Cleveland State University
Center for Election Integrity

for December 8, 2008

U.S. Election Assistance Commission

Hearing on

Tracking Voting System Performance

Statement of

Candice Hoke

Director, Center for Election Integrity
Associate Professor of Law

The Center for Election Integrity of Cleveland State University appreciates the invitation to participate in this Hearing on Tracking Voting System Performance. Since August 2006, our Center has held an appointment as Public Monitor of Cuyahoga County Election Reform, with the most intensive work occurring in the fall 2006 through early winter 2007.

You requested that I include in my testimony discussions of the Public Monitor's efforts in evaluating voting system performance in Cuyahoga County, including both proactive measures and election day monitoring and reporting. Responding to that request is my chief focus here. I also offer some suggestions on features the EAC might include in an EAC voting system tracking system, plus other activities that I believe the EAC should initiate to protect election accuracy and voter access.

I. Center for Election Integrity's Work as Public Monitor to Improve Election Administration in Cuyahoga County, Ohio Elections

A. Background

In Ohio, the federal primary is administratively the most complex election to manage and even more challenging than a presidential general election. For instance, in Cuyahoga County/Cleveland area, over 6000 separate ballot styles were required. Unfortunately, the former executive management of the Cuyahoga County Board of Election (BOE) chose the May 2006 primary to roll out two systems of HAVA-compliant technology. The result was widely viewed as

Administrative & Legal Training * Technical Support & Consultation * Studies in Election Law, Policy & Technology * Civic Education

A Partnership of the Cleveland-Marshall College of Law & the Maxine Goodman Levin College of Urban Affairs
Campus Address 1801 Euclid Avenue, LB 229   * *Mailing Address* 2121 Euclid Avenue, LB 138 Cleveland, OH 44115
216.687.2313 *Voice* * 216.687.6881 *Fax* * www.csuohio.edu/cei/

one of the nationally most notorious election debacles ever recorded. Every managerial task and every election function sustained some critical failure. The BOE had selected Diebold DREs (TSx plus VVPAT) for the polling locations and a central count optical scanning system for absentee ballots. The central count scanning operation, which was a networked set of scanners, failed its Logic & Accuracy tests for over a week, resulting in the Director's 2:00 a.m. telephone alert to BOE Board Members on Election Day. The Director stated that the scanning system had failed the pre-tests and that the BOE needed to initiate a hand count of all optical scan ballots.

While deeply troubling, the network scanning failure was not the only serious deficiency. In virtually every election function and managerial task, the BOE sustained major failures. Hundreds of poll workers failed to report to their locations; hundreds of DRE machines were not operating; numerous other poll workers were uncertain of their tasks; hundreds of reserve poll workers who were waiting in zone stations were never assigned to polling locations (because the calls were not transmitted); the precinct supply bags omitted essential supplies such as memory cards or security seals, or contained the wrong memory cards and hence the wrong ballots for a precinct; voters' and poll workers' calls to the BOE were blocked, unable to move through the overloaded phone system; over a hundred DRE memory cards were missing at the end of the night; hundreds of other security equipment items were missing, such as DRE supervisor and voter access cards, and DRE memory card compartment keys; precinct reconciliations of voters to numbers of cast ballots was highly "elusive"; and much more.

By mid-morning Election Day, the Board knew a major disaster had occurred and resolved to convene an independent review of the election preparation and management process. The BOE Board (followed by affirmation by the County Commissioners) appointed the three-member Cuyahoga Election Review Panel (CERP) to investigate and provide recommendations for improving the administration of the county's elections. A distinguished local judge, Ron Adrine, was named chairman, and a former BOE Director, Tom Hayes and I were named to the panel. I handled the staff hiring, and most training and research assignments. The BOE Board charged us to report back in 60 days. Our Final Report, 200 pages of findings accompanied by over 300 recommendations for reforms, and another 200 pages of appendices, may be the most comprehensive study of an election failure that has been written. It can currently be found at www.urban.csuohio.edu/cei and will be permanently posted at www.electionexcellence.org.

I am delighted to report that the Cuyahoga BOE has been restructured and has been managing increasingly successful elections despite its having a whopping 11% of Ohio voters on its registration rolls and 59 separate electoral jurisdictions within its boundaries.   It has managed 4 different voting technologies from November 2004 to November 2008, and at least 12 elections in 2008.

B. Public Monitor of Cuyahoga Election Reform

At the CERP investigation's inception, the BOE Board requested the Panel to recommend some form of "monitor" to ensure that the expected report did not become a dead-letter but would be implemented. In August 2006, the Board and County Commissioners appointed the Center for Election Integrity to be the independent Public Monitor of Cuyahoga Election Reform (lasting through 2008). No funding was attached to this appointment, however, which reduced the scope of activities but preserved independence.

Within a couple weeks of the appointment, the Monitor staff discovered that monitoring the implementation of the CERP Report was not the best use of our time. Though we had formulated a set of metrics for election performance (including technical equipment, such as the voter registration and tabulation databases), and planned to take an objective, arms-length role at the BOE, we found that staff often could not decide (or disagreed) on how to implement a CERP recommendation. We found deep morale problems and disagreement with the administrative reshuffling of positions, and a disbelief that much could change in their achievement. It did not seem that the BOE was ready to be monitored—it needed to be *supported* in achieving better understandings of the causes of election problems and in implementing sound improvements.

