Cleveland State University
Center for Election Integrity

MEMO

To: Cuyahoga County Board of Elections Board Members;
Cuyahoga County Commissioners Board Members (c/o County Administrator
Dennis Madden)

FROM: Candice Hoke, for the CSU Center for Election Integrity/
Monitor of Cuyahoga Election Reform

DATE: January 8, 2007

RE: Monitor Report: Possible Legal Noncompliance in the November 2006 Election

---

To fulfill our duty as the two public Boards' designated agent for election improvement monitoring, we submit for your consideration this memo. It identifies points of possible legal noncompliance that have come to the Monitor's attention in the midst of monitoring the fall 2006 federal election cycle. A number of these points are already known to the CCBOE Board Members but are collected here primarily for convenience. It does not purport to be an exhaustive inventory of possible legal noncompliance as this is not the task for which the Monitor was appointed. But we have a duty to relate to the principals any information that we obtain in the course of our work that bears on your own legal duties. We present these concerns here to fulfill our duty of full disclosure as agents of the Boards.

Some of these issues have already received some Board or media attention. For instance, CCBOE staff have been tasked with reviewing and documenting some previously discovered legal compliance problems, especially concerning the discrepancies between the precinct voter registry sign-ins and the numbers of ballots cast at the precincts on Election Day. Other topics presented here have not as yet received managerial attention and redress.

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/

This memo identifies potential legal noncompliance in these areas:

- Erroneous Voter Registration Deletions
- Poll Workers and Polling Places
- Legally Mandated "Seals" for Ballot Security
- Inconsistencies Between Numbers of Voters Signing Precinct Registry and Ballots Cast
- Legal Eligibility of Certain Employees for Their Job Assignments
- Election Tabulation and Related Technical and Security Issues

We endeavor here to identify facts that may raise some important legal questions and may warrant additional investigation or Board reports. We do not offer legal conclusions because you have legal counsel to whom you may refer any legal matters and because all the relevant facts have not yet been gathered. We include some citations to legal authority where they may aid in understanding the issues raised but this is not designed to be a legal meroandum.

An Appendix that contains some supporting factual documentation can be found in a separate attachment to the email enclosing this Memo.

1. Erroneous Voter Registration Deletions

This past fall, voter advocacy organizations, including the Greater Cleveland Voter Coalition and "election protection" entities, again testified to the CCBOE expressing concerns that voter registration records may have been dropped from the registration rolls.[1] In a conversation with Candidate and Voter Services (CVS) Manager Mike DeFranco, whose department handles voter registration, Mr. DeFranco said that he believes that a major, if not exclusive, reason for the lost voter records lies in the "merge records" function of the DIMS registration software.[2]

The CERP Final Report (pages 31-32) reviews some lost voter registration problems that have been documented by the CVS managers. One feature that the DIMS software does not include is an "undo" button or any other mechanism to recover or permit a quality control check for any voter registration records that were erroneously deleted when merged. In addition to records lost to erroneous merges, DIMS does not include an archive of deleted voter registration records, from

[1] Loss of a voter's registration record not only means that the voter is not permitted to vote but also that the recorded voting history is deleted and unrecoverable.

[2] In certain cases, a single elector may have two or more entries in the registration database due to, for example, a change of address within the county or a change of name. DIMS' "merge records" feature allows registration personnel to consolidate the elector's multiple entries into a single entry containing all relevant data. With the merging feature in DIMS, upon completion of a merger of two voter registration records, the original registrations are deleted entirely rather than archived and therefore cannot be recovered. If, due to a mistake or a mere misplaced keystroke, two registration records are merged which should not have been merged, the original registrations are lost and cannot be retrieved. Furthermore, with no record of the lost registrations, no auditing or quality control checking can be performed to detect cases of voters erroneously deleted from the registration database

merger or otherwise. Without an archive of the dropped or deleted registrations, whether a product of proper removal or merging, operator error or software defect, the CCBOE staff cannot evaluate the dropped registrations and restore those that were erroneously deleted from the registration rolls.

Diebold Election Systems, Inc. (DESI) promised that the merged voter function would be improved with an "undo" feature (a March 2006 publication; CERP Report at 2.2, page 32). Mr. DeFranco informed us that this capability has still not been added to the DIMS software, and that the problems have persisted. He stated that DESI keeps promising that the function will be coming.

Although DIMS problems were documented in the CERP Final Report (dated July 20, 2006), the CCBOE's upper management did not place inquiry into or correction of lost voter registrations in the list of essential foci for redress this fall before the November 2006 election. They also have not commenced or planned an independent technical assessment to determine both the full range of cause(s) for lost registrations, or the scope and rate of lost voter registration records. No concerted remedial planning for DIMS or for protecting the voter registration database has occurred as yet,[3] Nor, as far as Mr. DeFranco can discern, has CCBOE management pressured the vendor to correct the problems and perform on its promise. Given the documentation of the lost voter registrations dating back to the DIMS installation in August 2004, the CCBOE's failure to act to remedy the voter registration losses may constitute a serious breach of CCBOE's legal duty to safeguard voter registration records.

Because of his concern over the lost voter registration records, Mr. DeFranco has instituted some stopgap internal policies and procedures in order to prevent loss of voter records that occur by use of the merged voter function. He stated he has issued directions to departmental staff that prohibit any use of the merged voter function on the DIMS system. Mr. DeFranco's prohibition, as he underscored to the Monitor, hinders compliance with another more regulatory portion of election law: the direction to eliminate duplicate voter registration records. Pending the arrival and installation of the long-promised DIMS upgrade (for the undo feature), or some other remedy, Mr. DeFranco has chosen not to run the risk of losing on an irretrievably permanent basis voter registration records.

Mr. DeFranco's action to bar merged voter operations may assist in limiting CCBOE liability for it demonstrates some proactive effort to halt the loss of voter registration records. Such a proactive approach, if adopted at higher levels of CCBOE management, could further reduce possible liability and yield greater progress toward protecting registration records. The CCBOE Board's recent tasking of the Monitor with undertaking technical performance reviews also evinces a more proactive approach to safeguarding voter registration records.

