☞ **09hr_SC-LEUA_sb0435_pt02b**

⬆

Details:

(FORM UPDATED: 08/11/2010)

WISCONSIN STATE LEGISLATURE ...
PUBLIC HEARING - COMMITTEE RECORDS

2009-10

(session year)

Senate

(Assembly, Senate or Joint)

Committee on ... Labor, Elections, and Urban Affairs (SC-LEUA)

COMMITTEE NOTICES ...

- Committee Reports ... **CR**
- Executive Sessions ... **ES**
- Public Hearings ... **PH**

INFORMATION COLLECTED BY COMMITTEE FOR AND AGAINST PROPOSAL

- Appointments ... **Appt** (w/Record of Comm. Proceedings)
- Clearinghouse Rules ... **CRule** (w/Record of Comm. Proceedings)
- Hearing Records ... bills and resolutions (w/Record of Comm. Proceedings)

(**ab** = Assembly Bill)	(**ar** = Assembly Resolution)	(**ajr** = Assembly Joint Resolution)
(**sb** = Senate Bill)	(**sr** = Senate Resolution)	(**sjr** = Senate Joint Resolution)

- Miscellaneous ... **Misc**

* Contents organized for archiving by: Gigi Godwin (LRB) (August/2011)

City of Milwaukee

Board of Election Commissioners

Commissioners
Allen E. Campos
Robert F. Spindell, Jr.
Victoria L. Toliver
Executive Director
Susan M. Edman

August 31, 2009

Mr. John Washburn
N128W12795 Highland Road
Menomonee Falls, WI 53202

Dear Mr. Washburn:

I am writing in response to your letter dated August 4, 2009 wherein you request the following records pursuant to Wisconsin Statutes §§ 19.31-19.39:

1. The electronic copy (aka electronic backup) of the contents of removable memory card from the optical scanner used in Ward 114 during the November 4, 2008 election. The creation of this electronic election record and the retention of this record for 22 months are required separately under Wisconsin [WI Stats. §7.23(1)(g)] and federal [Title 42, Chapter 20, Subchapter 2, Section 1974] law.
2. The electronic copy (aka electronic backup) of the contents of removable memory card from the disability device (AutoMark) used in Ward 114 during the November 4, 2008 election. The creation of this electronic election record and the retention of this record for 22 months are required separately under Wisconsin [WI Stats. §7.23(1)(g)] and federal [Title 42, Chapter 20, Subchapter 2, Section 1974] law.
3. The electronic copy (aka electronic backup) of the contents of removable memory card from the optical scanner used in Ward 207 during the November 4, 2008 election. The creation of this electronic election record and the retention of this record for 22 months are required separately under Wisconsin [WI Stats. §7.23(1)(g)] and federal [Title 42, Chapter 20, Subchapter 2, Section 1974] law.
4. The electronic copy (aka electronic backup) of the contents of removable memory card from the disability device (AutoMark) used in Ward 207 during the November 4, 2008 election. The creation of this electronic election record and the retention of this record for 22 months are required separately under Wisconsin [WI Stats. §7.23(1)(g)] and federal [Title 42, Chapter 20, Subchapter 2, Section 1974] law.

5. The electronic copy (aka electronic backup) of the contents of removable memory card from the optical scanner used in Ward 215 during the November 4, 2008 election. The creation of this electronic election record and the retention of this record for 22 months are required separately under Wisconsin [WI Stats. § 7.23(1)(g)] and federal [Title 42, Chapter 20, Subchapter 2, Section 1974] law.
6. The electronic copy (aka electronic backup) of the contents of removable memory card from the disability device (AutoMark) used in Ward 215 during the November 4, 2008 election. The creation of this electronic election record and the retention of this record for 22 months are required separately under Wisconsin [WI Stats. §7.23(1)(g)] and federal [Title 42, Chapter 20, Subchapter 2, Section 1974] law.
7. The electronic copy (aka electronic backup) of the contents of removable memory card from the optical scanner used in Ward 255 during the November 4, 2008 election. The creation of this electronic election record and the retention of this record for 22 months are required separately under Wisconsin [WI Stats. § 7.23(1)(g)] and federal [Title 42, Chapter 20, Subchapter 2, Section 1974] law.
8. The electronic copy (aka electronic backup) of the contents of removable memory card from the disability device (AutoMark) used in Ward 255 during the November 4, 2008 election. The creation of this electronic election record and the retention of this record for 22 months are required separately under Wisconsin [WI Stats. §7.23(1)(g)] and federal [Title 42, Chapter 20, Subchapter 2, Section 1974] law.

With regard to items 1, 3, 5 and 7, I have attached an electronic copy of the contents of the removable memory card from the optical scanners used in Wards 114, 207, 215 and 255 from the November 4, 2008 election.

With regard to items, 2, 4, 6, and 8, your request is denied because there are no responsive records.

Wisconsin Statute § 7.23(1)(g), "Destruction of election materials," reads as follows:

(g) Detachable recording units and compartments for use with electronic voting machines may be cleared or erased 14 days after any primary and 21 days after any other election. Before clearing or erasing the units or compartments, a municipal clerk shall transfer the data contained in the units or compartments to a disk or other recording medium which may be erased or destroyed 22 months after the election to which the data relates.

Wisconsin Statute § 5.02(4m). "Electronic voting system." reads as follows:

(4m) "Electronic voting system" means a system in which votes are recorded on ballots, and the votes are subsequently counted and tabulated by automatic tabulating equipment. The term also includes a voting machine on which votes are recorded and tabulated by electronic means.

Based on our review of Wisconsin Statute § 5.02(4m), the contents of the removable memory card from the disability device (AutoMARK) is not subject to retention because it is not an electronic voting system.

Since the AutoMARK does not tabulate it is not an electronic voting system therefore not subject to data retention under Wisconsin Statute § 7.23(1)(g). The AutoMARK does not create a record; it marks the ballot for the elector. The ballot is then tabulated with other voted ballots. The total votes from the AutoMARK are included in the records that I have attached.

With the enclosed we have fully complied with your public records request by providing you with copies of all responsive records.

If you have any questions, please do not hesitate to contact me at 286-6119.

Sincerely,

Sue Edman

Susan Edman
Executive Director

N128W12795 Highland Road
Germantown, WI 53022
August 10, 2009

John Bigley
Clerk of the Town of Sugar Camp Wisconsin
4537 Highway D
Rhinelander, WI 54501

Dear Mr. Bigley:

I understand you are the keeper of the memory cards and the backups thereof. I would like to make some open records requests under WI Stats. §19. I would like the following election records from the November 4, 2008 election.

1. The electronic copy (aka electronic backup) of the contents of removable memory card from the optical scanner (ES&S Eagle) used in Town of Sugar Camp during the November 4, 2008 election. The creation of this electronic election record and the retention of this record for 22 months are required separately under Wisconsin [WI Stats. §7.23(1)(g)] and federal [Title 42, Chapter 20, Subchapter 2, Section 1974] law.
2. The electronic copy (aka electronic backup) of the contents of removable memory card from the disability device (ES&S Automark) Town of Sugar Camp during the November 4, 2008 election. The creation of this electronic election record and the retention of this record for 22 months are required separately under Wisconsin [WI Stats. §7.23(1)(g)] and federal [Title 42, Chapter 20, Subchapter 2, Section 1974] law.

Severability – The above open requests are separate and severable and are only including in this single correspondence in order to ease the administration of these requests and the thematic similarity among the requests. It is expected any delay in the production of records for one request will not impair or delay the production of records for another request.

Denial of Request – As required by Wisconsin's open records law as codified in §19, any denial, in whole or in part, of one or more of the public records requests above must state in writing and with specificity as to the reasons and statutory authority for denying the request. For the purposes of this requirement, an email response will be considered a written response.

Redaction – A redaction is a denial in part of requested record. There shall be a log which states in writing and with specificity to the reasons and statutory authority each redaction.

Duplication – If a single record satisfies one or more of the above requests, then only one copy of the record needs to be produced provide said record is accompanied by a notation as to which, multiple requests are satisfied by the record.

Promptness – The records requested above shall be provided "as soon as practicable" as required by Wisconsin statute.

Please contact me at your earliest convenience as to the costs of providing these electronic records in electronic form. If you have any questions, regarding this request you may contact me at this email address or at 414-375-5777.

In Liberty
John Washburn

Town of Sugar Camp
4059 CAMP FOUR ROAD
RHINELANDER, WISCONSIN 54501-8862
Phone: 715-272-1525 Fax: 715-272-1999 e-mail scamp@newnorth.net

September 21, 2009

Mr. Washburn,

I have talked to Ryan Mack from ES&S. At the time I sent the Town of Sugar Camp's memory pack in for the April election programming, all data from the November election was written over, no back up was made. Therefore, the only available data is the printed tape which I can copy for you. It will take 3 pages at a cost of $.75 and $.44 postage for a total of $1.19.

To answer your questions:
1. The Town of Sugar Camp does not have a memory pack with the November 4, 2008 election data. The Town has one memory pack and it was used in the April 2009 election. It was my understanding that a back up of the November 2008 data was to be kept by ES&S and it was not.
2. Memory pack and memory cards are owned by the Town of Sugar Camp.
3. ES&S will not store election results. They will re-burn a memory pack for $125.00 if we wish to re-run all the ballots. They will also re-burn the memory card for the AutoMark for $125 if we wish.

John Bigley,
Sugar Camp Town Clerk

John Washburn

From:	John Washburn [john@washburnresearch.org]
Sent:	Tuesday, September 29, 2009 11:15 PM
To:	'John Bigley; Sugar Camp Town Clerk'
Cc:	'wtowns1@frontiernet.net'; 'Michael.Haas@wisconsin.gov'
Subject:	Open Records Request
Attachments:	11_4_08 Election Data Request 3.doc

Dear Clerk Bigley:

I find the attached response to be perfectly satisfactory as an open records response; ES&S has destroyed the requested records and thus there are no records responsive to the request except those paper remnants you describe. I will not send the check as the paper records were not what I requested. The open records request is closed.