By late September 2006, we had concluded that since our overarching mission and charge as Monitor was to facilitate the improvement of election performance, we should modify our approach. We proposed to focus on 2 major areas and simply work with the managers and staff (sometimes vendors/contractors as well) to (1) flag developing risks to the November election and (2) offer suggestions for mitigating or eliminating those risks. We sought for the Center's staff to be sounding boards for the BOE managers in their new performance efforts, their frustrations, and their efforts aimed at removing perceived internal managerial impediments to improved performance. In short, we tried to provide a helping hand and morale boost.

During the fall of 2006 our Monitor work concentrated on two significant areas of election risk: (a) technical issues relating to accuracy, reliability and security with both the voter registration database and the voting systems; and (b) pollworker staffing and training, and conduct of polling place activities. We worked assiduously to facilitate internal improvements without becoming whistleblowers. Wherever possible, we tried to have the internal staff take the lead for the initiatives and the corrections of problems. We credited the staff and managers publicly for the efforts and achievements they were making. And by many measures, the November 2006 election was a far more successful election than was the May primary. The corner had been turned.

C. Technical Monitoring

For the CERP investigation, I had hired two software engineer-law students. These two CERP investigators had developed separate specialties in the DIMS voter registration database and in the GEMS election management system – which generated the electronic ballots and tabulated both optical scan and DRE electronic ballots. In the fall 2006 technical monitoring, we were joined by Tom Ryan, a law student who was a Senior Technical Consultant for a major international computer-technical systems consulting firm. (The resumes of two of these staff members can be found the California Secretary of State's Voting System Review webpage, under Documentation Review. http://www.sos.ca.gov/elections/elections_vsr.htm Our technical monitoring team possessed significant expertise in software, software industry practices, database structure and operations, stress testing of technical systems, and computer security, in addition to having general legal and Election Law knowledge.

As a team, we identified the areas that posed the greatest risks to the accuracy of the reported election results, and reliability-stability of the equipment. On site, we reviewed:

o the networking apparatus for the central count scanners;
o the physical and digital security plans;
o the L & A testing of equipment (both plans and conduct of the testing);
o the early scanning of absentee ballots and protection of the voting data;

o the DRE memory card tabulation activities on Election Day night into the morning.

In advance of the election, we reviewed the proposed Security Plan and offered amendments that promoted greater transparency, a solid chain of custody and record of access to tabulation equipment, and a record of any server events that might indicate the election results accuracy might have been injured.

II. Monitoring Relevant to Voting Systems Incident Reporting

We learned that the Diebold GEMS server had been crashing at least once a day for several weeks before the election. The team knew a number of major issues can arise for data accuracy when servers crash. Tom Ryan conducted additional research on the GEMS software as well. Tom outlined a series of concerns related to the GEMS architecture and specifically its use of the Microsoft JET "engine." The entire technical team reviewed these concerns and the supporting research. We then requested the vendor to provide procedural protection guidance to the BOE ballot and tabulation managers, so they would know what indicators might suggest serious problems with the tabulation, and what remedial actions to take. (One major Memorandum is attached here as Appendix A.) Given the BOE's legal duty to provide an accurate election results report, we considered it essential that the vendor disclose to the BOE the recommended steps to protect election tabulation accuracy.

As background, Diebold's use of JET might be analogized to building in 2003 a finely equipped racing automobile but instead of installing a circa 2003 engine, the manufacturer placed a 1973 engine under the hood. No matter how well designed the interior and the dashboard, the car would still have an antiquated engine, and would be operationally limited by it. Microsoft reported these JET flaws on its website so all users would be informed, and specifically cautioned against use of JET for applications where high accuracy and security are priorities. (These Microsoft notices are copied into the Memo attached here as Appendix A.) Microsoft particularly cautioned that database corruption could not be prevented. This point means the data can become degraded -- corrupted, inaccurate – simply because of technical events and operations, without any deliberate intrusions or "hacking." We believed it essential to bring this information to the BOE's attention and to the vendor.

In an October 2006 conference call with the vendor's GEMS architects and engineers, plus BOE managers and one BOE Board Member, the vendor stated that JET problems could not and had never affected GEMS operations. This was tantamount to saying that because the car was manufactured in 2003, the thirty-year-old engine's flaws would not affect the driving and gas consumption of the car. This was not a defensible technical position but this was the vendor's position. (See Appendix A to this memo for a further discussion of the issues that led to the conference call).

At least two serious JET deficiencies had not been the subject of vendor disclosures and directions to election jurisdiction customers: (1) the 2 gigabyte data limit, after which data corruption could occur, and (2) the small number of "concurrent operations" that could occur without risking data corruption. The vendor had not provided directions to customers to monitor the database growth at all times during tabulations, lest the 2 gig limit was exceeded, and also had not flagged what types of server operations could cause dramatic database growth. We later learned that in the May 2006 primary, the 2 gig limit had been exceeded, and still the vendor had not offered disclosures and mitigations to the BOE or presumably other election customers.

The vendor also had not disclosed to customers, and may not have even been aware of, the potential impact of server crashes and freezes on election results accuracy. Because the BOE sustained at least one crash and one freeze during unofficial tabulations, we requested and eventually received permission to conduct a review of the unofficial results database. With vendor representatives present, Tom Ryan identified a variety of indicators of possible data corruption, including time/date stamps returned to Unix time. I hand-delivered a one-page summary of findings to the BOE Board Members. This memo was published in the Cuyahoga Collaborative Public Audit and is provided in Appendix B to this statement.

