply telling the public to trust officialdom to run the election is not sufficient! We must eliminate the idea that some faceless "they" is at work setting up the election and counting the votes at the end of the day.

The Brennan Center for Justice at New York University is currently in the process of preparing a report for the Leadership Conference on Civil Rights that will recommend creating a permanent independent panel to serve as a public watchdog over the entire process. The existence of such a panel can be an important adjunct to this education effort.

3) Reconcile the number of voters with the number of ballots.

One of the central accounting measures that can be used to protect the integrity of the ballot box, whether electronic or paper, is the reconciliation of the number of voters who signed into the polling place with the number of ballots counted. If this number is brought forward through the canvass, we can gain a very useful check against classic forms of fraud such as ballot box stuffing, pollworker errors such as casting demonstration ballots on real voting machines, voters who have difficulty casting their ballot, and a variety of other problems.

I recommend, at the polling place, that the number of signatures in the pollbook be counted and reconciled with the number of ballots cast at the close of the polls. There will be discrepancies, but they should be very small, and to the extent possible, they should be investigated immediately. The following numbers should be tracked during the election:

Ballots Cast (as recorded by the voting machine)
Ballots voided after a voter attempted to vote and failed or fled

These numbers should add up to the number of signatures in the pollbook, and whenever ballots are voided, a record should be made, explaining why.

The above reconciliation will only be possible if a written log is maintained for all ballots voided, since there are other reasons to void a ballot, for example, when a voting machine is incorrectly used for demonstration. It would be appropriate for this log to be maintained for all precinct worker actions that involve precinct workers entering voting booths between the time the polls open and the time the polls close.

In addition, the number of absentee ballots received by the deadline should be counted (including those cast at satellite polling places during early voting) and the number of provisional ballots accepted should be counted. These, added to the number of signatures, give a measure of the turnout against which the number of ballots counted can be compared, not only at the precinct, but at vote collection centers and during the canvass.

Discrepancies, for example, precincts with unusual numbers of voided ballots, should receive intensive and early attention from auditors. It is useful to carry the turnout figures forward outside of the election management system using manual methods in order to act as a check on the integrity of the electronics. While canvassing an election by hand is horrible clerical work, doing this one sum manually or at least carrying these numbers forward outside the election management system should not be onerous.

Status: Connie Kaplan indicated on May 14 that this measure was already in place, at least in the form of reconciliation at the polling place. It is not clear that the reconciliation is carried forward through the canvass so that the turnout figures, computed from the polling place, are carried forward to an overall turnout figure at the time the canvass is completed. Furthermore, Steve Bolton at ES&S has told me that his investigations have shown that pollworkers have indeed been using regular voting machines to cast, and then void, demonstration ballots at some precincts, seriously complicating ballot accounting.

4) When the polls close, print and post an additional copy of the precinct totals.

Posting a copy of the precinct totals at the precinct allows any observer to note the totals for any races that interest them and to check them against the official canvass. This allows any interested person to help audit the integrity of the canvassing process and prove to themselves that the county or the election management system has not corrupted the count between the time that the polls close and the time the final canvass is published.

This measure only works if the final published canvass does not combine absentee, early voting and provisional ballots, so it is important to break these numbers out. Also, the number of provisional ballots collected at the precinct must be disclosed to any observers present at the closing of the polls so that they can verify that the number of provisional ballots eventually counted does not exceed the number distributed.

Status: Connie Kaplan indicated on May 14 that this procedure was the one she was familiar with in Chicago, and she wondered why Miami-Dade County was not doing this. Furthermore, she pointed out that it was required, if feasible, by Florida law. Staff at the meeting wondered if it was feasible with the amount of paper in the printers, but it appears that the consensus was that this procedure could be followed.

5) Reconcile the printed record from the precinct with the electronic record.

At the close of the polls, printouts from the precinct are saved, along with compact flash cards and the PEB that was used to close the polls, and all of these are delivered, through a secure chain of custody, to the vote collection center and eventually to the county's central vote tabulation center. Because of questions about the integrity of computerized vote tabulation technology, it is appropriate to finish the canvassing process by comparing the printed record from the precincts with the electronic records tabulated by the election management system.

In effect, once the voters are allowed to perform this reconciliation independently, it is wise for the county to defend itself by performing the same reconciliation in-house in order to catch and correct any errors before they are exposed to the public. This procedure is widely used elsewhere, including, for example, Dallas County, Texas (where Steve Bolton has observed it), as well as Iowa, where we are working to write it into law.

Status: Connie Kaplan indicated on May 14 that this procedure was already in place, and Orlando Suarez confirmed this on June 3. Clearly, observers at the canvassing center should be shown when this is being done so that they can satisfy themselves that the county is effectively defending itself against error in the canvass.

6) Guard the chain of custody for all election materials.

The chain of custody for election materials is strongest when we minimize reliance on locked doors at the precinct! It is one thing for the law to demand that there be a lock, but quite another for county officials to examine the locks to determine if they are genuinely secure or vulnerable to classical attacks with credit cards, hairpins and other commonplace tools.

If possible, open the polls on the morning of the election. I strongly recommend experimenting with the time it takes to open the polls to see if this is practical. The current procedure, powering up the machines the night before, may no-longer be needed. I recommend asking the IT support people who helped start the machines for this year's spring primary how long it took to get them running and if they believe it could be done in the morning without creating too much risk. On exploring the situation in Miami-Dade County with Steve Bolton at ES&S, he convinced me that it should be possible to open the polls using iVotronic voting machines running firmware version 7.5.1.0 in around half an hour to 40 minutes; on June 3, I confirmed this.

Similarly, at the close of the polls, data extracted from the machine immediately, using the data path for which the machine was originally designed and certified (the PEB) should be viewed as more trustworthy than data extracted from the machines using alternate data paths or at a later time, unless other evidence suggests otherwise. The questions surrounding extraction of audit data from the voting machines are complex enough to require a separate section, but in general, the normal path by which data is extracted from the voting machines must not involve leaving the machines unguarded for any length of time, nor must it place the machines in a situation where they are nominally under guard but where many people have access.