As an election law matter though I find the response deeply disturbing. In it you describe 4 felony violations of state and federal law. Specifically:

1. Federal statute requires 22 month retention of federal election records and papers (Title 42 chapter 20 sub chapter II section 1974). The election record requested (the backup of the memory cards) has been destroyed well before the 22 month retention period.
2. State statute, Wis. stats 7.23(1)(f), requires 22 month retention of federal election records. Again the requested records were destroyed well in advance of this 22 month retention period.
3. State statute, Wis. stats 7.23(1)(g), requires backups of memory cartridges used in optical scanners and other electronic voting systems. The statute, Wis. stats 7.23(1)(g), was designed to simplify the compliance with the above two requirements and to reduce the cost of compliance
4. State statute, Wis. stats 7.24, prohibits anyone other than an election official from being the custodian of an election record. You unfortunately followed the recommendation of the GAB letter dated December 18, 2009. Because of this you (and probably thousands of other clerks) turned over election records to ES&S and other vendors in express violation of Wisconsin state election law.
5. WI Stats. 12.13(2)(b)7 in conjunction with WI Stats. 12.60(1)(a) defines the above violations of state law to be Class I felonies. If you were lucky, the local DA might use WI Stats. 12.13(2)(a) in order to reduce the infractions to misdemeanors.

I will not file a complaint with DA Bloom as quite frankly the purpose the open records request was to verify the vendors were living up to the promises they made to the GAB back in November and December 2008. Clearly they are not. It is my opinion, the Government Accountability Board (GAB) is embarrassed that they have been caught refusing to a enforce a 20-year old election law (statute 7.23(1)(g) was passed in 1989) and then (as a palliative to this lack of enforcement upon clerks and vendor machinery alike) recommended clerks across the state violate a 34-year old election law (7.24 was passed in 1975) by allowing election records to be kept and archived by someone other than an election official.

I have included Michael Haas, the GAB staff attorney, and Richard Stadelman, Executive Director of the Wisconsin Towns Association, so as to alert them to the legal peril municipal clerks such as yourself may be in by following the recommendation of the December 18, 2009 GAB letter on memory card backups.

My personal advice to you is that you should research my statutory citations for yourself. Unless I'm wrong … but, you know, I'm not, this puts you at personal legal peril. You need to determine ***for yourself*** if this is the case.

Perhaps Brian Desmond, the Corporate Counsel for Oneida county, would be willing to give you an impartial opinion regarding the Wisconsin and federal statutes I have cited and the legal theory I have outlined in this email.

I consider the open records matter between us to be closed. I also consider the election law violations documented in your response are, at this time, best taken up with authorities other than local DA; Specifically, the several clerk associations, the election administration council, and the GAB itself.

I thank you for your time on this matter and I am sorry you were caught between the GAB and this Bluejay as I struggle to get the GAB to enforce decades old election laws and to force the vendors of election machinery to follow those same laws.

In Liberty,
John Washburn
Class of 1980

From:	john@WashburnResearch.org
Sent:	Monday, January 04, 2010 9:11 AM
To:	nat.robinson@wisconsin.gov
Cc:	michael.haas@wisconsin.gov
Subject:	Destruction of Election Records by ES&S
Attachments:	11_4_08 Election Data Request 3.pdf

To:
CC:
BCC:
Subject:Destruction of Election Records by ES&S

Dear Mr. Robinson:

Are you aware that ES&S has destroyed election records in Oneida and Sheboygan counties?

Essentially ES&S refuses to impliment option C of the December 17, 2008 memo to the GAB (http://elections.state.wi.us/docview.asp?docid=15541&locid=47).

The first problem with option C is that retention of election records by vendors is expressly forbidden under WI Stats. 7.24 and every clerk who excercied that option committed a Class I felony election fraud (presumably for each record so transfered). Transfer of an election record to non-election officials is election fraud under WI. Stats. 12.13(2)(7)(b) and that election fraud is defined to be a class I felony under WI Stats.
12.60(1)(a).

Overlooking the fact that the GAB recomended the clerks commit felonies, ES&S refused to make and retain the backups they promised the GAB during the research conductd as part of the December 17, 2009 memo. At this time, I can prove ES&S destroyed election record for olny in these two counties.
This is because these counties are the only two counties I happened contact regarding the WI. Stats 7.23(1)(g) backups. I suspect if I were to continue the compliance audit I would find that ES&S has destroyed election records in every county they "service".

I speculate this is the case because the letter from Ryan Mack of ES&S to John Bigley, Clerk of Sugar Camp, WI, is very clear. Mr. Mack states categorically that ES&S will NOT create, retain, or otherwise be responsible for the storage of any election records including the legally mandated backups of memory cards. Also, my audit was limited only to the November 4, 2008 election. I speculate records from both the February 17,
2009 and April 2009 elections were destroyed by ES&S as well. The number of election records destroyed by ES&S could easily number 10 of thousands records by now.

What is the GAB to do with this election-record destroying vendor?

If you would like more information or have any follow-up questions regarding this matter, you may contact me at this email address, by phone at 414-375-5777, or by mail at:
N128W12795 Highland Road
Germantown, WI 53022

Thanks you for your time on this matter.

John Washburn

John Washburn

From:	john@WashburnResearch.org
Sent:	Monday, January 04, 2010 11:36 AM
To:	nathaniel.robinson@wisconsin.gov; john@washburnresearch.org; michael.haas@wisconsin.gov; ross.hein@wisconsin.gov
Subject:	RE: Destruction of Election Records by ES&S

Dear Mr. Robinson.

I have been copying Mr. Haas since August. The CC'ing is easy, it is the response that has been hard to get.

:-)

Original Message:

From: Robinson, Nathaniel E - GAB Nathaniel.Robinson@Wisconsin.gov
Date: Mon, 4 Jan 2010 09:39:22 -0600
To: john@WashburnResearch.org, Michael.Haas@wisconsin.gov, Ross.Hein@Wisconsin.gov
Subject: RE: Destruction of Election Records by ES&S

A Happy 2010 to you Mr. Washburn,

Thank you for your correspondence. So that we are speaking with one voice on this matter, Staff Counsel Michael Haas is our single point of contact.
I see that you copied him on your missive. Please address all future correspondence regarding this matter to Attorney Haas.
Thank you.

Best wishes and kind regards,
Nat

Nathaniel E. Robinson
Elections Division Administrator
Government Accountability Board
212 East Washington Avenue, 3rd Floor
Madison, WI 53703

608 267 0715 (LAN)
608 267 0500 (FAX)

Nat.Robinson@wi.gov
http://gab.wi.gov

-----Original Message-----
From: john@WashburnResearch.org [mailto:john@WashburnResearch.org]
Sent: Monday, January 04, 2010 9:11 AM
To: Robinson, Nathaniel E - GAB
Cc: Haas, Michael R - GAB
Subject: Destruction of Election Records by ES&S

To:
CC:
BCC:
Subject:Destruction of Election Records by ES&S

Dear Mr. Robinson:

Are you aware that ES&S has destroyed election records in Oneida and Sheboygan counties?

Essentially ES&S refuses to impliment option C of the December 17, 2008 memo to the GAB (http://elections.state.wi.us/docview.asp?docid=15541&locid=47).

The first problem with option C is that retention of election records by vendors is expressly forbidden under WI Stats. 7.24 and every clerk who excercied that option committed a Class I felony election fraud (presumably for each record so transfered). Transfer of an election record to non-election officials is election fraud under WI. Stats. 12.13(2)(7)(b) and that election fraud is defined to be a class I felony under WI Stats.
12.60(1)(a).

Overlooking the fact that the GAB recomended the clerks commit felonies, ES&S refused to make and retain the backups they promised the GAB during the research conductd as part of the December 17, 2009 memo. At this time, I can prove ES&S destroyed election record for olny in these two counties.
This is because these counties are the only two counties I happened contact regarding the WI. Stats 7.23(1)(g) backups. I suspect if I were to continue the compliance audit I would find that ES&S has destroyed election records in every county they "service".

I speculate this is the case because the letter from Ryan Mack of ES&S to John Bigley, Clerk of Sugar Camp, WI, is very clear. Mr. Mack states categorically that ES&S will NOT create, retain, or otherwise be responsible for the storage of any election records including the legally mandated backups of memory cards. Also, my audit was limited only to the November 4, 2008 election. I speculate records from both the February 17,
2009 and April 2009 elections were destroyed by ES&S as well. The number of election records destroyed by ES&S could easily number 10 of thousands records by now.

What is the GAB to do with this election-record destroying vendor?

If you would like more information or have any follow-up questions regarding this matter, you may contact me at this email address, by phone at 414-375-5777, or by mail at:
N128W12795 Highland Road
Germantown, WI 53022

Thanks you for your time on this matter.

John Washburn

John Washburn

From: john@WashburnResearch.org
Sent: Monday, September 28, 2009 12:46 PM
To: Ross.Hein@wi.gov
Subject: Certification Testing re 7.23 and 7.24

Dear Mr. Hein:

I have two quick questions about the certification testing to be performed this week.

1) Will the mock election include a demonstration by the vendor that the system under test can produce the election records and backups required by WI Stats. 7.23(1)(f) and WI Stats. 7.23(1)(g)?

2) Are the backups created in order to comply with the legal mandates of 7.23(1)(f) and of 7.23(1)(g) in a form or on a medium which complies with WI Stats. 7.24? The statute, WI Stats. 7.24, requires the election clerks to assume and maintain title of ALL election records and is without exception as to whether the record is programming, data, or paper.

I ask this because the City of Milwaukee acknowledges they have failed to make records of the AutoMark programming as required by 7.23(1)(f) and 7.24.

Also the Town of Sugar Camp of Oneida County Wisconsin went with Option C of this GAB letter,
http://elections.state.wi.us/docview.asp?docid=15541,
for the 2008 general election and ES&S has now informed Clerk Bigley that ES&S has destroyed these 2008 election records.

There is also the matter of violating the records retention required by federal statute, but I recognize the authority of the WI Government Accountability Board only extends to state statute and have thus limited my questions to items in chapter 7 as those items touch on the utility and merchantability of a certified voting as required by WI Stats 5.91(10)and WI Stats. 402.314(2)(c).

In Liberty,
John Washburn

E-mail message checked by Spyware Doctor (6.1.0.447) Database version: 6.13360 http://www.pctools.com/en/spyware-doctor-antivirus/
No virus found in this incoming message.
Checked by AVG - www.avg.com
Version: 8.5.409 / Virus Database: 270.13.113/2400 - Release Date: 09/28/09 05:51:00

N128W12795 Highland Road
Germantown, WI 53022
January 4, 2010

Reid Magney, Public Information Officer
Wisconsin Government accountability Board
212 East Washington Avenue, Third Floor
P.O. Box 7984
Madison, Wisconsin 53707-7984

Dear Mr. Magney:

On September 20, 2009 I sent an email to Ross Hein, Elections Specialist - Voting Equipment Certification Coordinator, a question regarding the certification of the new ES&S voting system, Election Systems & Software's (ES&S) Unity 3.2.0.0 Voting System which includes the DC200 optical scanner. The email is attached for reference. Mr. Hein assured me on the system can and does make the legally required backups and does so in a form which permits the clerks themselves to retain the backups as required by state election law.