In April 2008, Premier Election Systems, Inc., Diebold's successor corporation, acknowledged in a Product Advisory Notice to its customers one of the points we had brought to its attention approximately 18 months previously. This notice issued only after an Ohio BOE had experienced some tabulation problems, the Ohio Secretary of State's office had become involved, and an independent test of GEMS occurred. It appears that this PAN is deficient in certain respects, however, yet there is no process for generating and publishing technical evaluations of it, for the benefit of election jurisdictions and voters.

The EAC was not involved in any of the events or reporting discussed above, and as far as I know, has made no effort to learn of field-developed voting system information such as that the Monitor reported to the local officials and to the vendor. A series of public efforts, including the VotersUnite.org website and the Election Protection Coalition incident reporting system (under the umbrella led by the Lawyers Committee for Civil Rights Under Law) have substituted for the EAC's role. *See A Preliminary Analysis of OVL Voting Equipment Reports*, retrieved November 14, 2008, from http://josephhall.org/OVL2008/.

I believe the work that we performed in Cuyahoga County could have been leveraged for national benefit had the EAC chosen to create the voting systems events clearinghouse, and still can. We might have posted the information on a blog but I am a supporter of government agencies fulfilling their role for the public. It does seem that the EAC has sidestepped voting system issues, and missed many opportunities for empowering officials and voters to help assure election accuracy. This hearing is a signal step forward, and I am hopeful that the EAC will develop a voting system tracking apparatus.

III.   EAC's Role in Tracking Voter Technology Performance

As other witnesses have commented on the EAC's jurisdictional authority, I will sidestep this question except to say that I have no doubt from my review and teaching of HAVA in Election Law courses that the EAC has ample statutory authority for tracking voting system performance. Even conceding a slight ambiguity, the fact that HAVA monies paid for a great deal of this equipment and also that the EAC is the only federal agency with any reporting or clearinghouse functions, militates in favor of the EAC's setting up a effective incident and performance tracking system.

But other efforts are also needed. Or instance, most of the other important technical limitations of JET have not been discussed in vendor PANs with recommended and effective mitigations.

A. Voting System Performance Clearinghouse

I would suggest that to balance the interests of the voters, election officials, and the voting system vendor/manufacturers that the EAC construct a reporting system "clearinghouse" that ***allows any witness (including voters and their voting assistants—as for the disabled voters), election official (including poll workers), and vendors to report equipment events.*** The EAC can state the disclaimer that it does not verify any equipment events but does verify that the event or issue has been reported to the local officials before being posted on the EAC inventory.

Additional features I would recommend:

o The EAC requests any "event/report submitters" to report the event to the local election officials at the same time (for instance in a cc) as to the EAC.

o The EAC website include a column for the election jurisdiction's response, which might be to verify that the problem occurred and the action that has been taken, or might say that they were unable to verify that the problem had occurred.

o The EAC website include a column for vendor response, if the vendors desire this opportunity.

o The EAC or NIST develop the technical staff capability to identify for each vendor component constellations of events or problems, which they then (a) discuss with officials and technical or academic consultants the appropriate best practice mitigations, (b) facilitate issuance of appropriate and prompt PANs (which it posts for election officials), and other actions that (c) demonstrate a proactive approach to achieving voting system accuracy.

o The EAC request that the Chief Election Officers of each State cooperate in the voting system performance inventory, and specifically authorize and encourage their local jurisdictions to report voting system equipment events to the EAC as well as to the State officials, and not require local reports to be filed first with the State for its approval as a prerequisite for a local report to the EAC.

B. Other EAC Voting System Performance Activities are Possible

Even with the institution of a voting system clearinghouse, significant gaps remain in the EAC's action program for supporting for election officials in achieving election accuracy, and in assuring that fundamental voting rights are protected. As food for thought for the future, and preferably near future:

1. PANs Inventory The EAC has not collected the voting system vendor Product Advisory Notices and provided a one-location electronic access point for election officials and voters. This is an essential for election transparency and for voters seeking to assure that their local officials are acting on the latest information. For jurisdictions that are considering changing vendors, the PANs are needed. The EAC could initiate this PAN clearinghouse immediately.

2. Computer–Based Election Equipment Best Practices Election officials should not have to be well versed in computer knowledge, but the current generation of election equipment and its vendor documentation mean that we have many electoral dangers that are largely unknown to

election officials. The EAC could consider working with academics in computer science and engineering, computer security, and other relevant academics in creating curricula on best practices dealing with current generation computer-based election equipment. Some of this instruction could take the form of DVDs that would be widely available to officials. It is deeply troubling, for instance, that some vendors have not disclosed the import of server events such as crashes on election tabulation accuracy, and what the "next steps" should be.

3. <u>Translating Voting Systems Scholarship for Election Officials</u> When scholarly studies are performed that relate to voting system performance in core areas, or that provide "mitigations" that can correct or prevent performance flaws, the work is largely unavailable to officials. As yet no federal mediating institution with the necessary technical qualifications is translating this material into useable information for election officials. The EAC could achieve this function through its clearinghouse functions. E.g., studies regarding

- <u>Voting System Flaws with Performance Implications</u> Tom Ryan and I published a peer-reviewed paper detailing a number of GEMS design issues that can result in inaccurate election results reports, but mitigations have not been designed and distributed to election officials by the vendor or a government agency. See *GEMS Tabulation Database Design Issues in Relation to Voting Systems Certification Standards,* http://www.usenix.org/events/evt07/tech/

- <u>Voting System Mitigations</u> When studies are published that outline mitigations for current voting system flaws, such as *You Go to Elections with the Voting System You Have: Stop-Gap Mitigations for Deployed Voting Systems,* by J. Alex Halderman, Princeton University; Eric Rescorla, RTFM, Inc.; Hovav Shacham, University of California, San Diego; David Wagner, University of California, Berkeley, http://www.usenix.org/events/evt08/tech/ some federal entity, most likely the EAC, needs to make this information available or to process it in a manner that is usable by election officials.