Use of security seals is valuable, but only if these seals are not cosmetic. There are reports from many jurisdictions of the use of custom printed numbered security seals where the numbers are never checked when the seals are broken. Such cosmetic procedures are of no use. Only if the seal number is recorded when the seal is applied and verified at the time the seal is broken is that seal of any value. Polling place, vote collection center and canvassing center workers should all be informed of this, and election observers should be aware of the need for these checks.

Status: The forms filled out during the canvass to report on the condition of information from the precinct in Miami-Dade County indicate a clear attention to the integrity of information from the precinct. This is good, but these same forms indicate that in some precincts, seals have not been properly applied at the close of the polls.

The current practice of starting the voting machines the night before appears to be entrenched to the point that even if the machines offered instant startup, there would be resistance to starting the machines on the morning of election day. This is unfortunate. Similarly, there appears to be a bit too much trust of locked doors to guard the integrity of the machines after the polls close.

Donald Llopis, of the Electronic Voting Division, expressed his personal support for opening the polls on the morning of election day in our meeting on June 3, and he has proposed two different ways of doing this that are discussed later. Lester Sola, Chief Deputy Supervisor of Elections, was hesitant, worrying that if just one PEB was bad at just one polling place, it would be a disaster. A later section discusses some ideas for reconciling these two positions.

7) Institute a program of rigorous testing.

Direct recording electronic voting systems have been described as *black box voting systems* because observers can do very little to assure themselves that the software and mechanism inside the voting machine performs correctly. This flaw is compounded by the fact that the voting system firmware and software in use today is proprietary and not open to public inspection. The most difficult part of the voting system to test for correctness is the touch-screen interface and the firmware behind it. In comparison, the canvassing procedure is far more open, particularly if the protective measures outlined above are in place.

The best available defense against the known risks of direct recording electronic voting machines is a rigorous program of testing. Unfortunately, the pre-election tests conducted on current voting machines are not sufficiently rigorous. The central problem is that if the machine is informed that it is undergoing a test, it can be programmed to perform differently under test than in a regular election. Therefore, an effective program of testing must include some tests that are significantly more rigorous than is conventional in pre-election testing or even the testing performed by the independent testing authorities that certify the machines to Federal and State standards. There are three categories of tests that are particularly important:

a) Challenge or red-team testing, where knowledgeable technicians and programmers attempting to find and exploit weaknesses in the voting system. Maryland had RABA Technologies of Columbia Maryland perform such tests on its voting system (the results are reported in the *Trusted Agent Report* of Jan. 20, 2004). Ohio had weaker tests performed by Compuware Corp. on 4 different voting systems, including the iVotronic (the results are available in *Direct Recording Electronic (DRE) Technical Security Assessment Report* of Nov. 21, 2003).

b) Serious investigation of how the system responds to normal errors, including how the consequences of these errors show up in the election results. This is a category of investigation that is important at the local level because local election workers are the most likely to know what kinds of errors are normal, and it is the local election workers who must recognize and correct such errors when they occur. Once you know what the normal errors are, the training materials may need adjustment to reflect this, not only with measures to try to reduce the frequency of these errors, but with specific procedures for dealing with their consequences.

Normal errors are the types of errors that a system invites. In the everyday world, for example, locking your keys in the car is a normal error -- a dispassionate observer of the driver-automobile-doorlock interaction can easily predict that, no matter how carefully you train drivers not to lock their keys in the door, some will accidentally do so. For a voting system, we know that forgetting to close the polls on one of the voting machines in the precinct is a normal error, but there are others that are less well known. The important quesiton for voting system administrators is, what are the normal errors and for each, how can we protect ourselves against it?

c) Parallel testing. Because we know that voting machine software can be prepared to recognize when it is being tested, the most effective tests of a voting machine will be tests that are as nearly indistinguishable from normal polling place operation as is possible. The best proposal for this involves selecting the machines to be tested at the last moment, and testing these machines from the minute the polls open to the minute the polls close.

Parallel testing, sometimes called parallel monitoring has been advocated by many people. The California Ad Hoc Touch Screen Task Force recommended parallel testing in their *Report* of July 1, 2003, and Hans Van Wijk of NEDAP, a voting system vendor based in Holland, presented a paper on parallel testing at the USACM Workshop on Voter-Verifiable Election Systems in Denver on July 28, 2003. This model of testing has been offered by a number of organizations as an alternative to the use of a voter-verified paper ballot printer on each voting machine. Parallel testing is strongly endorsed by the Leadership Conference on Civil Rights, and the state of California used parallel testing in the March 2, 2004 primary (see the *Parallel Monitoring Program Summary Report* prepared by R&G Associates, Apr. 19, 2004).

In summary, parallel testing is conducted by picking precincts at random and then having the testing teams arrive at those precincts at roughly the time the pollworkers arrive. Each testing team then selects a voting machine at random from the machines at the selected precinct as the machine to be tested. This machine is segregated from the other machines at the precinct, for example, roped off with signs indicating that it is under test. While the pollworkers open the polls at the other machines, the testing team opens the polls on the machine being tested, and then, all day, as the election is conducted on the other machines at the precinct, the testing team tests the machine under test. As the polls close, the testing team closes the machine under test, and then prints out the totals for that machine and verifies them against the test votes that were cast.

It is important that parallel testing be conducted in public because the public needs to know that the county is taking this measure, and at the precinct so that there is no way that the voting machine can be in any way specially prepared for the test. Given both of these conditions, it is reasonable to recruit members of the public to help. After voters have cast their ballots, for example, they could be invited to help cast test ballots. As each test ballot is cast, members of the testing team must note the votes on that ballot, so that they can compute what the totals should be at the end of the day. Any problems voters have with the machine under test should be noted as well, and of course, voters who helped with the test by casting test ballots should be rewarded, for example, with special stickers saying more than the usual "I voted."

Status: Steve Bolton of ES&S indicates that the company has contracted with Science Applications International Corporation to conduct a challenge testing exercise on the iVotronic. This is a good pro-active step on the part of the vendor! It will be interesting to see what results ES&S releases.

