

IN THE SUPERIOR COURT OF FULTON COUNTY
STATE OF GEORGIA

GARLAND FAVORITO, MARK SAWYER,))
RICARDO DAVIS, AL HERMAN,))
FRIEDA SMITH, KATHRYN WEITZEL,))
ADAM SHAPIRO, and CATHIE))
CALABRO,))
))
Plaintiffs,))
))
vs.) CIVIL ACTION FILE
) 2006CV119719
CATHY COX, Secretary of State,))
SONNY PERDUE, Governor of the))
State of Georgia, GEORGIA))
STATE ELECTION BOARD,))
))
Defendants.))

DEPOSITION OF
BRITAIN J. WILLIAMS, III

Taken on behalf of the Plaintiffs
Tuesday, July 31, 2007
10:30 a.m.

At the office of the
Center for Election Systems
Kennesaw State University
Kennesaw, Georgia

Sharon J. Ruschell, RMR, CRR, CCR No. B-1179
Certified Court Reporter

SHARON J. RUSCHELL, RMR, CRR
CERTIFIED COURT REPORTER
803 ROCKY RIDGE COURT
CANTON, GEORGIA 30114
(770) 704-5445

APPEARANCES OF COUNSEL:

On behalf of the Plaintiffs:

WALKER CHANDLER, ESQ.
15 West Jackson Street
P.O. Box 7
Zebulon, Georgia 30295
(770) 567-3882

On behalf of the Defendants:

STEFAN RITTER, ESQ.
Office of the Attorney General
40 Capitol Square, SW
Atlanta, Georgia 30334
(404) 656-7298
(404) 657-9932 (fax)

Also Present:

GARLAND FAVORITO
MARK SAWYER

- - -

INDEX TO EXHIBITS

EXHIBIT	DESCRIPTION	PAGE
A	E-mail from Garland Favorito to Dr. Williams dated 2-7-02 re Electronic Voting Machine External Audit Trails.....	30
B	E-mail from Brit Williams to Georgia Vine dated 2-19-02 re Conspiracy Theorist.....	30
C	E-mail from Garland Favorito to Brit Williams dated 3-31-02 re Professor Brit Williams (about the letter you wrote).....	30
D	E-mail from Brit Williams to Garland Favorito dated 4-2-02 re Professor Brit Williams (about the letter you wrote).....	30
E	The Georgia Vine newsletter.....	33
H	Letter to Robert Urosevich from Robert Ray dated 12-3-02 re Rough Draft Punch List with attachment; Letter to Robert Urosevich from Cathy Cox dated 12-2-02.....	58
I	Risk Levels of Identified Risks.....	61
J	Picture of mother board.....	79
K	Discussion Draft.....	71

P R O C E E D I N G S

- - -

MR. CHANDLER: This is the deposition of Britain Williams, being taken for use in the Superior Court Fulton County case of Garland Favorito, et al. versus Cathy Cox, the Secretary of State, and it's going to be taken for the purposes of discovery, use at trial and any other purposes allowed by the Civil Practice Act.

I presume that we will reserve all objections except as to the form of the question and the responsiveness of the answer and y'all will reserve the right to read and sign.

MR. RITTER: That is all correct.

MR. CHANDLER: Can you think of any other stipulations that I haven't remembered from our rote?

MR. RITTER: I think you've covered the standard stipulations, Walker.

(Discussion held off the record.)

- - -

BRITAIN J. WILLIAMS, III,

having been first duly sworn, was examined and testified as follows:

EXAMINATION

BY MR. CHANDLER:

Q. Please state your name for the record.

A. Britain Joel Williams, III.

Q. By whom are you employed?

A. I'm retired.

Q. Who was the last -- who was your last employer?

A. Okay. I have contracts right now with the university and with the Election Systems Commission.

Q. When were those contracts first entered into by you?

A. The current contract or the history of it?

Q. Just a quick history of it's all.

A. I have been working with the Secretary of State's office through the universities I was associated with, first Georgia Tech and then Kennesaw since the 1980's. I've been working with the Election Assistance Commission for a little over a year -- I'm sorry -- a little less than a year actually.

Q. Can you tell me briefly how you came to be involved under a direct contract to the State of Georgia say around 1998? Were you already under a contract with them at that time?

A. This contract has been renewed every year.

Q. Do you have a current title? Are you the sole

owner of your company?