- <u>Voting systems studies</u> commissioned by election officials, including the California TTBR (Top to Bottom Review), the UConn, and EVEREST reports, and others, need to be translated into useable information at the level of practice—for instance, for poll workers training and for professional election officials. In the TTBR Documentation Reviews, researchers (including myself) found, for instance, that vendors supplied profoundly insufficient information to election officials on how to protect the security of the voting equipment and the servers. The federal entity that is charged with promoting election administrative success—the EAC–could help to leverage the work for national benefit.

4. <u>Voting System Forensics</u> Many troubling and important technical events are occurring with the current generation of election equipment, yet the EAC has not offered forensics information for election officials to learn the indicators and "next steps" to protect election accuracy. *See, e.g.,* the election forensics paper that the American Bar Association posted on its website in several locations to assist election officials and their lawyers in achieving an accurate election. *Resolving the Unexpected in Elections: Election Officials' Options,* posted at www.electionexcellence.org (4 computer scientists and myself as co-authors, downloaded over 400 times prior to the November 2008 election).

- **Voting System Forensics Reports** in the aftermath of an election, such as the Princeton Sequoia report that issued in October 2008, see, e.g., http://citp.princeton.edu/voting/advantage/ and the SAIT (Florida State University) report on the controversial Florida CD-13 race in 2006 http://election.dos.state.fl.us/reports/pdf/FinalAudRepSAIT.pdf need to be gathered in one inventory and grouped by vendor so that the information is readily available to officials.

  - **EAC Guidance on Structuring a Forensics Review** could issue from the EAC, with assistance from the academics and others who have been involved in these efforts.

5. **Post-election Auditing** has been identified as the single most effective mitigation for current generation voting system deficiencies. The EAC has not yet started a clearinghouse on auditing models, experiences, and emerging best practices, but this would be a major advance.

6. **Voting system procurements and contracting** The EAC has not undertaken efforts to facilitate best practices in voting system procurements and contracting, which is a tremendous need. A significant amount of federal funding has been less than beneficially used because the local officials lacked information on how to evaluate what type of equipment would work best for a particular jurisdiction, how much of it is needed (backup equipment), and more. The ancillary equipment needed to allow the core equipment to function is also not well known. I have personally facilitated the efforts of three jurisdictions in learning about requests to pre-test equipment (not merely have it demonstrated), criteria of fitness for a particular jurisdiction, and contractual clauses that will protect voters and taxpayers' financial and accountability interests.

All the other good work and investments that the EAC and that state and local election officials make in improving their election processes is for naught if the technical equipment is not functioning in a manner that produces voter access and accurate totals.

The EAC could become far more proactive for the voters and election officials, and facilitate a far better electoral administrative system, by removing the "firewall" between the NASED-qualified equipment and that of the EAC's new certification system. That NASED-qualified equipment is being used in federal elections and much of it was purchased with EAC-distributed HAVA funds. Surely the EAC will actively seek to provide relevant information to election officials and the public so all might promote the most accurate and accessible elections possible.

Thank you for the opportunity to discuss voting system performance tracking with you. I am happy to be available for further discussion about any of these suggestions.   Appendices follow.

****

Appendices to Candice Hoke Testimony to the EAC, Dec. 8, 2008

Appendix A

Memo

TO: Project Director Tom Hayes

FROM: Candice Hoke, for the Monitor

DATE: **Expanded and Revised** – October 29, 2006
               (*Substitute Memo* for those dated 10/26/06 & 10/27/06)

RE: **Tabulation Server Concerns: Database Stability and Accuracy,
               Security, & System Testing**

      As you requested during a meeting concerning these issues on Friday morning, the memo we provided to you on Friday is now expanded and revised to include the points we discussed orally.

Core Concern: The tabulation database that Diebold supplied to the CCBOE as part of its election management system has data limits that will be exceeded by the absentee ballots scanned into it on Election Day.   We understand that there is no official vendor documentation and recommendation to the Board on what to do in this situation. Your Diebold technical consultant on site has identified a strategy that may work, but it has apparently not been thoroughly tested and documented as an officially approved and effective technique that does not harm or change the voting data that has been scanned into the system. There is an SOS Directive that might be violated, in spirit if not in explicit terms, if such a procedure is used on the tabulation server without following certain specified steps in advance.

      We wanted to bring this to your attention because it impacts two major constellations of issues: (1) the accuracy and security of the vote counts, and (2) the protection the CCBOE (and its staff/technical workers) might desire in advance of Election Day. Steps can be taken to provide employees' protection from any accusations can might be made that the CCBOE/its staff have taken inappropriate or invalid steps and thus compromised the vote tabulations. Each of these concerns are of the highest severity in the view of our most advanced software engineer who specializes in database contingency planning and testing for Fortune 500 companies with data-intensive operations.

      We want to share the information we have gathered so that the CCBOE can decide what it might want to do. For instance, posing some questions to Diebold Election Systems or your legal counsel might be considered.