In the discussion on May 14, it was clear that there was considerable resistance to the idea of parallel testing in the Fall 2000 cycle of elections. This is unfortunate. While it may not be possible to undertake a full-scale parallel testing program this fall, doing so in one precinct per congressional district in the August primary would be reasonable, and this might be expanded to one precinct per commission district in November. California's "Parallel Monitoring Program" was ordered only one month before the March 2004 primary, so it ought to be possible for Miami to do something at least as competent with several months of lead time.

Orlando Suarez, in our meeting on June 3, suggested that the Audit and Management Services Department might be interested in parallel testing. He had just given a presentation to that department on election auditing, presenting the work he had done the previous summer and ideas he had for the use of data extracted from the event log. He was uncertain, however, about the advisability of involving voters directly in the tests. I continue to advocate public participation in these tests.

8) Involve the county Audit and Management Services Department.

Counting votes is an accounting function, just as much so as counting dollars. As with all accounting, it is subject to both error and the threat of fraud. We deal with both of these threats in the world of financial accounting by conducting regular audits, and we know that, if it were not for the threat of such audits, corporate fraud would be far more common than it is.

In elections, the canvassing board conducts a number of self-audits with every election, and many of the recommendations given here aim to strengthen these. What we do not have in our election system in most of the United States is a system of external audits, where auditors from outside the election office examine the integrity of the process.

External audits could, of course, be conducted by the state election office, or by some national election authority, but we can gain much of the protection of such an external audit by bringing in auditors from the county's own audit department.

Status: The Miami-Dade County Audit and Management Services Department was brought in to examine the conduct of elections in April, September and October 2002. The audit reports from these elections (Dated Aug. 7, Sept. 30 and Oct. 8) contain many useful suggestions that confirm the competence of this department to conduct such audits. A later section of this report contains comments on the recommendations contained in these reports. It would be extremely desirable if this department was brought back on a fairly regular basis to observe future elections.

Orlando Suarez, on June 3, suggested that the Audit and Management Services Department might be interested in parallel testing. See additonal notes on this above.

9) Involve the county E-Gov Department.

Computerized voting systems contain computers. This is obvious, but what is not obvious is why local and state governments across the country are not recognizing this. Data processing or electronic government departments have decades of experience in questions of security, fault recorvery, backup policy, data communications and related domains, and all of this is applicable to election systems.

Status: The now famous "E-Gov" memo from Orlando Suarez to Jimmy Carmenate on June 6, 2003 makes it clear that there has been some cooperation between E-Gov and Elections in Miami-Dade County, and the followup work reported in his memo of June 9 to Donald Llopis and his further followup memo on Oct. 10, 2003 to Connie Kaplan makes it clear that this is an established relationship. These memos expose real competence and suggest that the addition of experts from this department to audit and testing teams would be very productive.

10) Improve incident reporting.

In general, the process of system certification requires feedback. Thus, for example, the Federal Aviation Administration requires reports for all incidents involving airplanes to be sent to the FAA as well as to whoever might have caused the incident. Without this feedback, the FAA would not have the information needed to improve their regulations, their testing of airplanes, or their operating rules. Similarly, in the voting system domain, the state elections office and the Federal Election Assistance Commission need to learn about any problems encountered by the counties so that they can adjust their certification requirements.

Unfortunately, nationwide, we have a problem with this. The Election Assistance Commission has no resources to handle incident reporting, and incident reports sent to most states are filed, never to be examined again. This must change, but change will require that the counties act, routinely reporting incidents to the state. If state authorities continue to ignore such reports, we will need to create a non-governmental organization to handle them.

Status: The E-Gov memo of June 6 from Orlando Suarez was addressed to Ana, with a copy to Jimmy Carmenate in the Elections office. Ana, it turns out, was Ana Queredo, the area manager for ES&S. This is typical of current practice -- incidents are reported to the vendor, and there is no formal process for collecting incident reports at any level of government.

The memo of Oct. 10, 2003, apparently describes additional incidents that Steve Bolton of ES&S says he was unaware of. This suggests that, as apparent size of the problem grew, the number of people informed of it declined. This is not good! Clearly, unless the vendor is informed of the extent of the problems, they cannot be expected to fix them.

Florida does appear to have a standard way of reporting irregularities that are found during the canvassing process, but much more is required, since incidents involving election equipment occur at many points during the election cycle, and all of them need to be tracked and available for study if we are to improve on the current status quo.

Donald Llopis mentioned, on June 3, that he was in contact with the state elections office as they attempted to follow up on the audit trail error that has been the focus of recent publicity. This is a positive development, and there is reason to hope that the channels of communication that have opened as a result of this will remain open.

11) Track software version usage.

The canvass for an election should include a record of the firmware and software version numbers of all electronic systems used in arriving at that canvass. These should not be taken from records of the version that was supposed to be installed, but should be taken from the systems themselves.

In fact, even this is inadequate, since a corrupt piece of software can report any version number it wants. There are unsolved technical problems involved in actually determining, to any degree of certainty, what software is actually running on an arbitrary computer. Therefore, for the time being, we must accept the report of the system and hope that the software certification process and the chain of custody from the certification authority to the voting machine are both rigorous enough to defend us against misreported versions.

Status: There are allegations that incorrect software versions may have been used in Miami-Dade County in the past. We know that incorrect versions have been widely used elsewhere in the United States, with solid proof in California, Iowa and Ohio. Tracking the version used in each election as part of the canvass is a strong defense against the temptation to install an uncertified version.

The version number of the iVotronic is reported at the top of the adding machine tapes printed at the precinct, both the zero tape and the poll closing tape (polling location report). I have verified with Steve Bolton at ES&S that hese numbers represent only the machine used to print the tape at the polls and not the full set used at the precinct, but checking these numbers at the time the adding machine tapes are checked against the canvass should be a straightforward enhancement to the assurances offered by the canvass.

12) Track the source of data used in canvassing.