I would like to make the following open records requests:

1. The electronic backup of the contents of each removable memory card used during certification testing of the Election Systems & Software's (ES&S) Unity 3.2.0.0 Voting System while that voting system was performing the first mock election required by ElBd 7.01(3). These backups are the backups created by the staff of the GAB during the certification testing in order to verify the Election Systems & Software's (ES&S) Unity 3.2.0.0 Voting System meets the minimum legal requirements of WI Stats. 7.23(1)(g) and WI Stats. 7.24.
2. The electronic backup of the contents of each removable memory card used during certification testing of the Election Systems & Software's (ES&S) Unity 3.2.0.0 Voting System while that voting system was performing the second mock election required by ElBd 7.01(3). These backups are the backups created by the staff of the GAB during the certification testing in order to verify the Election Systems & Software's (ES&S) Unity 3.2.0.0 Voting System meets the minimum legal requirements of WI Stats. 7.23(1)(g) and WI Stats. 7.24.
3. The electronic backup of the contents of each removable memory card used during certification testing of the Election Systems & Software's (ES&S) Unity 3.2.0.0 Voting System while that voting system was performing the third mock election required by ElBd 7.01(3). These backups are the backups created by the staff of the GAB during the certification testing in order to verify the Election Systems & Software's (ES&S) Unity 3.2.0.0 Voting System meets the minimum legal requirements of WI Stats. 7.23(1)(g) and WI Stats. 7.24.

Severability – The above open requests are separate and severable and are only including in this single correspondence in order to ease the administration of these requests and the thematic similarity among the requests. It is expected any delay in the production of records for one request will not impair or delay the production of records for another request.

Denial of Request – As required by Wisconsin's open records law as codified in §19, any denial, in whole or in part, of one or more of the public records requests above must state in writing and with specificity as to the reasons and statutory authority for denying the request. For the purposes of this requirement, an email response will be considered a written response.

Redaction – A redaction is a denial in part of requested record. There shall be a log which states in writing and with specificity to the reasons and statutory authority each redaction.

Duplication – If a single record satisfies one or more of the above requests, then only one copy of the record needs to be produced provide said record is accompanied by a notation as to which, multiple requests are satisfied by the record.

Promptness – The records requested above shall be provided "as soon as practicable" as required by Wisconsin statute.

Please contact me at your earliest convenience when these electronic records can be provided to me. If you have any questions, regarding this request you may contact me at this email address or at 414-375-5777.

In Liberty,
John Washburn

State of Wisconsin\Government Accountability Board

212 East Washington Avenue, 3rd Floor
Post Office Box 7984
Madison, WI 53707-7984
Voice (608) 266-8005
Fax (608) 267-0500
E-mail: gab@wisconsin.gov
http://gab.wi.gov

JUDGE WILLIAM EICH
Chair

KEVIN J. KENNEDY
Director and General Counsel

February 5, 2010

Mr. Timothy J. Hallett
Associate General Counsel
Election Systems & Software, Inc.
11208 John Galt Boulevard
Omaha, Nebraska 68137

Via Email Only (tjhallett@essvote.com)

Re: Open Records Request of: John Washburn (1/4/10)

Dear Attorney Hallett:

Mr. John Washburn presented the enclosed open records request to the Government Accountability Board on January 4, 2010 pursuant to Sec. 19.35, Wis. Stats. The open records request involves a desire to obtain the "electronic backup of the contents of each removable memory card used during the certification testing of the ES&S Unity 3.2.0.0 Voting System" for each of the three mock elections held during the testing process in September 2009. The Government Accountability Board possesses one of the three memory sticks. Please identify the location and status of the remaining two memory sticks, or provide information as to whether the memory stick in our possession contains the data from all three mock elections.

Furthermore, the Government Accountability Board is aware that ES&S may have copyright or other proprietary concerns regarding release of any data from the mock election memory sticks. The Government Accountability Board cannot assert your proprietary rights for you. Please note that there are multiple files and file extensions on the memory stick in our possession. Please provide, in writing, detailed explanations of any assertion of copyright, trade secret or other proprietary interests. Such explanation should identify those specific files or file extensions to which any asserted protective interests apply and to which files or file extensions they do not apply.

Please provide your response within the next 10 days. If you have any further questions, please do not hesitate to contact me.

Sincerely,
GOVERNMENT ACCOUNTABILITY BOARD

Shane W. Falk
Staff Counsel

Enclosures
cc: Mr. John Washburn (via email only: john@WashburnResearch.org)
Mary E. Burke, Assistant Attorney General (via email only: burkeme@doj.state.wi.us)

Falk, Shane - GAB

From: Robinson, Nathaniel E - GAB
Sent: Monday, January 04, 2010 9:52 AM
To: Falk, Shane - GAB
Subject: FW: Open Records Request

Attachments: OR Request 20100104.pdf; Certification Testing re 7.23 and 7.24.pdf; ElBd7.pdf

OR Request)100104.pdf (209 K. ;ertification Testing re 7.23 ... ElBd7.pdf (6 KB)

Shane, FYI!

Best wishes and kind regards,
Nat

-----Original Message-----
From: Magney, Reid - GAB
Sent: Monday, January 04, 2010 9:26 AM
To: Haas, Michael R - GAB; Hein, Ross D - GAB
Cc: Robinson, Nathaniel E - GAB; Kennedy, Kevin - GAB
Subject: FW: Open Records Request

I just received this open records request from Mr. Washburn.

I will acknowledge receipt.

Thank you,

Reid

Reid Magney, public information officer
Wisconsin Government Accountability Board 608-267-7887, office 608-279-0477, cell
reid.magney@wi.gov

-----Original Message-----
From: john@WashburnResearch.org [mailto:john@WashburnResearch.org]
Sent: Monday, January 04, 2010 7:55 AM
To: Magney, Reid - GAB
Subject: Open Records Request

Dear Mr. Magney:

Please find attached my open records requests and two supporting documents which explain the context fo the two requests.

If you have any questions you may call me at 414-375-5777.

In Liberty,
John Washburn

N128W12795 Highland Road
Germantown, WI 53022
January 4, 2010

Reid Magney, Public Information Officer
Wisconsin Government accountability Board
212 East Washington Avenue, Third Floor
P.O. Box 7984
Madison, Wisconsin 53707-7984

Dear Mr. Magney:

On September 20, 2009 I sent an email to Ross Hein, Elections Specialist - Voting Equipment Certification Coordinator, a question regarding the certification of the new ES&S voting system, Election Systems & Software's (ES&S) Unity 3.2.0.0 Voting System which includes the DC200 optical scanner. The email is attached for reference. Mr. Hein assured me on the system can and does make the legally required backups and does so in a form which permits the clerks themselves to retain the backups as required by state election law.

I would like to make the following open records requests:

1. The electronic backup of the contents of each removable memory card used during certification testing of the Election Systems & Software's (ES&S) Unity 3.2.0.0 Voting System while that voting system was performing the first mock election required by ElBd 7.01(3). These backups are the backups created by the staff of the GAB during the certification testing in order to verify the Election Systems & Software's (ES&S) Unity 3.2.0.0 Voting System meets the minimum legal requirements of WI Stats. 7.23(1)(g) and WI Stats. 7.24.
2. The electronic backup of the contents of each removable memory card used during certification testing of the Election Systems & Software's (ES&S) Unity 3.2.0.0 Voting System while that voting system was performing the second mock election required by ElBd 7.01(3). These backups are the backups created by the staff of the GAB during the certification testing in order to verify the Election Systems & Software's (ES&S) Unity 3.2.0.0 Voting System meets the minimum legal requirements of WI Stats. 7.23(1)(g) and WI Stats. 7.24.
3. The electronic backup of the contents of each removable memory card used during certification testing of the Election Systems & Software's (ES&S) Unity 3.2.0.0 Voting System while that voting system was performing the third mock election required by ElBd 7.01(3). These backups are the backups created by the staff of the GAB during the certification testing in order to verify the Election Systems & Software's (ES&S) Unity 3.2.0.0 Voting System meets the minimum legal requirements of WI Stats. 7.23(1)(g) and WI Stats. 7.24.

Severability – The above open requests are separate and severable and are only including in this single correspondence in order to ease the administration of these requests and the thematic similarity among the requests. It is expected any delay in the production of records for one request will not impair or delay the production of records for another request.

Denial of Request – As required by Wisconsin's open records law as codified in §19, any denial, in whole or in part, of one or more of the public records requests above must state in writing and with specificity as to the reasons and statutory authority for denying the request. For the purposes of this requirement, an email response will be considered a written response.

Redaction – A redaction is a denial in part of requested record. There shall be a log which states in writing and with specificity to the reasons and statutory authority each redaction.

Duplication – If a single record satisfies one or more of the above requests, then only one copy of the record needs to be produced provide said record is accompanied by a notation as to which, multiple requests are satisfied by the record.

Promptness – The records requested above shall be provided "as soon as practicable" as required by Wisconsin statute.

Please contact me at your earliest convenience when these electronic records can be provided to me. If you have any questions, regarding this request you may contact me at this email address or at 414-375-5777.

In Liberty,
John Washburn

From: john@WashburnResearch.org
Sent: Monday, September 28, 2009 12:46 PM
To: Ross.Hein@wi.gov
Subject: Certification Testing re 7.23 and 7.24

Dear Mr. Hein:

I have two quick questions about the certification testing to be performed this week.

1) Will the mock election include a demonstration by the vendor that the system under test can produce the election records and backups required by WI Stats. 7.23(1)(f) and WI Stats. 7.23(1)(g)?

2) Are the backups created in order to comply with the legal mandates of 7.23(1)(f) and of 7.23(1)(g) in a form or on a medium which complies with WI Stats. 7.24? The statute, WI Stats. 7.24, requires the election clerks to assume and maintain title of ALL election records and is without exception as to whether the record is programming, data, or paper.

I ask this because the City of Milwaukee acknowledges they have failed to make records of the AutoMark programming as required by 7.23(1)(f) and 7.24.

Also the Town of Sugar Camp of Oneida County Wisconsin went with Option C of this GAB letter, http://elections.state.wi.us/docview.asp?docid=15541, for the 2008 general election and ES&S has now informed Clerk Bigley that ES&S has destroyed these 2008 election records.