[3] The Monitor's proposal to commence vendor and technical systems reviews (that the CCBOE Board approved on December 18, 2006), if funded, should permit these assessments to move forward.

Some Federal and State Statutes Potentially Applicable

Voting Rights Act (as amended in 2006), specifically 42 U.S.C. § 1971(a):

> (2) No person acting under color of law shall –
>
> ....
>
> (B) deny the right of any individual to vote in any election because of an error or omission on any record or paper relating to any application, registration, or other act requisite to voting....

National Voter Registration Act, 42 U.S.C. §§ 1973gg-1 et seq., especially § 1972gg-6.

Help America Vote Act, especially 42 U.S.C. § 15483.

Ohio Election Law: O.R.C. §§ 3503.11- 3503.33 (Ohio's primary voter registration laws)

Some of the above-cited federal statutes expressly authorize a private party/citizen suit for certain statutory violations and others have been ruled to provide the substantive law that can ground a Section 1983 suit. The Ohio Secretary of State and potentially the Ohio Attorney General have the capacity to initiate investigations and seek to impose remedial measures for certain types of violations. Federal investigations by the Attorney General or by the U.S. Attorney may be authorized. Fines, damages, and legal fees in any litigation surrounding noncompliance would likely be far more extensive than would the costs of bringing CCBOE into compliance with applicable law.

2. Pollworker and Polling Place Issues

Ohio statutes specify in detail certain requirements for the staffing and functioning of Election Day polling places. Administrator Jane Platten was "re-tasked" in late August with managing poll worker recruitment, training and evaluations in addition to her other duties. Deputy Director Gwen Dillingham was re-tasked with managing the administrative division or "pod" that included preparing the touchscreen voting devices and voting locations for the election.

a. *Poll Worker Issues*

Ms. Platten instructed the Poll Worker Department managers that she expected the department's staffing and training activities to comply with governing law. She was aware that previously there had been little managerial emphasis on legal compliance but, consistent with the CERP Final Report, stressed this departmental obligation. Reportedly, she has also held certain staff accountable for failing to comply with the statutory requirements for pollworker appointments.

Despite these administrative efforts, it appears that compliance with various Ohio legal standards governing the staffing of polling places may not have been achieved. The Monitor received a number of reports from its Election Day monitoring staff, from precinct judges, and from the CCBOE departmental managers (including Ms. Platten and Mr. Lally) that in many precincts staffing assignments did not satisfy these Ohio statutes:

> ***O.R.C. § 3501.22 (A)*** (requiring the appointment of four judges per precinct; on November 7th, some precincts were staffed with as few as two judges).
>
> ***O.R.C. § 3501.22 (A)*** (mandating that no more than one-half of the precinct judges be from the same political party; on November 7th, in some precincts, all two or three judges present were Democrats).
> ***O.R.C. § 3501.22(A)*** (requiring appointment of a presiding judge who is to be from precinct's "dominant political party"; on November 7th, some precincts had no presiding judge or with a presiding judge from the incorrect party for the precinct).
>
> ***O.R.C. § 3501.22(D)*** (permitting High School students to serve as precinct judges but restricting this to no more than 1 per precinct under 18 years of age; on November 7th some precincts had two High School students and perhaps (but not known with assurance) the student poll workers were not yet 18).
>
> ***O.R.C. § 3505.24*** (directing that precinct judges who assist voters in casting ballots number at least two, and that they be from 2 different parties; many precincts lacked even one Republican judge and thus when voters needed assistance, only one party's judge was able to help).

In conversations with Ms. Platten and with other managers who worked in the Poll Worker department during the Fall 2006 election cycle, they related that DIMS was used to store the poll worker personal information (such as political party, address, age, training test results, and prior election official experience) and their status/assignments (presiding judge, precinct assignment).

Unfortunately, problems occurred which the departmental managers believe to be due to both DIMS glitches and some operator errors. The Monitor has been informed that often, essential poll worker applicant information became scrambled, deleted, or lost in the system and in need of recovery. These problems were exacerbated by a DIMS upgrade that was installed during the election cycle, and by the discovery that the statutory requirements for the presiding judge's political party had not been satisfied by the department. Ms. Platten then required staff to amend poll worker assignments to comply with the statutory law. Staff data entry, however, led to inaccuracies when reassignments occurred.

The departmental managers also provided the Monitor with examples that suggested DIMS software glitches and design obstacles led to their receipt of erroneous reports concerning how many judges had been appointed from each party, and how many poll workers were available in reserve. Because the DIMS reports had apparently assured the departmental managers that all the poll worker judges and EDT positions had been filled, hundreds (if not several thousand– no accurate records were kept) of interested citizens were turned away from serving as polling place election workers in November. The more accurate DIMS reports of which polling places lacked judges or EDTs, and whether appropriate party assignments for presiding judges had been made, was not available until very close to the election. Still, even through Election Day and thereafter, the DIMS system included erroneous information about various polling place officials, and currently it is not completely known how or why these DIMS errors occurred.

Ms. Platten and Mr. Lally have been forthright with Monitor staff in identifying various legal compliance deficiencies. Their planning and organizational efforts for the February special election includes additional efforts to satisfy more fully the legal specifications for polling place staffing.

b. ***Polling Place/Voting Locations Issues***

"Voting Locations" at one time was a separate department managed by Brian Kaluscak. With the advent of e-voting, and especially the extensive testing and other preparations that have to be undertaken for the DRE touchscreen machines to be readied for transportation to the voting locations, his department was merged with the voting devices preparation functions to create the Election Support division located in the Warehouse. This division is also charged with preparing and packing the precinct supply bags.

Mr. Kaluscak has mentioned to the Monitor that he would like to follow up fully on the adequacy of voting locations but the intense time demands for testing and otherwise preparing the DRE touchscreen voting machines leave him little time for ensuring that the polling locations are meeting legal standards for voting.

The Monitor has received reports from the November election that legal standards that are not consistently met in some voting locations. A few of these legal standards are:

> ***O.C.R. § 3501.29(A):*** location adequate for providing voter privacy in casting ballots; adequate lighting over the voting compartments. (see also ***O.C.R. § 3599.20*** concerning the protections and penalties for violating the rights to a secret ballot)
>
> ***O.C.R. § 3501.29(B)***: disability access (other state and federal statutes also apply).