The iVotronic system offers many ways to extract data for inclusion in the canvass. There are three internal flash EEPROM memories in the machine, from which data may be extracted using PEBs, compact flash EEPROM memory cards or a serial data link. Depending on which extraction path is used, it is possible that different data may be extracted!

Only summary data is extracted to the PEB, but this summary data is committed to paper immediately on the printer at the precinct, so it provides valuable protection against loss or corruption of data in the electronic transmission paths upward through the canvassing process.

As Steve Bolton of ES&S has explained, data extracted via the serial port, for example to a laptop computer, includes all vote image reports and event logs, but all of this data comes from the first of three flash EEPROM chips inside the iVotronic computer. This fact is important in the event that there is any disagreement between these chips.

Data extracted via the compact flash card also includes all vote image reports and event logs, but in this case, this data will come from any one of the three flash EEPROM chips, whichever one the internal firmware judges to be the most authoritative.

Therefore, in the event of disagreement between the internal EEPROM chips, data extracted via the Compact Flash card and data extracted via the serial port may differ, and these two paths are the only ways to extract detailed reports from the machine, as opposed to the summary data extracted via the PEB! Therefore, it is imperative to maintain a record, for each machine, of any alternate path used for data extraction. It is also noteworthy that the integrity of the data extracted may vary depending on the path by which it is extracted.

Ideally, ES&S (and other electronic voting system vendors) should incorporate data path and data source tracking into their systems, so that this information is automatically tracked by the canvassing system, but until this is done, manual records are essential. In addition, even when this is automated, it should be subject to routine testing, and this requires that manual records be maintained during the closing and canvassing of precincts that are subject to audit.

In summary, unless the iVotronic machine indicates a serious error condition because of a disagreement between the internal EEPROM memories, extraction by the serial port is an acceptable path, so long as chain of custody issues are carefully attended to. Extraction of data via the compact flash card should be acceptable once the problems with the Unity election management system are solved; these are the subject of a later section.

Status: Miami-Dade County has shifted from extracting event logs from the I-votronic by compact flash cards to extracting it using the serial link to a laptop computer, all without clear evidence of understanding of the difference between these paths. It is not clear to me that ES&S or, for that matter, the FEC/NASED standards themselves deal coherently with the redundant memory required in the voting system. This issue is at the root of the problems identified in the "E-Gov" memo from Orlando Suarez to Jimmy Carmenate on June 6, 2003, the subject of a later section of this report.

13) Allow only the minimum necessary software on election computers.

The Unity election management system makes little or no use of security technology to protect the integrity of election data, and the data downloaded from the iVotronic are similarly unsecured. These weaknesses are documented in the security assessment of the iVotronic system performed by Compuware for the State of Ohio, available on the web at:

http://www.sos.state.oh.us/sos/hava/files/compuware.pdf

It is worth noting, for example, that the database used within the Unity election management system is in dBase format, and files in this format can be manipulated by using Microsoft Excel.

Status: Donald Llopis assured me on June 3 that Excel is not installed on any of the machines used in Miami-Dade County to run Unity. Excel is, however, loaded on the server. I do not know how carefully the Unity machines are isolated from the server, nor how the software on the laptops is managed. As a rule, all machines running Unity need to be minimally configured, with no software installed that is not absolutely necessary. Furthermore, given that these weaknesses of the ES&S system have been disclosed to the public, it is important to make a public record of what software is loaded on a machine prior to using it for election management purposes.

Time to Open the Polls

On exploring the situation in Miami-Dade County with Steve Bolton at ES&S, he convinced me that it should be possible to open the polls using iVotronic voting machines running firmware version 7.5.1.0 fast enough that it should be unnecessary to start the machines the evening before. My estimate, based on his figures, is that it should be possible to start up a precinct containing 10 iVotronic voting machines in around half an hour to 40 minutes, and that, as soon as the zero tape is printed, it should be possible to open the polls to voters, even if some machines have not yet completed their initialization.

This is because the PEB used to initialize the machines and accumulate the zero tape can be moved from machine to machine fairly quickly (as soon as the display on the machine says that it is OK to do so). The basic procedure is to unpack one machine, set up its voting booth, and then put the initialization PEB in place. As soon as the next machine is unpacked and set up, it should be possible to move the PEB to that machine, and so on down the row. By the time all the machines are set up, one of the first machines set up should be done initializing, and it can be used to print the zero tape. The first machine to be set up should be the one equipped with the audio ballot, because it will take up to 20 minutes to finish initialization, but the PEB can be removed after only a minute or two and moved to the next machine. Of course, the county should not rely on this procedure until it has been tested by a crew at the elections office!

This estimate is based on Steve Bolton's estimate of 20 minutes to start the audio ballot machine and 3 to 7 minutes to start each of the others, plus the fact that the PEB can be removed from each machine about a minute or two into its startup sequence. If this is correct, then Miami should not need to start their machines the night before, and this should allow not only a considerable cost savings, but also an improvement in the chain of custody, since it allows the machines to remain sealed in their cases up until the morning of the election instead of unsealed and, relatively speaking, somewhat more vulnerable because they are unpacked and set up without guard overnight.

Donald Llopis, on June 3, confirmed my estimate for the time taken to open the polls, while Lester Sola was worried that if the PEB used to open the polls went dead during the opening of the polls, the result would be a doubling of the time taken, leading to unacceptable delays at any polling place where such a PEB failure occurred.

Donald Llopis suggested that there was a second way to speed opening, aside from the procedure I suggested above. His proposal was to complete the startup on each machine at the warehouse instead of at the precinct the night before, and then lock the machines at the warehouse prior to packing them for shipping to the precinct, so that all that remained to do at the precinct was to unlock the machines and print the zero tape. As far as I can see, this procedure, while a bit surprising, exposes the systems to fewer security vulnerabilities than the procedure of opening the polls the night before at the precinct, and it should allow time to redo the zero-tape collection process should the PEB that was used to prepare things at the warehouse fail at the precinct. Thus, the procedure I outlined would be the fallback in case of PEB failure, while this new procedure would allow very fast setup.