There is also the matter of violating the records retention required by Federal statute, but I recognize the authority of the WI Government Accountability Board only extends to state statute and have thus limited my questions to items in chapter 7 as those items touch on the utility and merchantability of a certified voting as required by WI Stats 5.91(10)and WI Stats. 402.314(2)(c).

In Liberty,
John Washburn

Chapter ElBd 7

APPROVAL OF ELECTRONIC VOTING EQUIPMENT

ElBd 7.01 Application for approval of electronic voting system. (1) An application for approval of an electronic voting system shall be accompanied by all of the following:

(a) A signed agreement that the vendor shall pay all costs, related to approval of the system, incurred by the board, its designees and the vendor.

(b) Complete specifications for all hardware, firmware and software.

(c) All technical manuals and documentation related to the system.

(d) Complete instruction materials necessary for the operation of the equipment and a description of training available to users and purchasers.

(e) Reports from an independent testing authority accredited by the national association of state election directors (NASED) demonstrating that the voting system conforms to all the standards recommended by the federal elections commission.

(f) A signed agreement requiring that the vendor shall immediately notify the board of any modification to the voting system and requiring that the vendor will not offer, for use, sale or lease, any modified voting system, if the board notifies the vendor that the modifications require that the system be approved again.

(g) A list showing all the states and municipalities in which the system has been approved for use and the length of time that the equipment has been in use in those jurisdictions.

(2) The board shall determine if the application is complete and, if it is, shall so notify the vendor in writing. If it is not complete, the board shall so notify the vendor and shall detail any insufficiencies.

(3) If the application is complete, the vendor shall prepare the voting system for three mock elections, using offices, referenda questions and candidates provided by the board.

History: Cr. Register, June, 2000, No. 534, eff. 7-1-00.

ElBd 7.02 Agency testing of electronic voting system. (1) The board shall conduct a test of a voting system, submitted for approval under s. ElBd 7.01, to ensure that it meets the criteria set out in s. 5.91, Stats. The test shall be conducted using a mock election for the partisan primary, a mock general election with both a presidential and gubernatorial vote, and a mock nonpartisan election combined with a presidential preference vote.

(2) The board may use a panel of local election officials and electors to assist in its review of the voting system.

(3) The board may require that the voting system be used in an actual election as a condition of approval.

History: Cr. Register, June, 2000, No. 534, eff. 7-1-00.

ElBd 7.03 Continuing approval of electronic voting system. (1) The board may revoke the approval of any existing electronic voting system if it does not comply with the provisions of this chapter. As a condition of maintaining the board's approval for the use of the voting system, the vendor shall inform the board of all changes in the hardware, firmware and software and all jurisdictions using the voting system.

(2) The vendor shall, at its own expense, furnish, to an agent approved by the board, for placement in escrow, a copy of the programs, documentation and source code used for any election in the state.

(3) The electronic voting system must be capable of transferring the data contained in the system to an electronic recording medium, pursuant to the provisions of s. 7.23, Stats.

(4) The vendor shall ensure that election results can be exported on election night into a statewide database developed by the board.

(5) For good cause shown, the board may exempt any electronic voting system from strict compliance with ch. ElBd 7.

History: Cr. Register, June, 2000, No. 534, eff. 7-1-00.

State of Wisconsin\Government Accountability Board

212 East Washington Avenue, 3rd Floor
Post Office Box 7984
Madison, WI 53707-7984
Voice (608) 266-8005
Fax (608) 267-0500
E-mail: gab@wisconsin.gov
http://gab.wi.gov

JUDGE WILLIAM EICH
Chair

KEVIN J. KENNEDY
Director and General Counsel

Sent Via Email Only
(john@washburnresearch.org)

March 9, 2010

John Washburn
N128W12795 Highland Road
Germantown, WI 53022-1507

Mr. Washburn:

RE: Open Records Request
ES&S Certification Testing / Mock Elections Back-Ups of Memory Sticks

In your email dated January 4, 2010, you included an attachment that requested the following information pursuant to Wisconsin's Open Records Laws:

"I would like to make the following open records requests:

1. The electronic backup of the contents of each removable memory card used during certification testing of the Election Systems & Software's (ES&S) Unity 3.2.0.0 Voting System while that voting system was performing the first mock election required by ElBd 7.01(3). These backups are the backups created by the staff of the GAB during the certification testing in order to verify the Election Systems & Software's (ES&S) Unity 3.2.0.0 Voting System meets the minimum legal requirements of Wis. Stats. 7.23(1)(g) and WI Stats. 7.24.

2. The electronic backup of the contents of each removable memory card used during certification testing of the Election Systems & Software's (ES&S) Unity 3.2.0.0 Voting System while that voting system was performing the second mock election required by ElBd 7.01(3). These backups are the backups created by the staff of the GAB during the certification testing in order to verify the Election Systems & Software's (ES&S) Unity 3.2.0.0 Voting System meets the minimum legal requirements of WI Stats. 7.23(1)(g) and WI Stats. 7.24.

3. The electronic backup of the contents of each removable memory card used during certification testing of the Election Systems & Software's (ES&S) Unity 3.2.0.0 Voting System while that voting system was performing the third mock election required by ElBd 7.01(3). These backups are the backups created by the staff of the GAB during the certification testing in order to verify the Election Systems & Software's (ES&S) Unity 3.2.0.0 Voting System meets the minimum legal requirements of WI Stats. 7.23(1)(g) and WI Stats. 7.24."

After a thorough review of your request and applicable law, I regret to inform you that the Government Accountability Board has to deny your request with respect to the electronic backup contents of the one memory stick that remains in the possession of the Board. Board staff does not possess the additional two memory sticks any longer. Pursuant to information obtained from ES&S, they no longer possess the additional two memory sticks any longer.

Wisconsin has a presumption of open access to all public records, which is reflected in both our statutes and case law. See Sec. 19.31, Wis. Stats., and Linzmeyer v. Forcey, 2002 WI 84. "The right to inspect public records, however, is not absolute." Osborn v. Board of Regents 2002 WI 83, ¶ 14. "Access should be denied where the legislature or the court has predetermined that the public interest in keeping a record confidential outweighs the public's right to have access to the documents." Id. "Thus, the general presumption of our law is that public records shall be open to the public unless there is a clear statutory exception, unless there exists a limitation under the common law, or unless there is an overriding public interest in keeping the record confidential." Id. (emphasis added.) First, an agency must determine whether the open records law applies to the records in question. Linzmeyer at ¶ 10. Second, an agency must determine whether the presumption of openness under the open records law is overcome by any other public policy. Id. at ¶ 11. To determine whether the presumption of openness is overcome by another public policy concern, the agency should use a balancing test to weigh the public policies favoring confidentiality and the strong public policy that public records should be open for review. Id. at ¶ 12.

ES&S has asserted that the entirety of the electronic backup contents of the memory stick is trade secret and proprietary information. Pursuant to Sec. 19.36(5), Wis. Stats., an agency can withhold access to any record or portion of a record containing information qualifying as a trade secret as defined in Sec. 134.90(1)(c), Wis. Stats. "Trade secret" means information, including a formula, pattern, compilation, program, device, method, technique or process, which derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by, other persons who can obtain economic value from its disclosure or use. See Sec. 134.90(1)(c), Wis. Stats. In addition, to qualify as a "trade secret" the information should be the subject of efforts to maintain its secrecy that are reasonable under the circumstances. See Sec. 134.90(1)(c), Wis. Stats. See Also ECT International v. Zwerlein, 597 N.W.2d 479 (Wis. Ct. App. 1999)(From Sec. 134.90(1)(c), Wis. Stats., three attributes of a protectible trade secret exist: 1) must be information such as a formula, pattern, compilation, program, device, method, technique or process; 2) that has independent economic value, available from only one source; and 3) is the subject of reasonable efforts to maintain its secrecy.)

ES&S has asserted the following to substantiate the nature of the trade secret:

> "In accordance with Section 19.36(5) of WSA, trade secret information is exempt from disclosure under the State's public records statutes. The ES&S Proprietary Information contains trade secrets which identify certain methods, techniques and processes on the operation of ES7S' voting systems. Specifically, the ES&S Proprietary Information contained on the memory card includes certain methods, techniques and processes ES&S utilizes when programming, tabulating and reporting election results through the use of ES&S' proprietary voting system software. ES&S only allows those customers who have executed a Software License Agreement with ES&S to have access to and use ES&S' proprietary software and trade secret information, including ES&S' Proprietary information which is contained on the memory card. Such ES&S Software License Agreement contains the terms and conditions by which a customer may use ES&S' propriety software and trade secret information. As the ES&S Proprietary Information contains ES&S trade secret information and ES&S has not agreed to enter into a Software License Agreement with the individual requesting such ES&S Proprietary Information, the ES&S Proprietary Information requested should not be subject to disclose under the Wisconsin Statutes Annotated."

The Government Accountability Board has determined that the electronic backup of the memory stick contains compilation, program, device, method, technique, and process information that has independent economic value to ES&S. This information cannot be obtained from other sources beyond the manufacturer, ES&S. If this information were to become generally known or readily ascertainable by other persons, i.e. competitor voting equipment manufacturers or service providers, those other persons certainly could obtain economic value from the disclosure. ES&S has taken several steps to preserve the secrecy of information contained in the electronic backup of the memory stick and the Government Accountability Board finds those measures reasonable. For instance, ES&S requires Software License Agreements with individuals seeking this proprietary information. The Government Accountability Board finds that ES&S could suffer harm from disclosing the information you seek because it contains trade secrets that would be disclosed, if the information were released. Based upon the evidence and assertions of ES&S, the Government Accountability Board finds that the information you request qualifies for the trade secrets exemption from disclosure for purposes of the Open Records Law. In light of this, the Government Accountability Board is unable provide you with a copy of the electronic backup of the memory stick used for a mock election during the certification of the ES&S equipment and software.

Additionally, the Government Accountability Board has determined that the public policy of openness of public records is overcome by significant public policy concerns favoring keeping the information you seek confidential. The public policy of openness is set forth in paragraph two above. There are two significant items of public interest and policy that favor keeping the information you seek confidential: 1) public interest and policy to insure the security of voting systems in Wisconsin and 2) public interest and policy to insure greater access to a larger number and variety of competitive voting systems manufacturers for Wisconsin.