3. **Legally Mandated "Seals" for Ballot Security**

Many Ohio Election Law statutes mandate "sealed containers" for ballots. The policy underlying the statutes appears to be that to protect the electorate's interest in an accurate and fair election, significant restrictions on physical access to the ballots must be in place to minimize the opportunities for fraud and manipulation.

Instead of using statutorily specified seals on ballots containers or bins (although sometimes it does this as well), the CCBOE maintains under double lock and key at least three separate vaults/ rooms that can hold ballots, memory cards that hold voted ballot records, and other protected voting records. The double lock and key system is designed to require no fewer than two staff members who will act as independent watchdogs of the public interest whenever a ballot area is accessed.

In the CCBOE Ballot Department, the managers relate that the Republican and the Democratic keys are separated into different offices in an effort to require that any access to the tabulation room (or the basement scanning room) when it is locked always requires at least two staff members from two different political parties. Other managers have informed the Monitor that the location of the keys is widely known and that it is relatively easy for a solo staff member to gain unauthorized access to protected spaces.

On the third floor, where a vault of voted absentee ballots (AB) are stored, it is unclear internally which department has administrative responsibility for the keys and the voted ballots. The Monitor observed the following practices for storing the keys to this AB storage area:

- storing a Republican and Democratic staff key on *separate* key rings but side by side in the same unlocked key box in a main hallway (not public accessible);

- storing on one key ring *both* the Republican and the Democratic keys (in that same unlocked key box);

- not maintaining a paper/ink log system for determining who has the keys, who has gained access to the storage areas, etc. (This has been a problem elsewhere in the CCBOE as well.)

The key system as currently structured permits any one staff member, or even a contractor or consultant, to gain unauthorized and unsupervised access to voted and unvoted ballots, memory cards holding votes, and other sensitive materials. Structuring the key access in these ways may violate the Ohio statutes and any SOS Directives that require "sealed containers." E.g., ***O.C.R. § 3501.29*** (protections for recounts). We raised this problem with several Ballot Department managers and Administrator Irizarry, who expressed interest in resolving it.

4. <u>Inconsistencies Between Numbers of Voters Signing Precinct Registry and Ballots Cast</u>

To promote basic election fairness (including no dilution of valid voters' votes), and to frustrate efforts to generate fraudulent votes, Ohio requires poll workers to undertake at the polling place a quick tally or audit of the number of voters signing the precinct registry and the ballots cast, the number of soiled ballots, etc. This audit occurs after the polls close and before poll workers pack the supply bags, with directions to include the completed form inside the supply bag. The statute also directs judges to explain any discrepancy in writing. ***O.R.C § 3501.26***

A number of poll workers did not comply with the audit provision and failed to complete the form. Additionally, a large number of precincts show discrepancies (that are sometimes quite large) between the number of voters signing the registry and the number of ballots cast from the precinct.

The CCBOE Ballot Dept. staff have been completing a more painstaking reassessment of the actual discrepancy in each precinct. They are examining the registries for voters who signed on precinct registry pages that had not previously been tallied, such as the provisional voter page. The Monitor has not received the final Ballot Department report on this problem.

One common explanation for the discrepancies – which were substantial when reviewed initially at the certification Board meeting – is that the polling place layout permitted a large number of voters to join the line for casting ballots without having gone first through the precinct tables for signing the registry. Another explanation is that the judges failed to ensure that their precinct's voters received voter access cards that were encoded by the precinct's own encoder – not a shared encoder for the entire polling place. Other administrative explanations include the departures of voters who had been processed to vote yet decided not to remain in line to vote (arguably because of delays to gain access to a DRE touchscreen machine).

What is not fully known at this point, however, is the degree to which the explanations above delineate the entire list of causes for the discrepancies. Effective and complete remedies for the forbidden discrepancies will require an accurate and complete understanding of their originating causes.

Where there are large unexplained discrepancies between the number of voters who signed into vote and the number of ballots cast, questions can arise of whether criminal conduct occurred. For instance, ***O.R.C § 3599.26*** proscribes tampering with ballots. Other statutes forbid tampering with voting records and polling place registries. Because the November general election was a federal election, federal statutes addressing these points may also impose certain legal duties and liabilities.

5. Legal Eligibility of Employees for Certain Job Assignments

To focus on the essential points for a successful November election, which in the Monitor's view made tabulation and security issues plus poll worker and polling place issues paramount, the Monitor did not address or monitor for personnel practices. The following legal compliance questions have been raised by others to Monitor staff. We have virtually no first-hand factual information regarding these points, recognize that they raise sensitive and complex issues, but also believe we have an obligation to pass these issues forward to you.

a. Indicted Employees Handling Voted Ballots: At least two of the CCBOE managers who were indicted on election fraud charges stemming from alleged activities during the 2004 presidential recount were reported to have been handling ballots during the November 2006 election cycle. Ms. Maiden was reportedly observed transferring DRE touchscreen memory cards between CCBOE offices on different floors. Ms. Dreamer was assigned to be CVS's absentee ballot assistant manager where she reportedly had to handle, and direct other staff to handle, voted absentee ballots that were returned to her department for processing.

The Monitor and many CCBOE staff were informed that the indicted employees were moved from their former assignments where they had exercised some control over voted ballots to other positions where they would be barred from and not need to handle ballots personally or supervise staff who handled voted ballots. We do not know the specifics of the CCBOE's policy concerning the work of these employees.

As mentioned, the Monitor lacks knowledge regarding the factual accuracy of these allegations. Additionally, we have not researched public employee, election, or other law to ascertain whether any legal compliance questions arise because these indicted employees have arguably handled ballots – voted or not. While such duties appear to contradict assurances that the CCBOE Board Members may have made about the revised scope of these employees' work assignments, it may be that no laws are violated by these assignments. We simply raise it for your attention.

b. Non-Citizens Handling Ballots and Tabulation Tasks: The Monitor has been informed that several CCBOE Information Services (IS) staff members are not U.S. citizens. Further, it may be that the immigration status of some employees does not include a "green card" and thus may be more vulnerable than those with a more protected status. Again, these are sensitive issues but the concerns that have been raised for election legality and integrity seem sincere and nonfrivolous.