It is important to note, with regard to both starting the machine the night before, and starting the machine days in advance at the warehouse, that the iVotronic, so far as I understand, draws no power or almost no power from its internal batteries when it is locked. It is the insertion of a PEB that causes the iVotronic to start up and begin drawing significant amounts of power, so neither of these procedures poses significant risk of running down the batteries.

The county's current approach to qualification testing of every PEB received from ES&S should markedly reduce the frequency of PEB failure. In discussing the PEB failures that remain, Donald Llopis suggested that physical shocks that knock the bar magnet inside the PEB loose from its mooring may be a significant. This bar magnet provides the signal to the iVotronic that a PEB has been inserted, and this is what actually turns on the iVotronic. If indeed there are PEBs in which the bar magnet has come loose from its moorings, ES&S should find some way to prevent this, and the qualification testing at Wyle Labs may need to be strengthened to include shock tests that more nearly approximate the handling that real PEBs have encountered.

Why is Miami using Bitmap Ballots

One of the puzzles that an outsider looking at the situation in Miami must ask is, why did Miami switch to using the bitmap ballot representation from the plain text representation used by most iVotronic customers? By way of explanation of these terms, it should be noted that plain text ballots are presented using a limited alphabet of letters and accent marks, in much the same way that text is represented by word processors. In contrast, the bitmap ballot representation treats the ballot display as an image, allowing display of arbitrary artwork. When text appears in a bitmap ballot, it is stored and displayed without any reference to the fact that the image happens to consist of letters. Bitmaps displays are more expensive to transmit and store than text, and this is part of the explanation for why the iVotronic system, as used in Miami, starts up more slowly than iVotronic systems in other counties.

This question was brought up anew in the *OIG Final Report* on Miami-Dade County Voting Systems Contract No. 326, dated May 20, 2003 and in the *ES&S' Response to the April 23, 2002 Draft Report of the Office of Inspector General*, dated May 2, 2003. The latter, on page 35, states a consensus that the use of bitmap displays was not needed for the trilingual ballot.

There are at least three answers to the question of why Miami chose to adopt bitmap ballots: First, ES&S is deliberately moving away from text ballots toward bitmap ballots. This move offers flexibility display of ballots in calligraphic languages such as Arabic, it allows display of candidate portraits or party logos on the ballot, and many other desirable features, as well as offering a partial defense against certain types of fraud that could be perpetrated by insiders with access to the voting system firmware. This, naturally, led ES&S to recommend use of the bitmap representation when Miami faced them with the need for a trilingual ballot.

Second, the alphabet used inside the ES&S iVotronic is small, much smaller than the alphabets supported by modern word processors that can easily present text in Japanese Kanji, Greek, Russian and other languages. Steve Bolton of ES&S has explained that the iVotronic alphabet is limited to 256 printable characters, and that this includes not only the alphabet, numbers and punctuation marks, but also the distinction between regular, boldface and large print. As such, the people at ES&S were worried that they would not be able to represent the diacritical marks required by Spanish and Haitian Creole all in the same alphabet. Creole does seem to use an alarming number of diacritical marks.

Third, the discussion on May 14, 2004 included mention of a three-column trilingual ballot created in text format. This was apparently unacceptable -- people said it reminded them of the butterfly ballot layout from Palm Beach in 2000. This demonstration does appear to have shown that the diacritical marks for Spanish and Haitian Creole can coexist, but when this ballot was rejected, the easy alternative, allowing arbitrary ballot layout, was to move to the use of bitmaps.

There is an alternate way to run a trilingual election, using two different bilingual ballots, one English/Spanish and one English/Creole. As far as the iVotronic firmware is concerned, each of these bilingual ballots would be in one language -- the English text in each of them, after all, uses the same letters as the Spanish and Creole, but with no diacritical marks. As a result, the iVotronic system would need to be configured with two different ballot styles, one per language.

If each language (or each of several bilingual ballots) requires a different ballot style, this might involve using the existing methods for formatting ballots in split precincts or primary elections. Where there would only be two styles in a one-language precinct, for example, Democratic and Republican, there could be as many as 6 styles in a trilingual precinct, Democratic-Spanish, Democratic-Creole, Democratic-English, Republican-Spanish, Republican-Creole and Republican-English. This would complicate ballot definition, precinct management and canvassing, and it allows the possibly illegal release of subtotals divided along ethnic lines.

Data Paths from the iVotronic to the Canvass (the Suarez Memos)

The memos from Orlando Suarez, dated June 6 2003, to Anna Quevedo and October 10 2003, to Connie Kaplan, raise serious questions about the integrity of the ES&S iVotronic system. These memos discuss examinations of the event log data produced in two small elections, a special runoff election in May 20, 2003 in North Miami Beach, and an election on October 7 in Homestead.

In examining the details of these memos, sample event logs from the election of March 9, 2004, and discussing these memos, with Steve Bolton at ES&S, I have concluded that there are two root causes of the anomalous event logs reported by Orlando Suarez:

-- First, the firmware being used on the iVotronic (version 7.5.1.0) is recording data in a format that is not fully understood by the Unity election management system software (version 2.4). It appears that the misunderstanding occurs only when the iVotronic attempts to recover from an error as it records data for the election management system.

-- Second, there is no standard for reconciling different records of the election in the event that they differ. The iVotronic maintains three copies of all key data, and in the event of an error, the particular copy that will be extracted from the iVotronic depends on the medium used to extract that data.

ES&S appears to have expected these errors to be extremely rare, while it appears that in fact such errors are fairly common -- the two elections Suarez examined in 2003 were apparently small, and yet, he found at least two instances of this error. If this is indeed the case, then these errors are very common! In the October 7, 2003 primary in Homestead, the problem was encountered in one out of 13 voting machines used.The frequency 1 in 13 suggests that there are really two problems with the iVotronic and Unity, one that causes Unity to incorrectly read data recorded to the compact flash card from the internal iVotronic flash EEPROM number 2 or 3, and one that causes the internal error that forces use of flash EEPROM number 2 or 3 with a frequency close to 1 in 13.