ES&S has asserted the following security interest:

> "In addition to ES&S' Proprietary Information containing trade secret information as discussed above, the disclosure of ES&S Proprietary Information by the State may compromise the security of ES&S' voting systems as the information contained on the memory device includes proprietary trade secret information and files related to the programming of the mock elections. Please be advised that ES&S takes every possible step to ensure its voting systems are secure, accurate and reliable, including requiring each customer to agree to certain terms and conditions related to the license and use of ES&S' software and related documentation. Included in these terms and conditions are actions which the customer is prohibited from taking, including but not limited to, causing or permitting any change to be made to the ES&S Software without ES&S' prior written consent. If the files, which are contained on the memory card, were to be provided to an individual or entity who was not under ES&S' strict licensing terms, such individual or entity may attempt to alter the files and information contained on the memory device and use such altered files in a compromising manner. As such, it is ES&S' position that all ES&S Proprietary Information contained on the memory card be exempt from disclosure under the WSA."

The Government Accountability Board has determined that there is a strong public interest and policy insuring the security of voting systems in Wisconsin. This public policy is statutorily prescribed as it relates to voting devices and equipment (Sec. 5.91(10), Wis. Stats.) and as it concerns the confidentiality of software components of voting systems (Sec. 5.905, Wis. Stats.) The Wisconsin legislature has already statutorily recognized the necessity of securing software components of voting systems in Sec. 5.905, Wis. Stats. Specifically, the legislature has stated that software components shall be secured and maintained "in strict confidence." Furthermore, the legislature has specifically provided that the Board "shall withhold access to those software components from any person who requests access under Sec. 19.35(1), Wis. Stats." The only exception to the prohibition of open records disclosures to the public under Sec. 5.905, Wis. Stats., occurs in the instance of a recount. Even in the instance of a recount, the legislature has provided that if the Board grants access to a software component, the Board shall require the grantee to enter "into a written agreement with the Board that obligates the person to exercise the highest degree of reasonable care to maintain the confidentiality of all proprietary information to which the person is provided access." Sec. 5.905(4), Wis. Stats.

The Legislature has also provided that devices and voting equipment must be "suitably designed for the purpose used, of durable construction, and is usable safely, securely, efficiently and accurately in the conduct of elections and counting of ballots." Sec. 5.91(10), Wis. Stats. Widely distributed trade secret, copyrighted, or patented information about voting equipment would damage the public interest and policy of securing Wisconsin voting systems. Similar to disclosure of software components, disclosure of mechanical and operational information about voting equipment could lead to election tampering or fraud, or even the appearance or vulnerability of the same. Similar to the trade secret discussion above, ES&S has asserted that disclosure of the electronic backup of the memory stick to the public could compromise the security of the ES&S voting systems because individuals who would otherwise not know how the systems are built or operated, would gain insight into such workings which may compromise the voting systems.

In order to preserve the public interest and policy of secure and fair elections absent even the appearance of tampering or fraud, the Wisconsin legislature has already codified a policy favoring no disclosure over the requirements of the Open Records Law in Sec. 19.35(1), Wis. Stats. The Government Accountability Board has determined that the public interest and policy to insure security of Wisconsin voting systems outweighs the public policy of openness. The information you request contains programming, mechanical and operational information about the ES&S voting systems that were tested in September 2009, which are trade secret or otherwise protected. Disclosure of this information could expose these particular voting systems to harm including tampering or fraud and harm the strong public policy favoring secure voting systems. Therefore, the Government Accountability Board is unable to fulfill your request for a copy of the electronic backup of the memory stick.

The Government Accountability Board has determined that there is a strong public interest and policy to insure greater access to a larger number and variety of competitive voting systems manufacturers for Wisconsin. This public interest and policy provides for competition of design, security, and efficiency of voting systems. Such a policy reinforces the strong public interest and policy insuring the security of voting systems in Wisconsin discussed above. With greater competition and availability of voting systems, Wisconsin can gain the benefit of new advances in voting systems technology, security and efficiency. Basic economic principles require manufacturers to protect proprietary information to keep a competitive edge over other

voting systems manufacturers. Competition to provide voting systems for Wisconsin can only occur if there is an economic benefit to the manufacturers. Widely distributed trade secret, copyrighted or otherwise protected, or patented information about voting systems would negate the ability of manufacturers to realize an economic benefit from making voting systems available in Wisconsin. The Government Accountability Board has determined that there is a strong public interest and policy favoring greater competition and more variety of voting systems in Wisconsin, which in turn reinforces the public interest and policy insuring security of voting systems in Wisconsin. This public interest and policy outweighs the public policy of openness.

The information you request contains programming, mechanical and operational information about the ES&S voting systems which were tested in September 2009, which is trade secret, copyrighted or otherwise protected, and patented. Disclosure of this information could be used by ES&S competitors and detrimentally affect ES&S's competitive and economic edge in Wisconsin. This in turn could result in reducing the number of voting systems manufacturers available to Wisconsin because releasing such information may cause manufacturers to refuse to sell their voting systems in Wisconsin. This would cause harm to the public interest and policy to insure greater access to a larger number and variety of competitive voting systems manufacturers in Wisconsin. Therefore, the Government Accountability Board is unable to fulfill your request for a copy of the electronic backup of the memory stick.

Pursuant to Sec. 19.35(4)(b), Wis. Stats., this determination is subject to review by mandamus under Sec. 19.37(1), Wis. Stats., or upon application to a district attorney or the Attorney General.

If you have any further questions, please do not hesitate to contact me at (608) 266-2094, or at Shane.Falk@wi.gov .

Sincerely,

SHANE W. FALK
Staff Counsel
Government Accountability Board

cc: Kevin J. Kennedy, Director and Legal Counsel
Nathaniel E. Robinson, Elections Division Administrator
Michael R. Haas, Staff Counsel
Ross Hein, Elections Specialist
David Buerger, Elections Specialist
GOVERNMENT ACCOUNTABILITY BOARD

ES&S, Attn: Timothy J. Hallet, Assoc. General Counsel
(Via Email Only)

John Washburn

From: john@WashburnResearch.org
Sent: Tuesday, March 09, 2010 1:38 PM
To: shane.falk@wisconsin.gov; john@washburnresearch.org; kevin.kennedy@wisconsin.gov; nathaniel.robinson@wisconsin.gov; michael.haas@wisconsin.gov; tjhallett@essvote.com
Cc: rdreps@gklaw.com
Subject: Re: Open Records Request--ES&S Memory Stick Backup Contents

Dear Mr. Falk:

I must respectfully disagree with your assertion that the memory stick is part of a voting system and your second assertion that the backups made pursuant to WI 7.23(1)(g) can be (in whole or in part) a trade secret.

As respects the first point, the records are not part of a voting system as covered by WI stat 5.905. I have not asked for any "vote-counting source code, table structures, modules, program narratives and other human-readable computer instructions used to count votes with an electronic voting system" software components. And, unless you can demonstrate that the GAB has already placed the contents of the 7.23(1)(g) backups made during the mock election into escrow pursuant to 5.905, then the GAB also does not consider anything of the 7.23(1)(g) to be "vote-counting source code, table structures, modules, program narratives and other human-readable computer instructions used to count votes with an electronic voting system". As such there is nothing contained in the 7.23(1)(g) mandated backups which is covered by the security concerns that the legislature has addressed through WI Stats. 5.905.

On a related note, the "security through obscurity" model invoked here by the GAB and ES&S is discredited by all who take security seriously. The most spectacular failure of "security through obscurity" model was the NSA developed "Skipjack" [see: http://en.wikipedia.org/wiki/Skipjack_(cipher)].
For 5 years the algorithm at the heart of the Clipper chip initiative was classified and independent authorities tested the algorithm. Those independent testing authorities assured the public that the algorithm and its implementation were secure. The algorithm was declassified 4 years after Matt Blaze demonstrated the Clipper protocol was defective. Within 48 hours of de-classification though, the Skipjack algorithm itself was shown to be fatally flawed. I cannot help but note the ominous and dangerous parallels the GAB and ES&S are drawing between the Skipjack algorithm and the election records created pursuant to WI 7.23(1)(g).

The second point is the offensive assertion that election records can be a secret and that, moreover, be the trade secreted election record is property of someone OTHER than an election official of the State of Wisconsin (ES&S in this case). The contents of the memory cards fail to meet the statutory DEFINITON of trade secret as it is defined in 134.90(1)(c)2 Subjecting ANY election record to ANY secrecy is an "unreasonable effort to maintain its secrecy that are unreasonable under the circumstances". Therefore, the contents of the memory cards fail to meet the statutory definition of a trade secret and thus cannot be exempted as a trade secret.

The backups created pursuant to WI Stats. 7.23(1)(g) are election records.

Moreover, these election records are "required to be kept" records and thus enjoy an absolute right of access [see:
http://www.doj.state.wi.us/dls/OMPR/2009OMCG-PRO/2009 Pub Rec Outline.pdf].
These election records [the statutorily required backups made pursuant to WI Stats. 7.23(1)(g)] are ""required to be kept" records because:
1) The creation of the record is expressly mandated by statute [7.23(1)(g)]
2) The custodian of the record is expressly mandated by statute [7.24]
3) The retention period of the record is expressly mandated by statute [7.23(1)(g)]

After consulting with my attorney, I will decide on how best to appealing this finding.

In Liberty,
John Washburn

----
mail2web.com – Enhanced email for the mobile individual based on Microsoft® Exchange -
http://link.mail2web.com/Personal/EnhancedEmail

No virus found in this incoming message.
Checked by AVG - www.avg.com
Version: 9.0.733 / Virus Database: 271.1.1/2733 - Release Date: 03/09/10 13:33:00

From: John Washburn [john@washburnresearch.org]
Sent: Friday, February 05, 2010 9:56 PM
To: 'Plotkin, Adam'; 'Wahl, Andrea'
Subject: RE: Another article on retaining memoyr cards

Yes but I did not include a link to the article.

DOH !!

BBV article: http://www.bbvforums.org/forums/messages/7659/76240.html?1265145348
Texas Sheriff Story: http://stxc.blogspot.com/2008/06/incumbent-webb-county-sheriff-attacks.html
OH report: http://www.bbvdocs.org/OH/state/AcademicFinalEVERESTReport.pdf

From: Plotkin, Adam [mailto:Adam.Plotkin@legis.wisconsin.gov]
Sent: Friday, February 05, 2010 8:53 AM
To: john@washburnresearch.org; Wahl, Andrea
Subject: RE: Another article on retaining memoyr cards

Thanks John.