The issues that have been raised with the Monitor are:

(1) Whether an employee with an immigration status that does not permit the individual to register to vote comports with Ohio statutory or administrative law for "election officials," given that they cannot be electors and cannot have an elector status of even "unaffiliated" or no party (N). The argument that has been raised to the Monitor is that to be able to have a party status, election officials must first be eligible electors. These employees are citizens of a foreign government and cannot register to vote in Ohio. Yet each of these employees has been assigned to be an "N" in recounts, at the tabulation server, and in other election roles. Their jobs include handling ballots and exercising certain technical powers over the voting rights/election tabulations for U.S. citizens.

(2) Whether, even if not a violation of Ohio election law, these employees' lack of legal rights to remain in this country renders them vulnerable to coercion and intimidation that might lead to participation in illegal or unethical election practices.

We offer no general knowledge of immigration law or the election law provisions that might come into play so we simply pass these questions forward to the Boards.

6. Election Tabulation and Related Technical & Security Issues

Electronic voting is very new to Cuyahoga County. The County has had only six months of actual election experience with this new technology. The relative inexperience of the Boards and public with e-voting issues, and the sea change it has necessitated in administrative and security systems, might reasonably cause impatience with the points of concern that follow. Additionally, unlike the topical areas above, technical and tabulation information can be daunting, often making it difficult to penetrate for those without significant technical training. Thus, we provide some additional background as a context before reviewing some legal compliance issues.

Policy Objectives Underlying the Law and Administrative Security Procedures: The constellation of issues addressed here is concerned first with safeguarding the voters' rights to an accurate tabulation of the ballots cast in accordance with applicable law. Second, it includes provisions for attempting to ensure that the systems in use – both electronic and administrative – are producing reliable, accurate and secure election results and preventing mistakes, corruption, fraud and manipulation.

Laws and standards governing electronic voting and tabulations, as well as scholarly and legal publications on electronic voting, emphasize security provisions – both physical security and digital security. Security is not a new concern to election law; the law governing punch cards and other traditional paper ballots also stresses security, chain of custody and accountability measures. Vigorous accountability measures not only allow the public's votes to be safeguarded but also help to protect election administrative staff members from unfair charges that they have engaged in vote or ballot manipulation. The record is available publicly.

Both electronic voting systems and punch-card systems feature strengths and weaknesses. But electronic voting and tabulations are subject to a host of vulnerabilities having no analog in the punch-card world. Practices and policies used to safeguard punch-card elections are often ill-suited to e-voting. With electronic voting, there are opportunities to make significant mistakes in tabulations as well as to maliciously tamper with voting results that did not exist with paper ballots. Indeed, tampering with e-voting tabulations can be accomplished remotely, without physical access to the system, and requiring only a few seconds. Because the risks and routes of access for vote deletions, manipulations (such as "vote flipping" between candidates), and other forms of tampering differ from the punch card world, different security measures must be implemented. Election managers need to operate in strict compliance with security and accountability procedures to guard against these novel threats.

Banks, credit card companies, and even our nation's military have had their records penetrated and manipulated by remote wrongdoers. Virtually not a week passes without press reports of some major electronic intrusions into what were considered highly secure and well protected data systems. With a great deal of public contracting and policies concerning financial and other major interests affected by election results, financial as well as other incentives may be present for remote manipulation of the voting results.

Remote access and manipulation are not the only risks to data systems, however. Well-protected financial entities have been subject to some internal data manipulation efforts to embezzle or cover other crimes. Judicial cases, including criminal prosecutions, have established that manipulation of data systems by internal staff has occurred in some locations elsewhere. Criminal cases have also established that some elections staff, in paper-based voting systems, have manipulated election results. For the voters' protection, the risks to election integrity must be identified and minimized whether potentially internal or external in origin.

Electronic voting and tabulation security provisions are designed to protect against the possibility of both remote and internal tampering with election results, and to protect the public's investment in expensive election machinery. The different potential risk routes (internal and external/remote/electronic) require somewhat different though harmonious sets of internal policies and procedures to safeguard the voting data and tabulations.

Achieving Data and Election Results Security: The existence of appropriate internal policies and procedures to protect data security is only the beginning. Generally, a number of other steps are required to implement and continually update an effective data security system. These include: well-documented and tested operating procedures, effective staff training in security procedures, periodic checks on the extent of employee compliance, accountability and discipline for employee noncompliance, periodic expert review of the adequacy of security procedures, and thorough routine auditing.

Legal Systems' Approach: Depending on the particular facts, interests at stake, and applicable laws, the legal system authorizes various forms of legal action for violations of data security rules. Significant penalties can be imposed. Employee noncompliance with internal policies for data security, especially broad noncompliance, can raise legal questions. Both civil and criminal law may be violated by noncompliance with election data security rules. Where the conduct or noncompliance occurs in a federal election, the federal and state legal systems share concurrent authority for involvement.

Ohio's "minimum requirements" for the counting of votes (see Directive 2006-85) are specified in O.R.C. § 3505.27. Additional state laws governing electronic voting systems are found in statutes (e.g., O.R.C. §§ 3506.01- 3506.23) and SOS administrative law (chiefly via Directives to Boards of Election such as Directive 2005-23 and Directive 2006-85). O.R.C. § 3599.16 specifies that no BOE employee, director or member shall willfully add to or subtract from the votes actually cast in any official returns. O.R.C. § 3505.27 directs the BOEs to supplement the State's minimum standards with procedures that "assure an accurate count of all votes cast." Arguably, by operation of § 3505.27 and Directive 2006-85, the security policy and procedures a BOE adopts have the force of law. Federal law also supplies some applicable standards (including HAVA– the Help America Vote Act). Generally, we will sidestep further legal citation and instead focus on the factual occurrences that raise concerns for legal compliance.