Caveats: We recognize that this is a fluid situation and that the information we gathered previously and present here may have become superseded, especially since I had orally flagged some concerns mid-week to Director Vu and later to Tom Hayes. Additionally, it is crucial to note that none of this memo is a criticism of any steps or planning efforts that have been taken by Mr.

Irizarry, Mr. Jaffe, or Mr. Bellis. The vendor appears to have left the CCBOE between a rock and a hard place by not identifying and resolving some of these obvious and foreseeable issues promptly. These gentlemen have been working to generate a technical and managerial solution in a very short time. But the risks that may follow are significant, potentially for the CCBOE and themselves personally, and thus we wanted to bring forward this information. Fortunately, the CCBOE has enough time to be able to handle these problems in some manner—even if it is not optimal. A longer range remedial strategy might be warranted after the election.

I've organized the memo so that the key points for us "average folks" (who are not software/IT specialists) can be found in the headings and bullets; we can skip the numbered subpoints which are provided in technical language for the IT specialists (who might be bothered by the translation into the nontechnical and somewhat imprecise language in the bullet points above).

A. <u>Data Limitations of the GEMS Tabulation Database</u>

- GEMS uses the Microsoft JET database "engine," which has a 2 gigabyte limit on the amount of data it can manage.

    <u>Tech 1</u> GEMS utilizes database technology known as Microsoft Database Joint Engine Technology (JET). JET technology has been used by DESI to create a custom database by using the programming tools known as Microsoft Data Access Components (MDAC).

    <u>Tech 2</u> JET has a known and documented limitation on the maximum file size of the database. This limitation is 2 gigabytes. The limitation is documented by Microsoft and included as an attachment to this Memo.

    <u>Tech 3</u> DESI's use of JET limits the size of the tabulation database to 2 gigabytes.

- If the database is compelled to accept more data than its limit, the behaviour of the GEMS server is unpredictable, but can include:

    -- corruption or loss of election data
    -- corruption of essential operating system components, possibly leading to crashes and
         overall instability.

- Based on CCBOE tests and estimates, it appears that that the GEMS database will grow well beyond the 2GB limit during the absentee ballot scanning procedures absent regular compaction (reduction) of the database; CCBOE estimates are that the 2GB limit will be approached every 1-2 hours of scanning.

- The problems associated with JET are so severe and so numerous that Microsoft no longer sells or supports this product. Current versions of Microsoft database technologies do not include JET. One example of a major problem in JET that Microsoft has noted:

    "**Database Corruption** When Microsoft Access databases (using the Jet engine) encounter an error or connection problem, the database may become corrupt. A corrupt database generally locks out all users of the database, and generally results in business disruption and infrequent data loss."

"Microsoft Access databases (using the Jet engine) are susceptible to corruption for a number of reasons. . . . " [Bold in original; Microsoft Corp. documentation in Appendix to this Memo]

- The ramifications of this "database corruption" on vote tabulations in the GEMS database are not known. Microsoft does not have any workaround or ways to prevent it.

- We understand that Diebold Election Systems (DESI) has not provided any written documentation to the CCBOE or in its standard training or other official materials on what measures to take when the vote tabulation database approaches the 2 GB limit. Indeed, from what we understand, DESI did not even flag this serious problem with their election management system in its documentation.

- The DESI technical consultant on-site at the CCBOE, Mr. Chris Bellis, recognizes the gravity of the 2 GB limit, and has searched within DESI for a solution. Mr. Bellis has identified an undocumented and unofficial procedure which he and Mr. Jaffe have discussed and tentatively plan to employ to reduce the CCBOE database size during absentee ballot scanning.

  Tech 4 In response to this anticipated and expected file size, ad hoc and undocumented procedures have been developed by some DESI employees/contractors elsewhere. Mr. Bellis has consulted with some of these individuals to identify and adapt a procedure for reducing the size of the expected CCBOE database. These procedures would then be undertaken by CCBOE employees on Election Day.

- DESI technicians have characterized this procedure as a "backup" operation, though this term is misleading when applied to CCBOE's situation.

  Tech 5: The "backup" may include some combination of data compression, storage optimization, and purging of data. JET offers tools which perform these functions programmatically through use of the JET Replication Objects API.

- Depending on the number of absentee ballots returned to the BOE before Saturday 11/4, and given that the 2 gigabyte limit is estimated by the CCBOE to be approached every 1-2 hours, some compression of the data will likely be occurring between 4 - 15 times on Election Day and more times thereafter as the remainder of absentee ballots are scanned. Each time the procedure is used, the entire database of vote tabulations is reduced in size, but the underlying procedures that are being performed are still not known. Most likely, the database is being compressed or optimized, but there is little to no information on the actual procedure that is occurring behind the scenes.

- The procedure or operation to shrink the database will require BOE staff to shut down the scanning process every time the 2 gigabyte limit is approached

- We understand DESI has provided no documentation on the procedure when it is run on election tabulations. Mr. Bellis also has said he does not know what occurs as a technical matter. With the number of unknowns about the operation and the underlying flaws in the Microsoft JET engine, it is not clear whether any voting data could be lost or corrupted, or in what ways.

11

- Use of undocumented, untested, and unapproved procedures may bring severe technical and legal risks to the Board. We fear that CCBOE employees who initiate undocumented, untested, and unapproved procedures on election vote tabulations may run the risk of charges for "tampering" with vote tabulations. Although an unlikely scenario, if there were major problems in this election, the use of untested and undocumented procedures in the midst of an election tabulation could raise the possibility of some personal criminal liability.