Orlando Suarez observed the misreporting of serial numbers in data extracted from the iVotronic, and he observed the loss of event log entries for "Normal Ballot Cast" events. In both cases, the audit data was extracted from the iVotronic machines via compact flash cards. This raises serious questions about the utility of the event log data extracted to compact flash cards!

ES&S' Explanation of the Problem

According to Steve Bolton at ES&S, there are 3 flash EEPROM memories inside the iVotronic, each with a capacity of 2 megabytes. Normally, these hold identical copies of the ballot image data and the event log, and they contain non-identical copies of the configuration data. The configuration data itself is supposed to be identical, but it is not stored in the same memory locations in the different EEPROM chips. There are valid technical reasons for at least part of this irregularity that follow from essential characteristics of flash EEPROM technology. The data in each chip is protected by some kind of checksum, so that a simple computation on the data in that chip is sufficient to detect the most likely errors that might corrupt the data.

The iVotronic runs comparisons between the EEPROM chips on a regular basis, comparing the vote image data and the event log data on the three chips, and declaring a major fault if it finds any difference. Under normal circumstances, when the data is extracted from the machine, it is read from EEPROM chip number one. In the event that the data is corrupted, however, it can be read from chip number two or chip number 3. Unfortunately, the different paths by which the data may be extracted do this differently:

-- When data is extracted via the serial port, the extraction is always from chip number 1. Extraction from chips 2 or 3 requires the replacement of EEPROM chip number 1 by a specially prepared *V-recovery* chip.

-- When data is extracted via the compact flash card, the extraction is from the lowest numbered chip that the iVotronic system believes to be correct.

The story is confounded by an additional element. The configuration data on the flash EEPROM shows the machine serial number and similar information. The Unity election management system, version 2.2, only knows how to read the configuration data when it is extracted from chip number 1. When Unity reads data that was extracted from chips number 2 or number 3, it misreads the serial number. This is the root of the problem Suarez observed, It implies that the firmware in the iVotronic found something amiss with the data in flash EEPROM number 1.

Another confounding factor is that if the Unity election management system receives two reports from the same voting machine, under some circumstances or as printed in some reports, it will delete or fail to report the data from one machine while reporting the data from the other, while under other circumstances or in other reports, it will merge the data from the two machines. in the Oct. 7 2003 election in Homestead, event log data from 5 out of 66 voting machines was not reported.

Steve Bolton at ES&S asserts that they dug into the data Suarez extracted and determined that, indeed, there was incorrect data in EEPROM number 1 in some of the cases that Suarez identified. This corruption did not trigger the iVotronic's warnings about problems in the vote image file or the event log because the bits that had changed were in unused parts of the EEPROM. Therefore, the vote image report and the event log extracted on the compact flash cards should have been correct.

Curiously, the voting machine serial number is recorded twice on the compact flash card. It is recorded in the configuration field of the 2 megabytes of data extracted from the flash EEPROM within the iVotronic, and Steve Bolton has told me that it is used as the name of the file holding this data, and on June 3, I confirmed this with the help of Donald Llopis. Because the compact flash card is recorded with a conventional file system, inserting the compact flash card in any compact flash reader attached to a Windows or MacOS machine should show the directory of the data on the card, and this directory will show the serial number of the machine as the file name on the 2-megabyte file holding the contents of that machine's internal flash EEPROM. Even when the serial number read by Unity is wrong, this serial number that names the file should be correct! This should allow manual checks of the serial numbers on compact flash cards that were read incorrectly by the Unity election management system.

Recommendation

Major parts of the certification of the firmware in the iVotronic was done by a different independent testing authority than the certification of the software in the Unity Election Management System. This difference makes the current certification system particularly vulnerable to the type of problems observed here!

All of the original testing and certification of the Votronic and the Votronic II was based on the use of the serial data link from the Votronic to the Unity Election Management System for extracting ballot images and event logs. Only with the iVotronic was the new data path added, via the compact flash cards. Therefore, the procedure currently under consideration in Miami-Dade County, extracting the data via the serial port to a laptop computer, is a reasonable and conservative approach because it uses the data path that has been subject to the greatest amount of testing. I recommend use of this approach, although I believe it is best to do this as soon after the close of the polls as possible, either by bringing laptops to the precinct or by immediate collection of the iVotronic voting machines.

I recommend that all of the compact flash cards be saved, and that the compact flash cards be used to recover the audit data in the event that any questions are raised about the integrity of the laptop route to recovering this data. Until such time as ES&S delivers a version of the Unity election management system that can correctly read the serial numbers from all compact flash cards, the serial number data should be looked at with a grain of salt and only trusted after checking against the serial number recorded as a file name on the card itself and with the written records of the serial numbers of the machines at the polling place.

Once ES&S has delivered a version of Unity that can reliably read the serial numbers, and once this has been run through its paces enough to convince people that it can indeed read the serial numbers that were read incorrectly by the old version of Unity, the use of the laptop computers can be phased out except in rare cases, for example, when the compact flash cards are lost or unreadable.

New Experiments

On June 3, with the help of Donald Llopis, I performed some experiments. We recreated the North Miami Beach runoff election of May 20, 2003 in a sample precinct with 4 iVotronics, in the hope that we could artificially recreate the serial number problem. We failed to reproduce the problem in this experiment, a likely outcome if the 1-in-13 frequency measured in the Homestead primary is close to being representative.

On failing to recreate the problem, we went back to the archive of data from the March 9, 2004 primary. On May 26, 2004, Donald Llopis had identified an example of the serial number problem in the data from precinct 315. We extracted this data from the archival copies of the audit data from this election -- archival copies made from the compact flash cards -- and we copied this archival data back to a flash card for processing.