Management: In the CCBOE, in preparation for the November election, the lead manager for the administrative "pod" within which the Ballot and Information Services Departments were located was Director Michael Vu. Mr. Lou Irizarry, who is the Administrator over these two departments, was next in the chain of command. The (interim) Ballot Department manager is (Mr. Matt Jaffe; for Information Services, Ms. Helen Tian.

A. Tabulation and Printing of Absentee Ballot Results Before Election Day

The CCBOE petitioned the Ohio Secretary of State for permission to scan into the election tabulation computer (known as the "GEMS server") the absentee ballots that voters had returned by Friday, November 3rd. When that SOS permission was not given, the County Prosecutor filed a judicial action to obtain an order permitting the CCBOE to conduct early scanning. Reportedly, part of the representations to the court concerned the security measures that would be taken by the CCBOE to prevent disclosure of election results prior to the legally permitted time-- after the polls had closed on Election Day.

On November 3, 2006, the court issued an order to the SOS directing that early scanning be authorized statewide but with certain security protections in place. The SOS followed with Directive 2006-85, which directed all Boards of Election to adopt enhanced security measures consistent with the injunction if they chose to move forward with scanning ballots prior to Election Day:

> those boards electing to scan absent voter's ballots prior to November 7 with automatic tabulating equipment *must have formally adopted and* ***have*** *implemented a security plan* relating to absent voter's ballots that ensures at a minimum: (i) controlled access to the location where ballots are counted; (ii) secured, password-controlled access to the automatic tabulating equipment; (iii) bipartisan (2-person) control over all absent voter's ballots at all times; and (iv) that, ***at no time, any person has any access to the count or any portion of the count before the polling places close*** on November 7, 2006.

(Directive 2006-85 with emphasis added; see Appendix at 16-19 for complete copy). The SOS appended the judicial order to Directive 2006-85 and sent it by email to all BOEs on November 4, 2006.

Consistent with the new Directive, the Cuyahoga County BOE Board Members met on Sunday, November 5th to discuss and adopt enhanced security policies for early optical scanning and for the election tabulations more generally. They approved a supplementary document that Director Vu prepared. They also approved a set of proposed policies that the Monitor quickly drafted and submitted (drawing on earlier discussions and submissions) after being given a copy of the Director's proposal roughly two hours before the meeting was to commence. (See Appendix at 13-15)

To review the election tabulations, the Monitor requested and eventually received several different types of automatically generated log records of GEMS computer activity. These logs appear to indicate that absentee ballot vote results were generated and printed on Monday, November 6, following the commencement of absentee ballot scanning, in disregard of the court order and the Directive.

A GEMS "Summary Report" contains tabulated voting data. The 27-page Cuyahoga County Summary Report shows the vote tabulations for every race and issue throughout the County that was part of the November 2006 general election balloting. The GEMS tabulation system can also be directed to produce shorter Summary Reports with selected cities or races. The System Event log information we have excerpted in the Appendix (pp. 2 - 3) shows the printing of both 6-page and 27- page Summary Reports on the evening of November 6th, after the absentee ballot early scanning had been completed.

In the Windows System Event Log, it records 7 print operations of GEMS Summary Reports on Monday, November 6, 2006 from 6:15 PM until 7:21 PM. (See Appendix at 2 - 3). In the GEMS Audit Log provided to the Monitor, there are ***no entries for any of the 7 print operations the System Event log has recorded***. (Appendix at p. 4).

In addition to the questions of whether, by whose action, and how the apparent early absentee ballot tabulation and printing of results occurred, we would flag several inconsistencies between these records that raise additional serious questions:

- The "Windows Event" log records 7 separate print commands for Summary Reports but the GEMS audit log records the printing of only 2 Summary Reports. Based on a comparison with other entries for GEMS report printing, the Monitor software engineer staff had expected that the data in these two logs would match. The GEMS software does not implement significant security measures to thwart tampering with the GEMS audit log, and the possibility of tampering with that log cannot be excluded.

- The Windows event logs record entries in the sequence in which they are generated, without regard to the time reported by the computer's internal clock. If the time on the system clock is changed, the timestamps on any events added to the logs will reflect the new clock time. Despite the changed timestamp, however, the events are still recorded in sequential order. Thus, a change in the clock time may result in forward-dated or back-dated timestamps, but the logs will still reflect the actual ordering of the events. In the case of the Summary Report printing events on November 6, 2006, the order of entries in the log establishes that the last GEMS report printing event occurred after 7:17:30***PM***, even though this last entry carries the time-stamp of 7:21:25***AM***. (Appendix at p. 3)

Among the concerns motivating the prohibition on generating reports of absentee voting results prior to the close of the polls on election day is that early access to absentee vote tabulations could be used to compromise the fairness and results of the voting on election day.   For instance, absentee voting results could be used to determine which precincts to disrupt on Election Day or to steer other forms of tampering. This concern is especially acute where the proportion of the votes cast by absentee ballot is extremely high, such as was the case in the November, 2006 election in which nearly 25% of votes were cast via absentee ballot.

During a recent meeting that had been arranged for other purposes, the Monitor's Project Director, Candice Hoke, showed to the three managers present the logs excerpts that indicated early tabulations. This meeting with Ballot Department Managers Jaffe and Cleary, and Administrator Irizarry occurred on January 4, 2007. Prof. Hoke next met with Director Vu to show him the logs, and left copies of these documents with the Director.

Given the log records and possible violations of law, it might be prudent to request the County Prosecutor, in its capacity as legal counsel to the Board, to arrange for secure preservation of all original security video recordings covering the Board of Elections facility, with special attention to the tabulation and scanning rooms (both first floor and basement) for the entirety of November 2006. We understand the recordings are located at the County's Central Services Office.   Also, an independent forensic software expert might be retained to preserve and analyze relevant records that are on the GEMS server currently and associated devices.

B. <u>Scanner Networking Connection</u>

The optical scanners the CCBOE purchased and leased for counting absentee ballots were installed in the CCBOE basement the week prior to the Election Day. Each of the 60 scanners were connected ("networked") through specially installed cables that fed into one device (called a "digiport") that then could be connected by a single cable to the GEMS computer located on the first floor. A different cable connected the GEMS computer server to the numerous DRE touchscreen units in the tabulation room which were used on election night for uploading voting data from precinct DRE memory cards.