A. I don't have a company.

Q. You don't have a company.

A. No.

Q. The contract is with you personally.

A. Right.

Q. Tell me what your academic background is.

A. Well, I have a Ph.D. in mathematics from the University of Georgia that was granted in 1964.

Q. Do you have special credentials as a computer scientist, computer expert?

A. I don't use the word expert to describe myself in anything. I've been working with computers since 1957. In 1964 there were no degrees in computer science but everybody of my vintage that works in computers is a chemist or a mathematician or a musician or something else.

And I have been on the faculty at the University of Georgia in the department of computer science and I was associate director of the computer center at the University of Georgia. I was director of computing activities at Georgia Tech.

Q. When you were under contract during the evaluation of what voting machines should be acquired for the State of Georgia to whom did you report?

A. There's a payroll reporting and then there's a

functional reporting.

Q. A functional reporting, yes.

A. From a payroll point of view, I worked for Kennesaw State University for the computer science department of Kennesaw State and therefore, my supervisor, so to speak, was the department chair. Functionally I reported to the election director of the State of Georgia.

Q. And the election director being a person under the Secretary of State.

A. That's correct.

Q. Were you familiar with the -- during the evaluation of what machines should or could be acquired to carry out voting processes in Georgia during the late 90's and early 2000's were you familiar with the federal and state certification requirements?

A. Yes.

Q. Did the federal government publish a list of certification requirements that you had to be familiar with?

A. There was at that time a voting system standard that was published by the federal government that was developed by the Federal Election Commission and is referred to as the 2002 standard.

Q. 2002 standard. Okay. Were you involved with the National Association of State Election Directors?

A. Indirectly, yes. I was not a member of that

organization because of the name State Election Directors but I served on their voting systems board.

Q. All right. Please identify any voting machine testing or certification guidelines that you wrote or helped to write for the NASED, which is the National Association of State Election Directors.

A. NASED does not have voting systems guidelines. The guidelines were produced by the Federal Election Commission.

Q. Are there any computer programming languages in which you have proficiency?

A. Historically, yes, but I haven't worked as a programmer in a long, long time.

Q. And I understand that now all the Basic and COBOL and stuff is in the past, ancient history. Are you familiar with the actual operating systems that are used in the voting machines that the State of Georgia is using currently?

A. Not at a detail level but if you want me to name them, yes. Like I say, I've been retired for five years and I have not worked as a technician for a number of years before that.

Q. What I'm wondering is do you have the capacity to oversee the work of technicians in the languages that are currently being employed by the current voting machines here

in Georgia.

A. Do you mean that from a managerial and supervisory point of view?

Q. No, sir; I mean that from a computer scientist point of view.

A. Then I'm not sure I know what you mean by oversee their work.

Q. And that's a point here is I don't intend to ask tricky questions and I can myself as a nonexpert ask confusing questions. What I'm trying to say is do you have yourself the computer scientist capacity to double-check the work of computer programmers.

A. From a managerial overview point of view, yes; from a pure technical point of view, no.

Q. Now, when you say a managerial point, what do you mean by a managerial point?

A. I have been involved with computers, as I've told you, for a long, long time and I have managed the development of lots of projects of various sizes and so from that point of view I know what has to be done to organize and manage and bring a computer system to fruition.

Q. I was wondering more about your capacity to detect, for example, inserted Trojans or other code which could operate to defraud computer systems.

A. No, I do not consider myself that technically

competent anymore.

Q. Are there people that have that sort of technical competence here at Kennesaw?

A. I don't know. I mean, you're asking me staffing questions that should be directed to the department chair.

Q. What I'm wondering, not so much the department chair but in this office of election systems are there technicians who can read code and find inserted malicious code?

A. Well, again, I'm not an employee of this center either but we have here people with technical backgrounds and I would assume they have that technical capability.

Q. What is your current role relative to the election systems of the State of Georgia maybe by definition in your contract and what you actually really do?

A. I oversee and direct certification of voting systems for the Secretary of State's office.

Q. And how long have you done that, been doing that?

A. Since 1988 with a few gaps in there but basically continued since 1988.

Q. Did you have any role in creating the RFP, the request for proposal that was sent out to the vendors, the various vendors of election system machines?

A. No.

MR. RITTER: Do you want to specify the

date we're talking about here?

BY MR. RITTER:

Q. 2002.

A. No.

Q. Who came up with that request for proposal?

A. That procurement was managed by the Georgia Technical Authority. What's the official name of them, Stefan?

MR. RITTER: GTA, Georgia Technology

Authority.

BY MR. CHANDLER:

Q. Do you remember when that proposal was issued?

A. No.

Q. Have you received any consulting fees or other funds from any source during the last say six or seven years?

A. I just told you I received consulting fees from the Kennesaw State University and the Election Assistance Commission.

Q. Have you received consulting fees from any private outside sources?

A. No.

Q. So this has been basically your -- other than any investments and things like that you have, this is your sole source.