In processing the recreated data for precinct 315, we observed that 1 of the 5 voting machines at that precinct had its serial number misreported. The correct serial number was 5117383. In the consolidated ballot image report, the data for this machine was reported as being from machine number 5117319 on May 26, 2004, but as being from machine number 5116491 on June 3. This is consistent with what Steve Bolton said about the likely "made up serial numbers" for this problem -- that they always seem to end with either 19 or 91, and it is similar to what Orlando Suarez observed in his June 6 2002 memo. The same machine's data was entirely absent from the consolidated event log report, when printed to paper, but it was shown on the display screen, with the serial number reduced to simply 91, with no other digits shown. In the system log showing all actions taken using Unity (specifically, that part of Unity called the Election Reporting Manager), the serial number in question was shown as V???????.

The behavior we observed for this data is fully consistent with the behavior predicted in the most up-to-date report I have from ES&S, an internal document dated May 26 2004, forwarded to me on June 7 by Steve Bolton.

Additional Recommendation

I conclude that, in the extremely unlikely event that the only surviving data from some precinct is the data extracted from the compact flash cards, or in the event that the reliability of the data extracted via the serial port and the reliability of the data extracted using the PEB for that precinct is challenged, that the following procedure should be effective for using the data from the compact flash cards:

Step 1) process the compact flash cards in batches by precinct, and take the consolidated ballot image report for each precinct at face value, recognizing that some serial numbers may be misreported.

Step 2) take the consolidated event log at face value, but expect that it will not include the data from some machines in the precinct, so the number of valid ballot cast events may be less than the number of ballots reported in the ballot image report for that precinct.

Step 3) examine the system log listing produced during steps 1 and 2. Wherever this includes serial numbers of the form V???????, go back to the pile of compact flash cards for the precinct and locate the missing cards (they will have a file name of the form Vxxxxxxx.BIN that is missing from the consolidated event log. For each of these, process the event log for that card separately, displaying it on the screen, and then print a screen-shot of that log (or screen shots if it requires more than one screen). This screen shot should account for the ballot cast events that were missing in the report for step 2.

Generally, this procedure should be unnecessary because, until the software involved has been fixed, the data extracted over the serial port to the laptop should be the primary source of data used for audit purposes until a bug fix for the serial number problem is installed.

Comments on the Inspector General's Report

The Inspector General's Report, *OIG Final Report* on Miami-Dade County Voting Systems Contract No. 326, dated May 20, 2003 and in the *ES&S' Response to the April 23, 2002 Draft Report of the Office of Inspector General*, dated May 2, 2003. These documents cover a wide range of issues, many of them outside the area of my competence, but some are worth commenting on.

Ease of use, page 8, *OIG report*. Indeed, this is correct. The current FEC/NASED standards and the testing done by independent testing authorities under these standards almost completely ignore human factors. Only where handicapped accessibility is involved is the coverage significant, and even there, aside from questions of type size and mechanical usability, the coverage is weak. Nowhere in the standards does it ask if real people under real polling place conditions can successfully use the machine to cast real votes. I do not know how Florida standards address these issues, but it is unfortunately the case that the burden in most states falls on the county to determine the answers to the central questions of usability.

Certification for multilingual ballots, page 11, *OIG report*. It is not clear to me that the current FEC/NASED certification covers specific languages. I do not know about Florida certification. Certainly, the ITA reports don't address this in any detail that I have seen.

Questions of processor power and memory capacity, page 30, *OIG report*. Here, I agree with the *ES&S Response*, page 36. The iVotronic is indeed an embedded system, and the choice of components in this device is appropriate for such an application. I have great distrust for personal computer hardware in embedded systems. When you buy a "state of the marketplace" PC, you expect it to last 5 years, rarely more. I do not believe that Miami-Dade County wants to buy voting machines every 5 years! Embedded systems are generally designed to last much longer, which requires the use of conservative designs using parts that will remain on the marketplace for many years. I am aware of numerous embedded computer systems still running today that are based on 30-year-old computers. The voting system used in my county, Johnson County Iowa, uses 20-year-old precinct-count optical mark-sense scanners.

Attachment of SRAM to the motherboard, page 31, *OIG report*. Here, again, the *ES&S response*, page 40, explains the lack of sockets for these chips, but it is worth adding this explanation. Studies done in the avionics industry show that connector sockets are one of the primary points of failure in embedded computer systems. Every pin of every socket is a possible failure point. The more connector pins, the more likely the system is to fail. Therefore, to produce reliable systems, as few components as possible should be socketed. I have seen evidence that in the consumer electronics field, some manufacturers routinely expect 20 percent of all products to be returned for service or replacement within the first six months. I do not believe that Miami-Dade County would tolerate such a failure rate in its voting systems!

Questions of Compact Flash card cost, page 35, *OIG report*. Here again, I agree with the *ES&S Response*, page 44. Consumer electronics and industrial electronics are frequently made to the same external specificaiton, and this is certainly true of Compact Flash cards. Generally, consumer grade equipment comes with lower tolerance to variation of temperature and humidity, and it is not designed to last as long. With industrial grade equipment, you pay for very specific guarantees about temperature and humidity tolerance and product lifetime. I have, for example, worked on software designed for launch into orbit. A radiation hardened launch certified 8088 microprocessor cost thousands of dollars, where an exactly compatible part could be purchased at Radio Shack for under five dollars. The situation with Compact Flash cards is far less extreme, but in the end, the difference comes down to similar considerations. The commercial grade cards might work just fine in an air conditioned home or office, but there is some security in buying industrial grade equipment made and tested to survive mistreatment that the compact flash card in your digital camera is unlikely to encounter.

ITA Test Reports and Technical Data Packages, page 36, *OIG report.* As the OIG states, the county should have someone review this material! The ITA test reports are boring reading, admittedly, but on many occasions, they have revealed very important things about voting systems. Whenever the county purchases a new voting system or an upgrade to an existing system, it is very important to peruse this material carefully.

Maintenance Manuals, page 38, *OIG report.* Curiously, when ES&S came to Iowa for initial certification of the Votronic II, they included the maintenance manual, schematic diagrams of all of the electronics, and even mechanical diagrams of the PEB interface, as part of the technical data package. I suspect that, when ES&S offered the technical data package to the county, these materials were included!