Because a direct network connection from the GEMS server in the tabulation room to a site or sites elsewhere in the building constitutes a significant security risk, and likely violates regulations imposed by the Secretary of State for tabulation security, the Monitor staff raised its concerns during the fall before the election. We were orally assured that the network cable to the basement scanning room would be disconnected from whenever scanning was not occurring. The CCBOE Security Policy does not specifically address this point, however.

Part of the Security Policy adopted by Board action on November 5, 2006 was to require paper/ink logging of network cable connections and disconnections. (See Appendix pp. 13-15, under Tabulation Room point #3). Although the Monitor requested copies of these paper logs over a month ago, none have been provided.

The Windows Events log entries indicate that the network cable from the scanning room was disconnected from the GEMS server at 10:45 PM on November 5th following the completion of the testing of the scanners. For an as yet unknown reason the cable was then reconnected to the

GEMS server at 11:38 PM prior to the securing of the tabulation room for the evening. (Appendix at pages 5 – 6). There is no log entry indicating that the cable was disconnected until Monday evening, following the scanning of the absentee ballots. We do not know what, if any, network connections were made while the GEMS server was shut down.

Absentee ballot scanning began at roughly 7:00am on November 6th. The Monitor staff member who was present from roughly 6:45am forward pointed out to Manager Jaffe the 11+ hour difference between the correct current time and that of the GEMS clock. Mr. Jaffe changed the clock to the correct time immediately.

The oddity here is that the GEMS clock had been running accurately at other times when it was observed by Monitor staff. But apparently over the night when the tabulation room was reportedly locked and sealed but with the network cable to the basement remaining attached to the server instead of unplugged, the clock had somehow become over 11 hours ahead of the correct time. But we do not know what happened to cause the clock time to change. It warrants consideration and further investigation.

C. Failure to Assign Traceable Tabulation "User Names" and Limited Accounts

One basic principle of computer operator accountability is for each person having access to the computer to have their own distinctive password or user name so that their activity can be effectively monitored. This is standard operating procedure for the private sector but also for the educational and governmental sectors as well.

A second basic principle is that not all operators should have the same power over the computer. Control over some features, such as the computer's configuration, the setting and changing of passwords, the ability to install new software and access certain databases, or the ability to access (and change) the logs recording operator activity on the computer or the clock time, can be restricted via the type of account that a particular user/operator is given. These user accounts also then help to protect employees from false accusations that they have modified data or the computer in some wrongful manner; the activity logs track their conduct and the accounts lock out certain users from having any control over many sensitive functions. Those few managers or administrators who have the higher level privileges can themselves be held accountable for any changes that occur to restricted data or computer settings.

CERP Finding and Recommendation In reviewing the deficiencies of the May 2006 election, the CERP Final Report discovered that these user account practices that are the baseline elsewhere had not been a part of the CCBOE's practices. It meant that "all operators could change both the data in GEMS via the gemsuser account and reconfigure the system using the gemsadmin account." CERP Finding 2.104. Greatly exacerbating the problem, CERP found that "the fact that all operators used the same, anonymous accounts (gemsuser and gemsadmin) prevents anyone examining transaction logs from determining which person made a particular modification to the system." (CERP Finding 2.104, drawing on a report from the National Institute of Standards and Technology--NIST).

CERP's Recommendation 2.105 for curing the disturbing conduct reflected the NIST presentation of well established and broadly accepted computer security practices:

> Basic security practices must be adopted and enforced for the GEMS system. Important aspects include: limiting authorized operators, limiting operators to appropriate roles, and ensuring identification of specific operators for logging and auditing purposes… They should be designed by security experts, have penalties for employee noncompliance, and be a part of Ballot and IS Department training.

Individualized User Names   Assignments of user names and an allocation of privileges could have been administratively achieved immediately following the issuance of the CERP Final Report, even without formal Board action but no immediate change occurred.

In the documents he submitted to the Secretary of State seeking permission for early scanning and in later revisions of the document Director Vu stated:

> [T]o address concerns regarding the pre-release of election results, GEMS contains an audit log . . . that records certain events that take place within the GEMS program, including production of a Summary Report (i.e. election results). With the audit log, the Board of Elections may be able to determine ***if a Summary Report was generated, when it was generated and by whom.*** [emphasis added]

The Director's statement thus promises that the log will show by whom an elections results report was generated -- a representation that distinct user accounts would be used.

The Board's commitment to implement the individualized user account policy was reflected in the CCBOE's revised Security Procedures plan drafted by Administrator Irizarry (charged with oversight of IT and Ballot Departments). Administrator Irizarry and Director Vu presented the plan to the CCBOE Board for action on October 2, 2006. The plan states the Board management's response to the CERP findings and recommendations concerning the untraceable anonymous user accounts that the CCBOE deployed in May. The plan states these commitments for the November 2006 election:

> ANSWER: User accounts will be utilized for November. Admin account use will be restricted to a few individuals that are competent to operate as Admins. All others will have access levels that complement their knowledge and GEMS abilities and requirements.
>
> ANSWER: Log sheets binders are in place at all GEMS servers and are required to be filled in at all times by anyone making a change to a GEMS database.

See Appendix pp. 11–12. Formal Board action to approve the Security Procedures occurred at the October 2nd meeting, with the proviso that it was expected to be a continuing work in progress.

Between the unofficial tabulations and the official, the Monitor discovered that the Audit Log showed no implementation of the individualized user accounts security policy. In a memo that managers Irizarry and Jaffe and Director Vu received before the official tabulations began, the Monitor emphasized the need for the user accounts to be created.

Despite these published policy commitments to institute individualized user accounts and the reminder from the Monitor, the CCBOE did not implement the user accounts policy. The Ballot and IS department practices this fall deviated substantially from the Security Procedures plan the Board had formally approved. Review of the logs shows that the IT and Ballot Departments appear to have basically continued May 2006 approach: no individualized user accounts were created and used, and all actions on GEMS were performed by "admin."