- Private sector companies in data intensive industries tend to engage in significant testing and documentation of all proposed operations so that they know precisely the impact of any operation on their databases before they go "live." This extensive testing and documentation provides the company with the opportunity to tweak or reject proposed "fixes" and thereby protects the valuable data from harm. Additionally, having documented and officially mandated procedures for dealing with certain occurrences also protects technical employees from unfair and professionally injurious allegations of tampering or other malfeasance.

- Without the extensive testing and documentation of any procedures that are hypothesized to solve a problem on crucial databases, it cannot be known whether there are any risks to the data when the operation is run or whether the overall risks of any database malfunctions (including crashes and freezes) are increased. It can be analogized to being a part of a pharmaceutical experiment with a test drug. It may work without serious side effects or might cause a stroke, but without the careful controlled tests, the likely impact will not be able to be known.

- It is important to note, however, that the shrinking of the database does not, by itself, suggest a loss of data contained in the file, and that any measure taken to prevent the database from growing beyond the 2GB limit will require some form of compaction operation.

- ***The compaction of the database is not in itself sinister and we do not want to be read as implying that it implies some malfeasance.*** The concerns are that the proposed process is an unofficial procedure, untested, and undocumented. The GEMS database requires manual intervention to prevent data overflow. If problems arise on Election Day regarding the integrity of the data, how will the BOE respond? How will Diebold respond? Will this procedure be identified as a potential source of data corruption? And if so, how will those database operators who implemented this procedure be characterized?

- Thus far, it seems the CCBOE has not engaged in any testing of this operation on its GEMS server to attempt to discover what it does to tabulation data, and we do not know if they have planned any testing of it, or have any non-DESI-affiliated consultant who can advise them how to structure such a testing operation;

- We do not know whether there is special DESI or other software that must be downloaded and installed for this procedure, or whether it makes use of components already installed as a part of GEMS. If it is the latter, the procedure would probably be using GEMS components or an available GEMS operation to achieve an objective for which the operation was not originally designed or intended.

- The Secretary of State has issued Directive 2005-23, which states in part:

  II.   Downloading Software
  a. Unless specifically authorized in writing and in advance by the Director and Deputy Director of the Board of Elections, no one shall download or install software on any voting device, tabulation device, election management system, … or any component of an Election Information System.

     A copy of the written authorization must be submitted and received by the Secretary of State prior to the actual download or installation of any software or component.

The Directive could be read as outlining at least part of the approach that could be utilized here—that the Director and Deputy Director provide written authorization for the operation, and that it be submitted to the SOS.   Although the Board's legal counsel would need to provide advice, it may be that this approach would help to protect the technical workers who are faced with the need to compact the database during tabulations.

- We do not know whether the May 06 primary tabulations of memory cards reached the 2GB limit and necessitated some form of database compaction, or whether the 2 GB limit was monitored at that time (and by whom). We do not know whether there was any contingency plan in place for May absentee ballots in case the 2 GB limit was approached, and if so, what the database management plan was.

Options for Dealing with the Database Limitations With so little time, the CCBOE's options are few. We can identify at least four sets of responses that might be valuable.

1. Questions that might be posed to DESI for official answers on how the CCBOE should deal with the 2 GB limit in light of the voting tabulation data that will exceed this limit;   and, for any testing/results and documentation that has been done on the operation that is suggested on the internal bulletin boards or by DESI technicians in oral communications.

2. Questions that might be posed to the CCBOE legal counsel, including advice on the legality of using undocumented and untested procedures in the midst of election tabulations; any liabilities for those operators implementing the procedures; and, any authorizations internally or externally that should be sought before the election.

3. Simulation of the 2 GB limitation, and CCBOE testing of the procedure that is planned for use.

4. Creating written documents containing all server procedures to be used in the CCBOE on Election Day that are not a part of the official Diebold documentation, and obtaining the Director's and Deputy Director's authorization, plus providing notice to the SOS of all of these.   (And testing of these procedures in advance in a simulated election database.)

B. Scanner Network Security

- All the wires to the basement and the pink room generate open access to the server. Security questions probably need to be revisited and enhanced security might be contemplated. The SOS Directive may need to be consulted.

- Data intensive and security conscious private sector entities' "best practices" would include:

  o replicating the physical security measures used for the GEMS server in the glassed-in tabulation room for any point a network connection to the server exists;

  o implementing security measures immediately, because the infrastructure is now in place for remote access to the GEMS server;

  o implementing security procedures to govern physical access to the basement scanning room and network routers that match physical access to the tabulation room. Employees who currently do not have access to the tabulation room do, however, currently have access to the basement scanning room, and thus potentially have access to the GEMS server. Malicious software can be uploaded in advance into the GEMS server that could disrupt the election tabulations and greatly harm the chances of a prompt and accurate unofficial election result report.

C. GEMS Server Currently Needs Regular Rebooting

- When servers freeze up and crash, non-recoverable data errors can occur. We understand that GEMS crashes now approximately once a day even with no severe stress placed upon it.

- As far as we can discern, testing of the procedures to restore the GEMS database after a crash or freeze, and testing of the impact of a crash or freeze on election tabulation data has not occurred and has not been planned or recommended by Diebold. Thus, it is not known what will happen to the vote tabulation data when a crash, freeze, or restoration procedure occurs. Unless CCBOE can understand and document the impact on election data of any crash or exception condition, and a procedure to restore the database, the appropriate steps are for vote tabulation to start over from the beginning.