Comments on the Auditors' Recommendations

In general, the reports signed by Cathy Jackson of the Audit and Management Service Department and addressed to David Lehy, dated Aug 7, Sept. 30 and Oct. 8, contain a huge number of recommendations that I heartily endorse. There are, however, some recommendations that need clarification:

Election Backup, Aug. 7 *Audit Report*, page 3. The data to be backed up should be the raw data files extracted from the iVotronic via the serial port or via the compact flash cards. Additionally, the composite files produced by the Unity election management system should be backed up, but because the election management system has been observed to disregard data from some compact flash cards (see, for example, the report by Orlando Suarez to Connie Kaplan on Oct. 10, 2003), which is to say, from some iVotronics, it is important to back up the raw data itself before Unity is allowed to process it. It is encouraging to find that, as of June 3, the county appears to have a complete archive of the data from the compact flash cards collected from the March 9 primary!

Network Security, Aug. 7 *Audit Report*, page 4. The recommendation that some type of virus protection be installed on the PEB and on the iVotronic is probably based on a misunderstanding. Because these computer systems do not run conventional operating systems, they are not vulnerable to the viruses that attack conventional operating systems. While they may have vulnerabilities, commodity anti-virus software is not relevant. Security assessments are needed to examine the protocols used to communicate with the PEB and iVotronic, but these assessments will not resemble the assessments that might be conducted for a server or a desktop computer running a general purpose operating system such as Windows or Linux. (It is worth noting that the PEB is indeed a computer system and not a passive memory device, so it does require such an assessment.) It is my understanding that ES&S has requested such assessments from Science Applications International Corporation. It will be interesting to see the results of this work.

Transparency of Tabulation, Aug. 7 *Audit Report*, page 6. There is a real need for a county and voting-system specific observer's manual that explains, to election observers, what it is they are seeing. In Geneva Switzerland, where they use Internet voting as well as optical mark-sense ballots in precinct and by mail, they have discovered that the best solution is to offer the same training courses to election observers as they offer to the workers being observed. Release of the pollworker and canvassing manuals may have some value, but I suspect that custom documentation for the observers would have real value. It may be that this documentation would best be produced by an outside entity such as the League of Women Voters or the Election Reform Coalition, but the county ought to cooperate with and encourage such a venture.

It would be useful for the Elections department to release a report that answers the auditor's recommendations, indicating, for each, the progress made toward compliance or the reason for continued noncompliance. Such a report would be a great confidence builder, in part, because it would advertise the attention the county has paid to trying to get things right with this voting system.

Comments on the Florida Recount Procedures

This entire exercise, focusing as it does on the event logs, brings into question the role of these event logs. Florida's administrative code, section 1S-2.031, *Recount Procedures*, is quite puzzling in this regard. Subsection 5c governs recounts on the iVotronic, offers no role for the inspection of the event logs.

In fact, the situation may be worse. This subsection begins: "1. The county canvassing board shall be required to produce printed vote totals for the affected race or races for each precinct." Does this refer to mere recovery of the paper records printed at the polling place, or is it a demand to print new paper copies from the election management system? In the former case, there is no proteciton against the corruption of the paper record (for example, by someone who commits forgery, substituting new paper for old), while in the latter case, there is no protection against someone modifying the electronic records from which the paper record is reprinted.

The rule continues: "2. The county canvassing board shall verify that the total votes for the recounted race or races taken from the printed vote totals for each precinct are the same as the total votes shown on the county totals from election night." Are the records from election night that are subject to this comparison to be the totals from the electronic record, for example, the PEB, or the paper printed at the polling place? No guidance is provided.

The rule continues: "If there is a discrepancy, the county canvassing board shall investigate and resolve the discrepancy." How? What evidence is admissible? Perhaps this is the point at which the event logs should be inspected to check that the number of ballots cast matches the number of ballots reported in the two disagreeing reports, and to check that all ballots were cast after the polls opened and not too long after the polls closed, and similar details.

There are additional problems with Florida's recount law that are raised by the existence of the event logs. For example, there appears to be no provision in Section 102.166 of the Florida Statutes for requesting a recount if the margin in an election exceeds half a percent in the second set of unofficial returns, no matter what evidence there may be of errors or omissions in those returns. If, for example, the event logs showed that a significant number of votes had been cast prior to the official opening times for the polls, or if the number of signatures in the pollbook was radically different from the number of ballots recorded, there would appear to be no recourse, short of contesting the election under the rules of Section 102.168. That section of the Florida code focuses on misconduct, fraud or corruption, all of which are generally willful acts, leaving few grounds for challenge if the central issue is error or some kind of failure in the mechanism.

Additional Notes on the Limitations of this Report

This is not a complete security audit for the iVotronic system, nor does it address the public issue of whether direct-recording electronic voting machines such as the iVotronic should be equipped with a voter-verified paper trail.

The most comprehensive security assessment of the iVotronic system that has been released to the public is the one performed by Compuware for the State of Ohio, available on the web at:

http://www.sos.state.oh.us/sos/hava/files/compuware.pdf

This report has serious shortcomings, but it also identifies numerous areas where the security of the iVotronic could be materially improved. The risk mitigation strategies recommended in that report, unfortunately, all require upgraded software from the vendor, and the timetable for the certification of such software upgrades makes it unlikely that any such changes will be available in time for the November 2004 general election.

There is considerable agitation nationally to demand that direct-recording electronic voting systems be equipped with a voter-verified paper trail. This report does not address this issue. The reason is, there in no voter-verifiable paper trail retrofit available for the iVotronic now, nor is any expected by the November general election. Were such a retrofit available, it would offer the possibility of an additional layer of security for the iVotronic system, and the decision to adopt or not to adopt this technology would require serious evaluation.

Some opponents of direct-recording electronic voting systems such as the iVotronic have advocated the total abandonment of these machines in favor of machine counted paper ballots, using the absentee ballot processing machinery already in place. In theory, Miami-Dade County still has the option to do so, and if the problems with the iVotronic had turned out to be more severe, or had Miami-Dade County been less aggressive in pursuing defensive measures, such a move might have been appropriate.