In the meeting on January 4th with Professor Hoke, Mr. Irizarry and Mr. Jaffe acknowledged that no individual user accounts were ever created. Mr. Jaffe stated he had tried once to create the accounts but he needed Mr. Irizarry's assistance to do this. They both reported that Mr. Irizarry was not available at the time Mr. Jaffe attempted to create the accounts. They also suggested that this had been a task that had just "fallen through the cracks."

Mr. Irizarry also acknowledged at the same meeting that he had conducted no employee training for implementing the new Security Procedures, had undertaken no assessments of implementation and employee noncompliance with the Security Procedures policy, and that no employees had been held accountable for failure to comply with the Security policy.

Additionally, Mr. Irizarry stated that although he knew the CCBOE Board Members had expanded and strengthened the Security Procedures at their special November 5th meeting required by the SOS in order to conduct early scanning, he had not added these to the earlier-approved Security Procedures plan. As far as he could recall, no one had distributed to CCBOE staff the Board's November 5th additions to the security practices and he stated he did not consider it his responsibility to do so.

Given the various irregularities noted in this memo both above and below this section, the failure to create user accounts throughout the fall and both tabulations in November election is problematic. The individualized accounts would have shown who was using GEMS at a particular time. The Security Procedure additions (approved on 11/5) also provided that paper/ink logs of the operators and those who entered the tabulation room were to be kept but the Monitor staff observed inconsistency in signing in and reporting computer events.

The Monitor software staff has identified numerous other events and anomalies in the various GEMS computer logs that probably warrant further investigation. The first step in reconstructing the activity of a particular time so that its import can be discussed and assessed would generally be to determine who was operating the computer/server at the time. Security video tapes can be used to identify operators but that process is time-consuming and more difficult, and may be defeated by remote access from a basement cable especially if the lights were not turned on in the basement.

In the January 4th meeting, when Prof. Hoke inquired who had any privileges at the GEMS server during any of the time from the unofficial through the official counts, the three managers listed three persons: the (interim) Ballot Manager and (interim) Assistant Manager and one other full time Ballot Department staff member. When Professor Hoke asked specifically about one temporary staff member who was observed operating the GEMS keyboard on November 8, they acknowledged she was printing a GEMS report but they did not amend their prior representation that only three individuals were authorized to be at the GEMS server during election activities.

The Monitor software staff personally observed several other temporary staff at the GEMS keyboard as the primary operator during unofficial tabulations in addition to the three full time employees the managers had mentioned. The Monitor does not know why in the meeting on January 4th, the IT and Ballot managers chose to list only the full time Ballot department employees as the only personnel whom they authorized and who actually operated the GEMS computer during the election tabulations.

Controlling Levels of Computer Access By not creating the individualized user accounts, the IT Administrator and Ballot Manager departed from the Security Policy commitments in another manner: they did not distinguish the "access levels" of the GEMS users. The Monitor's review shows only one account, with one level of access, for everyone using the computer. The CCBOE Security Policy states that different CCBOE personnel who operate GEMS have different "knowledge, … abilit[ies] and requirements" yet the insight was not implemented.

The Monitor's analysis shows that all persons who operated GEMS this past fall had full administrator access to GEMS, with no individualized restrictions on the changes they could make to the GEMS system or database. Additionally, this full administrative access (perhaps by most or all IT and Ballot employees) made no distinction between employee authority to engage in activities to prepare for the election (e.g., configuring precincts and races, modifying ballot styles) and those permitted and fully trained for the tabulation required for the unofficial or official counts. By circumscribing privileges, the CCBOE lowers the risk that an operator can intentionally or inadvertently alter the configuration or data in an election database.

D. Changing the GEMS System Clock

Based on observations of Monitor staff on November 5th and 6th, 2006 and an analysis of the GEMS audit and Windows System Events logs , it appears that the system clock on the GEMS server was changed sometime between 7:15 PM on November 5th and 7:20 AM on November 6th. In this interval, the time on the GEMS system clock advanced almost 12 hours.

The Monitor staff monitoring the GEMS server on November 5th observed the GEMS clock running with accurate time during the scanner testing, so it is puzzling why the clock had changed and become fast by almost 12 hours. The coincidence of the basement scanner network cable remaining connected all night and the clock no longer reflecting accurate time raises serious questions.

Further inquiry appears warranted. (Appendix at 3-4 provides some relevant log records)

E. The "Security Events" and Other Windows Logs

The GEMS tabulation server is a Windows-based application. The Windows Security Events log is a standard portion of the Windows operating system software that tracks certain conduct and events that relate to data security.

The Monitor requested the three standard types of Windows logs for the first time on November 14, 2006. (See Appendix at 7) These logs were not provided promptly but when they finally arrived, we discovered the Security Event log recorded only one entry: that the audit log had been "cleared" by an Administrator on December 8, 2005. The Security Events log shows no events or activities for the entirety of 2006.

The CCBOE GEMS server had not been delivered or installed on the date the Security Events log records it had been "cleared." This probably means that the manufacturer cleared and configured the log so that it would not record any security events. If the default setting at the time of delivery was not to record security events, we do not know why, once delivered to the CCBOE, the log was not reconfigured. It would seem that in the "mission critical" and highly regulated election tabulation context, the log would have been reconfigured to record security events over a broad time period that embraced all testing and tabulations of a given election. Additionally, for utmost value, the CCBOE would have made archive copies of the Security Event log entries at each election's conclusion.

In light of the various irregularities identified above and below in this memo, it is worth determining:

- what is Microsoft's recommended configuration for this log in mission-critical applications;

- whether other Ohio BOEs using the GEMS software have differently configured and active security event logs, and if so, why Cuyahoga's differs;

- whether any manual changes of the GEMS clock would generally be noted on the Windows security event log;

- whether the Security Event log could have been cleared more recently and whether it also would permit an operator to change the date/time stamp on the log in a manner that would conceal the activity;

- whether the Monitor was provided a true copy of the log maintained on the GEMS server;

- whether other software resident on the GEMS server may be interfering with the logging of security-related events;

- what is the role of Digital Guardian software (mandated by the SOS), and a comparison of the events it recorded with those of the GEMS and Windows logs discussed above.