A. That's right.

Q. All right. Do you invest in any technology stocks?

A. Not directly. I have mutual funds that may invest in technology stocks but none directly.

Q. Did you have any role in selecting the technology 2001 pilot project?

A. No.

Q. Do you remember what qualification criterion voting machines had to meet to participate in that pilot project?

A. In the pilot project?

Q. Yes, sir.

A. Yeah. They had to produce a paper receipt, some sort of something called VVPAT, voter verifiable paper audit trail.

Q. Were the machines required in that pilot project -- was this to be a piece of paper that was produced at the time the person voted?

A. Yes.

Q. And was the plan -- would the idea be that those pieces of paper that were produced could be stuck in a ballot box or something for later accumulation and correction?

A. They were accumulated in a roll on the machine

itself and then taken off at the end of the day.

Q. Were they printed at the time of voting?

A. The receipt was printed when the voter cast their ballot.

Q. And then it was rolled conventionally; is that correct?

A. That's correct.

Q. Were there any concerns about the privacy of the ballot because of the sequential nature of the voting on that roll?

A. Yes.

Q. Did that lead later to an idea that such paper ballots should be cut off separately?

A. Oh, you mean as opposed to --

Q. As opposed to sequentially on a rollup.

A. I don't know what you mean by lead to that but that is the other type of paper technology. There are two. One is the sequential roll and the other is what they call cut sheet technology.

Q. And of the vendors that had voting equipment available in 2001 and 2002, do you recall those that had the cut sheet or the individual --

A. In 2001 and 2002?

Q. Yes, sir.

A. I only recall one.

Q. And which system was that?

A. Avante.

Q. Did Avante participate in the pilot project in the 2001 pilot project?

A. 2001?

Q. Was there a 2001 project?

A. Not that I'm aware of.

Q. Did Avante ever participate in any pilot project?

A. They bid on the original purchase.

Q. Do you know why their bid was not accepted?

A. No, I don't. I was not on the procurement committee.

Q. Who was on that committee, to your knowledge? I mean, I understand you might not have a comprehensive list in your mind of who was on that committee.

A. Since I wasn't on the committee I'm not real sure. I attended at their invitation one or two of their meetings and I remember some of the people that were in the room but I don't have a direct knowledge of who was and who was not on the committee.

Q. All right. Was Secretary of State Cox on that committee?

A. I would assume so but again, I don't know.

Q. Do you know what the official name of that committee was?

A. The procurement committee?

Q. Yes.

A. No, I don't.

Q. Can you explain your role in the evaluation of the machines that were purchased in 2002?

A. That were considered for purchase?

Q. Yes, sir. What was your role in the whole process?

A. As I said earlier, I do certification evaluations for the Secretary of State's office and in order to bid on that procurement a system had to have state certification and so I did the certification evaluation of the seven systems that bid on that procurement.

Q. And what aspects of that certification or evaluation were you responsible for, all of it basically?

A. No. By law the Secretary of State certifies equipment, voting systems. My role was to evaluate the system for compliance with the federal standards, compliance with the code of Georgia and usability.

Q. I see.

A. And then I wrote a report to the Secretary of State and then the Secretary of State, based on that report plus whatever else she knew about the company, made the decision as to whether or not to certify the system.

Q. What systems -- do you recall which systems passed

your evaluations and were therefore considered by the State of Georgia?

A. That were allowed to bid?

Q. Yes, sir. I believe the question was which systems passed your evaluation.

A. I'm trying to list them here. I've got -- there was Avante, which we just mentioned, Global, which at that time was Global Election Systems, which during the process of the procurement was purchased by Diebold and is known now as the Diebold voting system, the Hart InterCivic voting system, the Sequoia voting system, the Election Systems & Software voting systems, ES&S. It seems there were two more. I seem to recall there were seven systems that bid but I don't remember the other two.

Q. All right. Now, do you remember which -- did you prioritize those systems?

A. No.

Q. You merely said which ones --

A. I'm just saying that they comply with the FEC standards, with the Georgia code and that they're reasonably usable to the point that we think we can install them in Georgia.

Q. Now, of those systems, which ones had a VVPAT, a paper audit trail?

A. I don't think any of them except Avante at that

time.

Q. Did not the certification requirements of Georgia code require essentially a paper audit?

A. No. The Georgia code doesn't and neither did the federal standards at that time.

Q. But your remembrance, only the Avante actually produced one.

A. Yeah, and I'm not real sure about that. I know they do now. They're the only one, I think, that produces a cut sheet code and I believe they were the only one in that procurement.