Adam Plotkin
Clerk, Committee on Labor, Elections, and Urban Affairs
Office of Senator Spencer Coggs
phone, 608-266-2500
fax, 608-282-3546

From: John Washburn [mailto:john@washburnresearch.org]
Sent: Friday, February 05, 2010 8:33 AM
To: Wahl, Andrea; Plotkin, Adam
Subject: Another article on retaining memoyr cards

Dear Andrea and Adam:

I would like to add the article below, the linked newspaper article, and the linked OH Everest study to the committees archives on SB-535 and AB-646. In the particular case at hand the removable memory card called a PEB had different contents than the removable memory cards called the compact flash. Under the current statute 7.23(1)(g) the contents of both are required to be backed up and preserved. This is not happening, but it is supposed too.

The vote total and "ballot image"[1] contents of the two kind of removable memory cards should be the same, but was not. Be nice if these had been kept here in Wisconsin to see if this defect in the ES&S used in the state. But, no such records were retained nor would be retained under the GAB proposal because "ballot images" are not covered by the proposed language of AB-646 or SB-435. The ES&S iVotronic, M100's, M150's,and M650's are used in 25 of Wisconsin's 72 counties. See: http://elections.state.wi.us/docview.asp?docid=2728&locid=47

I have created a login now on the notify system. The notify system is still broken, but the tech team work out a way for me personally to avoid the defect for my particular account. If the notice for the initial hearings on AB-646 or SB435 have already been posted then I missed them. If the initial hearing for next week are already schedule can you let me know the dates so that I may make arrangements with my employer to have the day off to come to Madison from Milwaukee?

In Liberty,
John Washburn

[1]“Ballot Images” are neither pictures not graphical representations of ballots.

America's Elections Watchdog Group

BlackBoxVoting.org

SHORTCUTS: How to find what you're looking for

SHOW SUPPORT

LATEST NEWS

INVESTIGATIONS

PRESS KIT

FORUMS

CONTACT

HOME

(ES&S) 6/08 - iVotronic, Unity: Flash...

Original URL: http://www.bbvforums.org/forums/messages/7659/76240.html?1265145348

Author

Bev Harris
Board Administrator
Username: Admin

Post Number: 8669
Registered: 12-2004

Best of Black Box? N/A
Votes: 0 (A keeper?)

Message

Posted on Thursday, June 26, 2008 - 7:37 am:

(From BBV admin): Results on cartridges don't match results from the flash card. Please see following post for an excerpt from the EVEREST report which will shed more light on this.

South Texas Chisme blog - June 19, 2008; Also independent corroboration provided to Black Box Voting by e-mail

http://stxc.blogspot.com/2008/06/incumbent-webb-county-sheriff-attacks.html

Incumbent Webb County Sheriff attacks integrity of E&S voting machines in his recount loss

After the primary election, Martin Cuellar beat incumbent Rick Flores by 37 votes. After the first recount, Flores beat Cuellar by 133 votes, a 170 vote swing. After the second recount, Cuellar came out on top by 39 votes. The second recount was monitored by the court and allowed poll watchers to actually watch. E&S [sic]software is blamed for difference in election day results versus second recount results.

[Webb County Elections Administrator Oscar Villarreal] said electronic voting machines use what is called a Personal Electronic Ballot (PEB), which is a cartridge that stores vote information. The PEB is inserted in a computer that tallies the votes.

"That (information) is downloaded into the computer, and the computer includes it into the totals," he said. "On a recount, you can't print ballot images from the PEB; you have to actually insert a flashcard."

Navigation
Topics
Log In
Log Out

Special Search
New Today
New This Week
Advanced Search
Tree View

Your Account
Edit Profile
Register
Forgot Password

Tools
Help/Instructions
Policies

CLICK STATE TO SEE:

"WATCH LIST"

Marked with:

"OPEN & HONEST"
Marked with:

He said Precinct 231 illustrated the problem.

"In 231, it was reported that 72 people voted (electronically) ... on election night through the PEB," he said. "When ballot images were shown from the flashcards, it was only showing 43."

That seems like a large software problem to me.

In the recount of the electronic voting machines the discrepancies were almost evenly split between the two candidates with Flores actually gaining one vote.

There were discrepancies election night with double counting of some ballots boxes and then a correction.

The first recount smells like a large farting elephant in the room. Cuellar's attorneys called for an investigation and the Webb County Democratic party chair, Sergio Mora, agreed.

Bev Harris
Board Administrator
Username: Admin

Post Number: 8670
Registered: 12-2004

Best of Black Box? N/A
Votes: 0 (A keeper?)

Posted on Thursday, June 26, 2008 - 7:39 am:

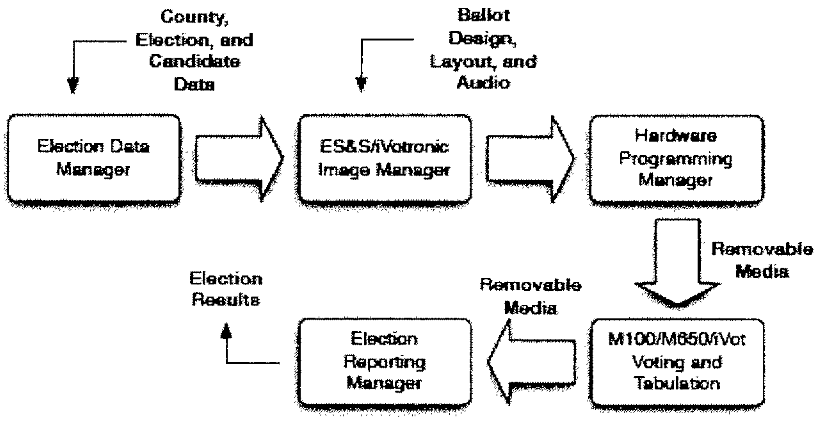
Webb County uses the ES&S iVotronic system for polling place votes, the M100 for absentees, and the ES&S Unity election management system. See items marked in red that indicate something is amiss in Webb County.

See Election Systems & Software (ES&S) section in EVEREST academic report:

Here is a copy of the full report, which was commissioned by the state of Ohio: http://www.bbvdocs.org/OH/state/AcademicFinalEVERESTReport.pdf

Relevant excerpts:

Flow chart showing how ES&S components fit together


County, Election, and Candidate Data
Ballot Design, Layout, and Audio
Election Data Manager
ES&S/iVotronic Image Manager
Hardware Programming Manager
Removable Media
M100/M650/iVot Voting and Tabulation
Removable Media
Election Reporting Manager
Election Results

Pg 32: iVotronic terminals are activated using special hardware tokens called **Personalized Electronic Ballots (PEBs)**, which are also used to store ballot definitions and election results. PEBs are typically programmed via a supervisor terminal at the start of an election, and read using either a supervisor terminal or a dedicated PEB Reader connected to the machine running the Election Reporting Manager at the end of an election.

Pg 32: The voter iVotronics also use **Compact Flash cards** to store large ballots, audio ballots, and election result audit files.

Pg 33: 5.2.1 Unity
Unity is the Windows-based software suite for managing elections. It contains tools for creating and managing election databases (**Election Data Manager**), designing the appearance of ballots (ES&S and iVotronic Image Managers, AutoMARK Information Management System), tabulating and reporting results Election Reporting Manager). Additionally, there is a tool to audit the use of the other components of Unity (**Audit Manager**), and a tool for abstracting programming and communicating with the various hardware components used by several Unity components (**Hardware Programming Manager**). The various components of Unity communicate with each other indirectly through common files stored on the Windows filesystem.

Pg. 33: **Election Data Manager** The Unity Election Data Manager **(EDM)** is a Windows XP application which is used for creating and updating the election database used by the other software components of Unity. The database for each county is stored in a single file in the Windows filesystem known as the "Ballot Data File" (BDF)

Each BDF is logically made up of two different databases: the "County Database" which contains tables of data which does not change from election to election, and the "Election Database" which contains the data defining a single election. Reusing the County Database from election to election is encouraged through an import feature which copies from a prior election's BDF to a new one, and the initial County Database can be filled in from another county's BDF as well. The remaining data entry is done either through the Windows GUI, or by importing text files in a number of formats.

In addition to specifying the races, candidates, proposals and other data that will appear on the ballot for an election, EDM is also used to select the equipment which will be used to cast votes in the election and specify any policies particular to the jurisdiction which influence ballot design (e.g. candidate position rotation). Finally, centralized configuration of the iVotronic passwords (see below) is performed from within EDM.

Other modules of Unity read and parse the BDF directly, as well as using "Intermediate Interface Files" (IFF) and "Ballot Set Collection" (BSC) files produced by EDM in a process referred to as "merging the election database". While the ballot data file is updated automatically when any changes are made in EDM, the other files must be re-generated by merging the election again.

Pg 34: **iVotronic Image Manager**

The iVotronic Image Manager (iVIM) is a Java Windows application for designing text, graphical, and audio ballots for the iVotronic DRM. iVIM relies on a MySQL database server to store its settings, which can either be installed on the same machine as iVIM or accessed remotely. The main input to iVIM is an XML file exported by EDM, along with graphical templates bundled with iVIM. Once layout is complete, iVIM exports the ballots as an iVotronic Election Definition file and a folder containing bitmap images and file hierarchy for the **iVotronic Compact Flash card**. Audio ballots for ADA voting are not managed within iVIM. Instead, an HTML document listing the necessary recordings and filenames to save them as is produced along with the other output files.

Pg 35: **Election Reporting Manager**

The Election Reporting Manager (ERM) is used to collect and report results from an election. Like HPM, it is a COBOL Windows program which relies on several helper applications and libraries written in other programming languages to access the removable media containing votes. It uses the same directory of data files generated by HPM upon importing an IFC file, and creates a new election database file used to store results.

Election results are collected from M100 and M650 scanners directly using an external PCMCIA card reader and Zip drive. **iVotronic results can be collected either from the Compact Flash card ["CF card"] of each machine, or from the Master PEB used to close several iVotronics.** The CF card is read directly using a USB card reader, while the Master PEB can be read using either a Supervisor iVotronic or PEB Reader connected to the serial port of the machine running ERM using the same command-line tool used by HPM.

Once retrieved from memory devices, the COBOL code processes the results files and records the official election results. ERM has features for producing election reports per contest, per precinct or summary results. Additional details that can be reported include the totals for each type of ES&S tabulation device.

Pg 37: 5.2.4 **Personalized Electronic Ballot**
The Personalized Electronic Ballot (PEB) is a palm-sized device containing a PIC microcontroller, 2MB of flash storage, a bi-directional infrared (IR) transceiver, and battery. The PEB is activated by a magnetic reed switch, and contains a magnet to activate the corresponding reed switch in the iVotronic PEB socket.