All three Windows log files that were submitted to the Monitor in response to our requests were are far smaller in size then we expected and contain fewer entries than we expected. The Windows System Log contained only 1.4MB of data; the Windows Application Log contained only 125kB and dates back to only 10/09/2006. And as noted above, the Security Log contained only one entry dated 2005, before its shipment and installation locally.

It may be that to enhance security and accountability, reconfiguration of these logs is warranted Configuration control over the logs could also be restricted so that no CCBOE employees can reset them. Additionally, the file size/maximum storage capacity for each log can be set so it is large enough that the system never needs to delete old entries to make room for new entries during an election cycle. These steps would facilitate the tabulation accountability in e-voting that Election Law and voters expect.

F. Additional Questions

These issues are presented briefly:

Use of Flash Memory (for uploading the election results from the GEMS tabulation server to the web on Election night). The IS Manager, Helen Tian, used one of the CCBOE-purchased flash memory devices to download the tabulation results every 15 minutes or so, and to post them to the website. Mr. Irizarry said this process had been planned in advance and used previously, although it is not a part of the published Security plan. When the GEMS server is connected via a "jump drive" that intermittently to the internet, does this practice violate the SOS Directive 2005-23 or other law? Presumptively the jump drive or flash memory is an uncertified piece of hardware and the resident memory was not tested before being connected to the GEMS server. The Monitor flagged this issue for the Director and the IT Manager on Election night, suggesting that a CD be burned instead of using a jump drive but the suggestion was rejected.

Password Practices During Tabulations Did the CCBOE's password and user account practices during early scanning and other tabulations violate Directive 2006-85 or other Directives, its own Security Policy and/or other policies having the force of law?

Paper/ink logs (that were mandated on 11/5/06 as a part of CCBOE Board action to enhance security): to what degree were these logs accurately and completely maintained, for: (a) early scanning, (b) for the unofficial tabulations, and (c) for the official tabulations? Were paper/ink logs accurately kept of GEMS server events? For instance, the GEMS server crash during the early scanning operations was not recorded until the Monitor staff insisted it was an event that must be logged. Additionally, when the backup operation failed, the GEMS operator did not record that event until the Monitor requested it in the presence of two Board Members. Do the paper/ink logs reflect all Optical Scan ballot batches (in both the unofficial and official counts) that were deleted and rescanned as provided in the 11/5 security amendments? Did all GEMS operators log in on the paper/ink logs as mandated in the 11/5 security amendments? Did noncompliance with these security procedures formally adopted constitute violations of law?

Bipartisan Presence at the GEMS server – To what degree is it legally permitted for a person of one party to operate the GEMS server during the period an election is "open" for tabulations (either unofficial or official) without an employee of another party sitting at the GEMS keyboard observing all operator activity? The CCBOE Ballot Department practice is simply to require a person of another party to be somewhere in the large room – which extends over 30 feet away from the computer screen. Even a five foot distance eliminates the ability to read certain information on the computer screen.

Laptop in scanning or GEMS tabulation room – Is it legally permissible for the Director or a CCBOE employee to have a laptop computer with him/her in one of the tabulation locations? The Director was observed multiple times carrying a laptop while he walked around the basement scanning room during the early absentee ballot scanning operations, and also carried the laptop into the GEMS tabulation room. He was observed using his laptop in the GEMS tabulation room during the L & A testing of the scanners.

Configuration of JResults Server on Election Night: It is not clear whether the JResults software had been installed on the GEMS server before Election night, November 7th. The managers report the software had been previously installed but had not been tested and readied for Election night tabulations by IS Manager Tian. The Monitor software engineer present at the time the 11/7 tabulations began (just after 9:00 pm) reports that the JResults software had not been not correctly configured for use and had not been tested on the main GEMS server before it was needed for posting election results to the web.

The Monitor software staff observed several troubling occurrences on November 7 - 8 that Diebold later explained were at least partially a result of the concurrent use of GEMS and JResults. The Monitor's legal questions include:

- Has the "JResults Server" software been certified for use by an ITA and by the Ohio Board of Voting Machine Examiners (the administrative examining process for election systems)?

- If so, does the certification approval specify any restrictions on use of the JResults while GEMS is running, and if so, did the manufacturer provide these to the CCBOE?

- Does the apparent omission of manufacturer documentation of procedures for how and when to use JResults with GEMS violate O.R.C. §§ 3606.05(B) and 3606.05(C)(1)?

- Does the CCBOE's apparent omission of public testing for the JResults software violate O.R.C. §§ 3606.05(B)?

Non-implementation of the CCBOE Security Policy: Where, as apparently at the CCBOE, there have/has been:

- no managerial effort to ensure that all CCBOE employees have been trained in the new Security Procedures policies that were adopted by CCBOE Board at various public meetings (under general statutory authority plus pursuant to the orders issuing from a court and the SOS Directive 2006-85);

- many apparent departures from the Security plan during the last election cycle, with some being serious departures undermining the most critical needs for accountability and security;

- no assessment of the scope of Security plan implementation or of employee noncompliance with the Security policy even though well over a month has passed since the November election was certified, and almost two months since the November 7th Election Day and initial tabulations;

- no accountability for managers or line staff for their failure to implement or personally comply with the Security policy; and,

- unexplained and possibly illegal events apparently demonstrating a breach in security;

what is the legal duty of the CCBOE or BOCC Board Members (or others) for convening further inquiry, for reporting the possible deficiencies, or for redressing the situation? Is a report to the

Elections Division of the Secretary of State warranted? Does managerial failure to implement the Security Procedures policy constitute a legal violation that must be corrected before conducting future elections?

****

As you know, the Monitor endeavored throughout the fall to enhance the relevant CCBOE managers' attention to and understanding of the security issues that inhere in e-voting. The factual record that we place before you now troubles us. We are additionally concerned about the continued apparent lack of concern at the CCBOE about security issues.

The Monitor staff are available for further discussion or assistance. Thank you for your attention.