D. Stress Testing the Scanning Set-up

- A scientifically sound, realistic stress test has not been fashioned to determine the reliability, accuracy, and overall capabilities of the central count absentee ballot scanning system.   DESI has tested and verified the ability to link successfully 40 scanners together in a central count system. The CCBOE plan is to try to use 60 scanners simultaneously on Election Day.

> > Tech 6: The highest number of concurrent scanners tested by DESI is 40. CCBOE will be using 60 concurrent scanners on Election Day.

- Results from independently verified (and not relying on vendor recommendations as to the stresses to which their equipment should undergo) professionally designed stress testing will allow the CCBOE to make adjustments to the Election Day procedure, which may include scaling back the number of scanners. This stress test should be designed to ensure the new infrastructure installed by the CCBOE county is ready for Election Day.

> > Tech 7: A system stress test should be run that can check whether the untested number of concurrent scanners will not create conflicts within the system or local network that could lead to degraded data transmissions.

- Such a stress test cannot, however, verify that the GEMS system can perform with 60, or even 40 or 50 simultaneous optical scanners, for sixteen hours with only limited relief. A stress test run before Election Day will allow the BOE to address failures and limitations of their procedures, including logistical problems of coordinating temporary work staff. It will assist the CCBOE from scrambling for answers from DESI in the stress of an Election Day and allow the CCBOE managers to create appropriate contingency plans.

- But stress tests should be limited to investigating the procedures planned for Election Day by CCBOE.

> > Tech 8: The stress test should not include core product functionality as it is not the responsibility of the BOE to verify DESI has supplied functional software. Limited data checking should be performed, but this is not meant to replace the certification process DESI is required to undergo per the Secretary of State.

- The ability of the GEMS system to function correctly with more than 40 concurrent scanners remains an issue, but CCBOE is limited in its ability to address or resolve GEMS product limitations this close to an election.

- Time remains, however, for being able to fashion and conduct sound stress testing, instead of having the first real stress test on Election Day.

Additional Recommendations:

1. Consider inviting the monitor's software engineers with the appropriate specialties to provide free consultation to CCBOE Managers on what testing structures/procedures would be put into place in the private sector by high quality security conscious entities taking into account the short time remaining before the election, and any obvious security measures that should be taken.

2. Document in writing all proposed GEMS operator interventions in advance of the election, with appropriate written CCBOE executive approvals.

3. On Election Day, and during any tabulations for the unofficial or the official/certified count, document all GEMS interventions on an external paper log (including the operator, real time/date, witness, and procedure taken (perhaps by noting the intervention number stated on list in 2 above).

4. Invite the Monitor (via software engineers/specially trained and Project Manager-vetted individuals) to supply independent verification of tabulation interventions on Election Day.

5. Review and revise the draft CCBOE Security Policy; modify to strengthen in light of the basement scanning set-up, tabulation room verification of interventions, and other points above.

6. Generate an entire GEMS report before and after each compression operation, marking these with real time and initialling them, as well as sealing the reports for comparison later to discover any data disruptions that may have occurred from the undocumented procedure.

Relevant CERP Findings that identified some of these risks:

> **2.108 Finding:** Core aspects of the GEMS architecture are not well suited to CCBOE's present needs and, further, cast doubt upon its capacity to meet future needs. GEMS relies on a Microsoft Access database. MS Access is typically used for home and small business database applications and as a tool for rapid prototyping. It is not marketed as a robust, scalable and secure enterprise database solution such as Microsoft's SQL Server and numerous products from other vendors. The use of this more-limited underlying database system constrains GEMS' capacity for intrinsic security and auditability, concurrent usage, and system performance. … GEMS architecture does not permit practical concurrent usage.
> Anticipated increases in the complexity of Cuyahoga County's election needs (with factors such as multiple ballot languages on the horizon), may further tax the GEMS design and its underlying Access database management system.

> **2.109 Finding:** A usage restriction on GEMS recommended by DESI and promulgated by Secretary of State, permits the use of only one computer (the GEMS server itself) for GEMS data entry, tabulation and reporting. At all levels, this restriction is presented as a security measure, and it does undeniably reduce to some degree the potential for tampering with the insecure GEMS database. It is important to note, however, that the GEMS architecture would not efficiently support multiple clients performing concurrent resource-intensive operations even if security was not an issue**.**

Appendix: Microsoft Corporation Documentation for IT Professionals

We can supply the full documentation/sources if desired.

Access and the Jet Engine

Access has its own database engine—the Microsoft Jet database engine. **Jet is designed as a file share database that supports single and multi-user database applications with databases up to 2 gigabytes (GB) in size.**

Access is more than a database engine. It is a development environment that allows users to design queries, create forms and reports, and write macros and Visual Basic code to automate the overall application. In its default configuration, Access uses Jet internally to store its design objects such as forms, reports, macros, and code, and also uses Jet to store all table data.

One of the key benefits of Access when upsizing is that you can redesign your application to continue to use the forms, reports, macros, and code you have already designed in Access, and replace the Jet engine with SQL Server for your data storage. This allows the ease of use of Access, with the reliability and security of SQL Server.

Copyright [for above]

****

Limitations of *Access*   [compares to SQL Server, another Microsoft database product]

Although it has many advantages, Access has limitations that prevent its use in some cases.. . .

Scalability

One Access database (using the Jet engine) is limited to 2 gigabytes (GB). If a database exceeds that, the solution can't be entirely solved by Access. Access databases also have problems with too many simultaneous users. The number depends on what they are doing.