In addition to the flash storage, the PIC microcontroller contains a small amount of non-volatile storage which is "burned" to the PIC during the PEB manufacturing process. This area contains the PEB firmware, PEB firmware version number, PEB hardware revision number, PEB serial number, and 'PEB Kind' variable.

The microcontroller firmware implements the passive half of a very simple command/response protocol between the PEB and host over the PEB IR port using IrDA SIR (Serial Infrared). The host sends the PEB one of several commands along with an address and fixed mount of data depending on the command, and the PEB performs the command and returns a response and command-determined amount of data. The primary operation is reading and writing 128 byte blocks of the PEB's flash memory, or verifying the integrity of blocks using a cyclic redundancy check (CRC) stored with each block. In addition, the serial number, PEB kind, battery voltage can all be retrieved but not modified by the host device. While all PEBs are internally identical in construction, they are discernible from one another by the read-only information burned in the PIC: their serial number, and more importantly by their PEB Kind (both read-only values once the PIC inside is burned). The two documented PEB Kinds are supervisor and voter, which are visually differentiated by a red and blue band in the casing. ... **There is a third (undocumented) PEB Kind recognized in the iVotronic source code**.

Pg 37-38: **5.2.5 PEB Reader**
The PEB Reader is a standalone cradle used by devices with standard RS232 serial

ports to communicate with PEBs. It acts as a media converter between the RS232 serial connection and the IrDA connection to the PEB. The PEB Reader does not contain any functionality in hardware other than this media conversion; all protocol implementation for communicating with a PEB must be done in software on the device connected to the PEB Reader. Despite its name, there is nothing preventing a PEB Reader from being used to issue commands to write to or erase a PEB if controlled by suitable software.

Pg 38: **5.2.6 Compact Flash Cards**
Standard Type I Compact Flash cards are used by Unity and the iVotronic to hold files too large to fit in the PEB flash storage as well as audio ballots and audit and results data. Cards contain a standard FAT16 Windows filesystem and are accessed through a dedicated slot in the iVotronic and an external USB reader on the Unity PC. In Windows, these are mounted to the desktop and accessible to any Windows application with no special libraries.

The ballot data is accessed by the iVotronic on demand, but the presence of the CF card is checked periodically and the iVotronic will not boot without its presence. **That same CF card must be present to close the polls**. An audit log can be saved to the card when the polls are closed. It is a raw dump of the internal flash memory, compressed and encrypted before saving.

Pg 41: **Election Day**
On election day poll workers unpack and set up
the blue iVotronic terminals, plug in the RTAL printer [not applicable in Texas - this is the voter verified paper trail] and power cables. A properly programmed CF card must already be installed in the terminal, (this is usually done at Election Central and a tamper-evident security seal usually placed over the CF slot), before powering the terminal on. **A master PEB is required to open each terminal for voting, and only that same master PEB can be used to close the terminal after the polls have closed.** At this time a zero tape showing no votes cast may be printed, but this is optional. For each voter, a supervisor PEB containing the ballot images must be inserted into the iVotronic. Insertion of the PEB turns on the iVotronic, checks the EQC, and initializes (loads in) the ballot. The poll worker removes the supervisor PEB, the voter votes, the RTAL printer prints the results [RTAL may not be applicable in Texas] and the electronic ballot is stored internally in the iVotronic until the terminal is closed.

Pg 41: **Vote Tallying**
To close a terminal, the master PEB is inserted, which collects and stores the tabulated data, copies of the "images" of the ballots cast and time and date information. At closing the iVotronic firmware automatically uploads Audit Data onto the CF card. At this time a results tape can be printed using a special

external printer.

The results tape, zero tapes, Compact Flash cards, and Master PEB are then returned to Election Central.

At Election Central **the results can be imported into ERM using either the Master PEBs or the Audit Image on the CF cards.**

Pg 49: **We found fundamental security deficiencies throughout the ES&S Unity EMS, iVotronic DRE and M100 optical scanner software and hardware.** Virtually every mechanism for assuring the integrity of precinct results and for protecting the back-end tallying system can be circumvented. Election results can be tampered with in the ES&S system by exploiting any of a number of different vulnerabilities we discovered. The normal access provided to individual precinct poll workers (and in some cases to voters themselves) is sufficient to conduct attacks that alter county-wide election results and that, in some cases, cannot be detected or recovered from through audits or recounts.

Pg 49-50: **6.1 Ineffective Access Control**
The firmware and configuration of the ES&S precinct hardware can be easily tampered with in the field. Virtually every piece of critical data at a precinct – including precinct vote tallies, equipment configuration and equipment firmware – can be compromised through exposed interfaces, without knowledge of passwords and without the use of any specialized proprietary hardware.

Pg 50: **6.1.1 iVotronic passwords and PEB-based access controls**
Access to the iVotronic DRE configuration is protected by several hardware and password mechanisms, **all of which can be defeated through apparently routine poll worker (and in some cases voter) access**.

The primary mechanisms for preparing iVotronic DREs for deployment at precincts and for managing them throughout the election day (e.g., enabling them for each voter) employ the Personalized Electronic Ballot (PEB) interface.

As discussed in Chapter 5, a PEB is a small module that communicates with the iVotronic via a magnetically switched infrared (IrDA) bidirectional data interface on the face (voter side) of the terminal. PEBs are used for several different kinds of functions. Some of these functions are intended to be performed at the county headquarters (e.g., loading ballot definitions and basic configurations), while others are performed by poll workers (e.g., opening the terminals at the beginning of the day, enabling a voter to use a particular ballot, closing the terminal and collecting vote totals). In the mode used in Ohio, the PEB slot is empty whenever a voter is voting. PEBs are used as external memory devices that communicate through a simple protocol that allows the iVotronic to read and write memory blocks stored in the PEB. **Access to PEB memory is not protected by encryption or passwords**, although some of the data stored on them is encrypted (see Section 6.4). PEBs themselves are proprietary devices (and are apparently not commercially available except through ES&S). However, they employ a widely-used infrared communication standard (called IrDA).

In spite of the proprietary nature of the "official" PEB, **we found it to be relatively simple to emulate a PEB to an iVotronic or to read or alter the contents of a PEB using only inexpensive and commercially available IrDA-based computing devices (such as Palm Pilot PDAs and various mobile telephones**).

Most of the administrative and poll worker functions of the iVotronic (e.g., pre-election ballot loading, enabling voting, etc) require the insertion of a properly configured "supervisor" PEB and, in some cases, the entry of a password on the terminal touchscreen. However, **we found it to be possible to defeat both of these security mechanisms.** This makes practical several possible attacks at polling stations.

Pg 51: **Undocumented PEB features can be used to bypass password checks**
Many of the more sensitive iVotronic administrative functions (closing the polls, clearing the terminal, etc) require the entry of passwords in addition to the insertion of a supervisor PEB. **However, there is a special Quality Assurance (QA) PEB type recognized by the iVotronic firmware that behaves essentially as a supervisor PEB but that, when used, does not require the entry of any passwords. This PEB type does not appear to have been described or documented in any of the ES&S manuals or training materials** provided to our review.

This undocumented PEB feature can be used to neutralize the security of any iVotronic administration features that depend on passwords, no matter how carefully passwords are managed by a county. Anyone with such a PEB – whether it was supplied by ES&S, stolen, or emulated with a palmtop computer – effectively has a "back door" that bypasses this basic security check. As noted above, a simple Palm Pilot-type device can be programmed to emulate a PEB. QA PEBs are no more difficult to emulate than regular supervisor PEBs; they are similar to supervisor PEBs but with a single character changed in the communication protocol.

Note that while the QA PEB bypasses password checks, there is another iVotronic security feature required for access to some (but not all) administrative functions, For these functions, a PEB must be configured with the correct Election Qualification Code (EQC) (a 32 bit random number assigned for each election). However, as noted in the next section, precinct poll workers (and others with brief access to the poll worker equipment) can easily extract this code from the precinct's supervisor PEB using a palmtop computer.

Pg 51: **Unauthorized PEB copying and alteration**
Anyone with physical access to polling station PEBs can easily extract or alter their memory. This requires only a small magnet and a conventional IrDA-based palmtop computer (exactly the same kind of readily available hardware that can be used to emulate a PEB to an iVotronic terminal). Because PEBs themselves enforce no passwords or access control features, physical contact with a PEB (or sufficient proximity to activate its magnetic switch and IR window) is sufficient to allow reading or writing of its memory.

The ease of reading and altering PEB memory facilitates a number of powerful attacks against a precinct's results and even against county-wide results. An attacker who extracts the correct EQC, cryptographic key, and ballot definition can perform any election function on a corresponding iVotronic terminal, including enabling voting, closing the terminal, loading firmware, and so on. An attacker who has access to a precinct's main PEB when the polls are being closed can alter the precinct's reported vote tallies, and, as noted in Section 6.3, can inject code that takes control over the county-wide back-end system (and that thus affects the results reported for all of a county's precincts).

Pg 52: **6.1.2 Physical security, locks and seals**
Many aspects of the ES&S system's security as a whole depend on the integrity of the interfaces and removable media associated with precinct equipment. Some of these interfaces and media are protected by software security (e.g., access passwords, encryption, etc); potential attacks against such mechanisms are discussed in other sections of this report. Many interfaces and media are also protected (partly or entirely) by physical mechanisms: locks, seals, and procedures.

Although this study did not aim to conduct an exhaustive analysis of the physical security of the ES&S equipment, **we found many of the basic physical security features that protect precinct hardware to be ineffective or easily defeated**.

iVotronic
Several features of the iVotronic's physical security were especially problematic:

- The PEB interface on the iVotronic terminal is exposed and readily accessible to the user during voting. As noted above, this facilitates several important attacks.

Pg 53: **6.2 Critical Errors in Input Processing**
At least two critical components of the ES&S system suffer from exploitable errors in functions that process input over their external interfaces. Both the Unity tallying system and the iVotronic terminal have buffer overflow software bugs that allow an attacker who can provide input (e.g., on a PEB or memory card) to effectively take control over the system. A buffer overflow in input processing is common type of programming error, one that has been responsible for many security failures in modern computing. Avoiding buffer overflows in input processing is regarded as one of the most basic defenses a system must have.