If there's a lot of data, SQL Server is the better choice. SQL Server also supports more users and traffic, not only through its limited bandwidth traffic, but also with the ability to improve performance, by investing more in hardware through more memory, more CPUs, and more computers. This option is not available for file server databases like Access.

Related to scalability is the option of consolidating multiple Access databases into one large SQL Server database. Although you may combine several Access databases into one, if the size, security, or other requirements exceed Access capabilities, SQL Server is ideal. Having one large repository has the potential for using Business Intelligence (BI) tools and Web publishing with significant business and operational opportunities.

Security

Although Access databases **(using the Jet engine)** can be password protected and encrypted, **these databases do not have the same level of security** as SQL Server or mainframe database systems. . . .

Data Integrity

Similarly, **data integrity and recovery is not as robust on file-based databases using Jet,** compared to SQL Server with its triggers, transaction logs, and repair processes.

File server databases using Jet may become corrupt and require regular maintenance to maintain optimal results. Even with maintenance, the chance of failure is much higher than with SQL Server.

The Total Visual Agent (http://www.fmsinc.com/products/agent/) product addresses the administrative needs of daily database maintenance (compacts and backups), but it's not the same as the built-in features of SQL Server.

Backups

Access databases (using the **Jet** engine) are easy to back up (copy the .mdb file). However, these databases require user initiative, unless an automated process or tool, like Total Visual Agent, is in place.

If the Access database is open and the data is changing, **it cannot be backed up while users are in it.** is is a major problem, if the database is critical and used 24 hours a day, seven days a week. . . .

Transaction Logs and Rollbacks

If you need to know who modified what data, and undo changes, SQL Server's built-in features and triggers support this.

An Access application can try to replicate the tracking of changes by managing user interaction with the data. However, it would require programming and could not be managed at the core data level. Mistakes in the application or other applications in contact with the Access data **could cause data changes that are not documented. There are also no rollbacks in Access after a transaction is committed**.

The above from:

Microsoft Access or Microsoft SQL Server: What's Right in Your Organization? SQL Server Technical Article December 2004, from Microsoft

Cuyahoga Collaborative Public Audit of the November 2006 General Election,
Appendices 16-17, found at www.csuohio.edu/cei/ and permanently at www.electionexcellence.org

Appendix 16
Indicators that MAY Show Database Corruption
(Discovered in the Monitor's Review of CCBOE *Unofficial* Results Database on 11/17/06)[10]

1. Table element entries were missing date/time stamps of when the information was entered.

2. Table element entries had date/time stamps of January 1, 1970, which is the epoch (zero-point) of UNIX time.

3. In an email dated November 3rd, 2006, from DESI's Talbot Iredale, he claimed

"Accounting for transaction overhead, I do not expect the database to grow by more
than 100 MB during absentee processing. However this will vary dependent on what
other other activities (printing, reports, etc.) occur during the processing."

The database grew to a size greater than 100 MB for absentee processing and a size above 1000
MB for the full election. What happened? Why were the estimations wrong? Precision is very
important, especially when dealing with votes. Where else were DESI calculations imprecise?

4. Vote totals in two separate database tables held different values. DESI has provided a
response, but as of yet, this response has not been tested or verified.

5. In an email from Chris Bellis dated Monday, November 20, 2006, Mr. Bellis summarized the
"large amount of concurrent activity" that was occurring on the GEMS server on election night.
This included DRE uploads, the JResults server running, the AVServer running, and Digital
Guardian running, all interacting with the database in varying functions. In a subsequent email
from Jessica Hiner, dated Sunday, November 26, 2006, Ms. Hiner stated "In the context of an
online system with many users, Jet would not be an appropriate choice, but that is not how we
use it."

It appears in DESI's own words, Hiner acknowledges that when there is a large amount of
concurrent activity, Jet database corruption can occur. Chris Bellis has said that on election night,
there was a lot of concurrent activity on the server. Taking these two statements together, it would
seem very possible that corruption may have occurred.

Microsoft's own documentation has stated that database corruption within JET is unavoidable.
This statement is without qualifiers. Normal operation of the Jet database includes corruption.

Appendix 17
Excerpt from Microsoft Documentation on JET-Access Databases
(emphasis added)

Security
Although Access databases (using the Jet engine) can be password protected and encrypted, **these databases do not have the same level of security** as SQL Server or mainframe database systems. **If data security is critical**, a SQL Server solution is the better choice….   SQL Server allows distributed data in a controlled and highly secure manner.

Data Integrity
Similarly, **data integrity and recovery is not as robust on file-based databases using Jet….**
File server **databases using Jet may become corrupt** and require regular maintenance to maintain optimal results. **Even with maintenance, the chance of failure is much higher** than with SQL Server.   ….

Transaction Logs and Rollbacks
If you need to know who modified what data, and undo changes, SQL Server's built-in features and triggers support this *[but not Access using JET—ed.]*
An Access application can try to replicate the tracking of changes by managing user interaction with the data. However, it would require programming and could not be managed at the core data level. **Mistakes in the application or other applications in contact with the Access data could cause data changes that are not documented**. There are **also no rollbacks** *[opportunities to "undo" the operation—ed.]* **in Access after a transaction is committed**.

The above paragraphs can be found in *Microsoft Access or SQL Server: What's Right in Your Organization?* at
 http://www.microsoft.com/sql/solutions/migration/access/compare-access.mspx