We found numerous buffer overflows throughout the ES&S system. Several of these buffer overflows – in the Unity tallying software and in the iVotronic terminal firmware – have extremely serious practical security implications. **An attacker who can present input to any these systems (on an iVotronic PEB or on an M100 memory card from a precinct) can exercise complete control over the results reported by the entire county election system**.

Most seriously, the nature of these vulnerabilities means that there are few barriers to obtaining the access required to exploit them. In the case of the iVotronic system, voter access to the terminal is sufficient.

In the case of the Unity system, brief access to any iVotronic or M100 optical scan results media returned back to the county for processing is sufficient. As discussed in the Section 6.3, it is also possible to carry out the attacks against the Unity system by tampering with the firmware of precinct equipment.

Pg 53: **6.2.1 Unity**
The Unity election management system processes all precinct results and produces the tally reports that, in most cases, constitute the official tallies in races. After polls are closed, precinct-counted ballot results are received into Unity through several different media, including iVotronic PEBs, iVotronic CF cards, and M100 PCMCIA memory cards.

While Unity appears to correctly process properly-formatted results from such media, buffer overflows in Unity allow a maliciously altered iVotronic or M100 tally from a precinct to execute arbitrary software on the computer on which Unity runs, to replace or alter the Unity software, and to make arbitrary changes to the tally database and other election records. There may be no indication to the operator that this is occurring, and a system thus corrupted may continue to appear to operate normally when it is actually running software controlled by an attacker.

Because these attacks are carried out entirely through media routinely brought in to the county headquarters from precincts on election night, an attacker need not have any physical access to the secure county facility in which Unity is located. It is entirely sufficient for the attacker to have access to media (such as PEBs or M100 memory cards) returned to the county at the end of the election, or to equipment (such as iVotronics and M100s) that write to such media. Poll workers handle such media in the normal course of their duties, and may have unsupervised access at various times of the day.

And as noted in the next section, a voter using an iVotronic DRE may be able to circumvent the iVotronic terminal in a way that causes it to automatically produce such media when the polls close at the end of the day.

Note that because these vulnerabilities affect the central counting system, a corrupted media attack conducted from any single precinct can corrupt results for the entire county.

We have successfully implemented PEB-based attacks against Unity (at the University of Pennsylvania and atWebWise) **and have confirmed that such attacks represent a readily-exploitable threat** in both iVotronic and M100-based systems.

Pg 54: **6.2.2 iVotronic**
The iVotronic terminal firmware has several exploitable buffer overflow errors in its PEB input processing functions. These buffer overflows **allow a PEB** containing carefully-structured data (or an emulated PEB based on a palmtop computer) **to take control over the terminal.** The implications of attacks against iVotronics are discussed in Section 6.3.

We found it to be straightforward to exploit the iVotronic buffer overflows in several different ways (by emulation of a QA or supervisor PEB with a palmtop computer or by writing data to a precinct's supervisor PEB) at various times while opening polls and during the polling day), and with various degrees of access (as a poll worker or as a voter). The exposed nature of the PEB port and the many different scenarios under which it can be exploited make attacks against the iVotronic very difficult to effectively guard against under operational election conditions.

Pg 54: **6.3 Ineffectively Protected Software and Firmware**

The integrity of election results depends heavily on the integrity of the software and firmware that runs the central election management system and the precinct hardware. The consequences of any attack that alters, replaces or otherwise compromises this software or firmware are sweeping and often impossible to recover from. The security features that protect election software and firmware from unauthorized tampering are therefore among the most critically important safeguards in the system as a whole.

We found exploitable vulnerabilities that allow an attacker to replace or alter the firmware and software of virtually every component of the ES&S system, either by circumventing access controls or by triggering software errors.

Pg 54: **6.3.1 iVotronic firmware**
The iVotronic terminal is based on an Intel 80386 embedded computer processor controlled by firmware stored on an internal flash memory chip. **The firmware is designed to be field-updated** through an administrative menu function, with new firmware loaded though the terminal's CF card interface. Four security mechanisms are intended to protect against unauthorized firmware loading:

- Access to the firmware update menu function requires a supervisor (or QA) PEB.

- A 6-8 character password is required to enable firmware update.

- The firmware is loaded through the CF card interface, which can be protected by a sealed sliding cover.

- The firmware update function is disabled while the polls are open.

Unfortunately, these mechanisms are ineffective. **We found several practical ways for an attacker to bypass each of these security mechanisms and successfully replace or alter the iVotronic firmware, without knowledge of any passwords or secret election parameters, possession of a PEB, or breaking any seals.** We found ways to carry out these attacks even when the polls are open. It is possible, for example, for a voter (with no inside assistance) to load new firmware into an iVotronic after he or she is finished voting.

We found at least three different vectors that an attacker could exploit to load unauthorized iVotronic firmware under various circumstances.

Pg 55: **Via direct replacement of the internal flash chip**: The iVotronic terminal housing can be disassembled easily without breaking the seal that protects the CF slot. Disassembly requires only the use of a readily available Torx security screwdriver. Once the housing has been removed, the internal flash chip can be removed from its socket, reprogrammed with a standard flash writer, and replaced. Note that while surreptitious terminal disassembly is unlikely to be possible in an active polling place, it may be an attractive option for an attacker who enjoys unsupervised access to stored terminals (e.g., the night before an election).

Via the firmware update menu: This is the most direct attack against firmware. As discussed above, a palmtop computer and a magnet can be used to emulate a QA PEB and bypass the password check. If the polls are open, they can be closed by using a an emulated QA PEB to clear the terminal first. Note that with this approach, the firmware must be loaded though the external CF card interface, which might be protected with a tamper-evident seal (although that seal can be bypassed by removing the housing).

Via the PEB interface, during the polling day: This is perhaps the most serious practical threat to the iVotronic firmware. As discussed in Section 6.2, errors in the iVotronic's PEB input processing code allow anyone with access to the PEB slot on the face of the terminal including a voter) to load malicious software that takes complete control over the iVotronic's processor. Once loaded, this software can alter the terminal firmware, change recorded votes, mis-record future votes, and so on throughout the election day and in future elections.

Any attack that compromises iVotronic firmware is extremely serious; it can be very difficult to detect whether such firmware has been used in a live election or meaningfully recover once it has. The firmware controls every aspect of the ballot presented to voters, the recorded votes, and the interface to the tally system.

...

Compounding the problem is the fact that there are apparently no tools available to counties in the ES&S system that reliably extract or audit the actual firmware present in any given terminal. The version number is displayed at boot time, but that is not a reliable indication of whether the firmware has been compromised, since the message is part of the firmware itself. Compromised firmware can display any version number that it wishes to impersonate.

The iVotronic firmware code includes a number of internal consistency checks intended to detect corrupted firmware. While these checks may be able to detect accidental memory errors, they are ineffective against maliciously installed firmware, which can simply bypass or omit the integrity check functions.

Pg 56: **6.3.4 Viral propagation**

The software or firmware of almost every major component of the ES&S system can be altered or replaced by input from the other components with which it communicates. In particular, note that, by design or software flaw:

- The Unity system software can be modified by election results media originating from iVotronics and M100s (due to Unity buffer overflows)

- The iVotronic firmware can be modified by configuration media originating from the Unity system (due to iVotronic buffer overflows).

Pg 57: **6.4 Ineffective Cryptography and Data Authentication**
Much of the critical election data in the ES&S system – ballot definitions, precinct vote tallies, and so on – are communicated between the central county headquarters and precincts through small removable storage media. In iVotronic DRE-based systems, the primary media are PEBs and, in some cases, CF memory cards. In M100-based precinct counted optical scan systems, the primary media are PCMCIA memory cards.

These media share two important characteristics that make them attractive targets for attack: they have no intrinsic security properties of their own and they may pass through many hands on the way to polling places, during the polling day, and back from polling places. **That is, it is simple to read or alter data on these media,** and many people may have the opportunity to do so during an election. For example, iVotronic PEBs are handled by poll workers all through an election day, with memory that can be read or written with a standard palmtop computer and a small magnet. PCMCIA and CF cards, similarly, can be readily read or altered with standard laptop computers.

The usual approach (indeed, generally the only practical approach) for securing data stored on such media is the use of cryptographic techniques that prevent meaningful access to data without knowledge of the correct key.

Unfortunately, the ES&S system does not employ cryptography at all in the M100-based optical scan system. **The iVotronic DRE system does use cryptography, but errors in its implementation render the protection completely ineffective.**

The lack of effective cryptographic protection enables a large fraction of the exploitable vulnerabilities discussed in this report.

Pg 57-58: **6.4.2 Ineffective iVotronic cryptography**
The iVotronic DRE uses cryptography to protect data stored on the PEB and in the CF card. The Blowfish cipher is used.4 Unfortunately, the manner in which the encrypted data is stored on the PEBs effectively neutralizes the cryptographic

protection. The PEB contains an EQC, encoded using an unkeyed (non-cryptographic) algorithm. The EQC is used to encrypt the Blowfish key, which is used to the encrypt the rest of the data on the PEB. That is, although much of data on the PEB is encrypted, there is unencrypted information stored along with it that allows an attacker to easily discover the key.

There are at least another 40 pages of documented and proven attack vectors and specific vulnerabilities in this report. In short, when you have data that does not match between the PEB and the Compact Flash card, there is data corruption or tampering in the system. In the system with no voter verified paper trail, as is used in Webb County Texas where the PEB reportedly didn't match the CF card, it is not possible to authenticate the results.

Geoffrey R. Pollich
Voting Rights Forum Participant
Username: Gpollich

Post Number: 1
Registered: 2-2010

Best of Black Box? N/A
Votes: 0 (A keeper?)

Posted on Tuesday, February 2, 2010 - 9:20 am:

A question - the main firmare is located in the iVo on the U1 chip - now the U2 contains the ballot info and tally as part of the triple redundancy scheme. If the U2 is compromised or contains non-certified code (such as am earlier version of the certified firmware - can that be accessed or altered by the CF slot? I realize the U1 can be (this what is read when the unit boots)- what about the U2 where the actual election data is held...

Catherine Ansbro
Frequent Voting Rights Forum Participant
Username: Catherine_a

Post Number: 5637
Registered: 12-2004

Best of Black Box? N/A
Votes: 0 (A keeper?)

Posted on Tuesday, February 2, 2010 - 1:15 pm:

Geoffrey, that's an interesting question.

Forums powered by Discus Professional - http://www.discusware.com/.
Original site and logo design is by Andy Markley - art101.com.

Fair use exemption to the copyright is claimed as this material is to be used for public discussion before a legislative body
John Washburn April 8, 2010