MR. RITTER: I just want to make clear --

MR. CHANDLER: If you want to make it a clear question, that would be fine.

MR. RITTER: I just don't understand whether -- is it your testimony that they did then or you're not sure whether they did then?

THE WITNESS: I'm not sure whether they did then. I'm not sure at what point in time they put that paper receipt on their system. I know they were one of the first systems to have one but I'm not sure -- I don't remember if the one they bid had it.

MR. RITTER: Thank you for letting me clarify.

MR. CHANDLER: Sure.

BY MR. CHANDLER:

Q. Regardless of the certifications, did the question of having a paper audit trail concern you personally?

A. No.

Q. Why didn't they?

A. Because, like I say, we evaluate those machines. They go through extensive testing and we didn't feel at that time that a paper receipt was at all necessary.

Q. Okay. Were you familiar with the bid prices that came down as a part of that evaluation?

A. No.

Q. Were you never aware of what the bids were?

A. No, not prices.

Q. You said that one of the other issues besides certification compliance was usability?

A. Right.

Q. And did all of these systems, these I believe you said seven systems all together meet the usability criteria?

A. Yeah. That's subjective. That's not something that you can measure hard, but basically what we're looking there is do we think this system is easy enough to use that it can be installed and operated within Georgia precincts.

Q. What about hackability; in other words, the ability let's say of people in the voting booth to tamper

with the machine?

A. That's one of the things you look at but hackability is a product of not just the machine itself but also the procedures under which you implement the machine.

Q. And also the machines at the end of the day are essentially combined into server systems to download their information, are they not?

A. Yes.

Q. I was thinking about there are different levels of hackability, if that's my word, and one of them is a person in the booth itself using one of the authorization cards -- I mean under the Diebold system -- and then, of course, the other somehow hacking into the accumulation system and counting system. Were there any concerns with any of these systems about in the booth hackability of any systems?

A. Oh, sure, there are concerns. I mean, you know, you look at the construction of the machine. You look at whether or not there's doors, how hard it is to get to the cards, how hard it would be -- how difficult it would be for someone in a voting booth to get a card out and put it back in without you noticing it, and you use that information then to design the procedures that you put around it to compensate for the things that you think are vulnerabilities.

Q. Was any consideration given to the standards

published by the FEC in April 2002 prior to purchasing the machines on May 3 of 2002?

A. Okay. Those seven systems all had to comply with the FEC 2002 standards.

Q. I'm just going to go back for a second. When did you first enter into a direct contract with the State of Georgia to do the work, the type of work that you do?

A. I started doing this in 1988. I was at Georgia Tech at the time. And when we first started doing this this was all -- let me give you a little bit of the history. Okay? We're talking about this abstractly and it doesn't make sense without the history.

When the FEC was directed by Congress to develop voting system standards Max Cleland was Secretary of State. Max was on the FEC advisory committee and Max thought that this was something that had potential impact and he wanted somebody from Georgia involved.

So he called out at Georgia Tech and called the head of GTRI, Georgia Tech Research Institute, and asked if they had somebody that could go up to Washington and go to one of these meetings and decide what we needed to do. Somehow that wound up on my desk. That was in 1988.

And since then I have worked with the Secretary of State's office in this area of certification of voting machines. I was on the committee or part of the committee

that wrote the original FEC standards that were published in 1990. I was on that committee again in 2002.

I was on the IEEE committee that was working on voting system standards and I'm now on the technical guidelines development committee that's created by HAVA legislation that is charged with developing guidelines for voting systems. So I've been involved with the development of voting system standards from the get-go.

Now, initially when I was working with the Secretary of State's office we did this on a contract basis. If a vendor brought in a system and they want it certified, then the vendor paid all the cost of certification and we charged the GTRI going rates.

That was difficult financially because some systems were simple and some were not and so forth and so on, and so at some point in there, and I could go back and find out when, but at some point in there it was suggested to me that rather than bill this thing up and down on an hourly basis that they just contract with the university for a hunk of my time and then if I put more in it this week and less next week, so be it.

So since then it's been just a constant contract at a fixed dollar amount and then I provide whatever services are necessary. Sometimes it's a lot; sometimes it's not so much, but over time it kind of tends to average

out.

Q. Did you write the report for or directed to the Secretary of State that evaluated the machines that were piloted?

A. Yes, all seven of them. That's what I just said. We did the certification reports on them, and basically what our report says is that they comply with the federal standards; they comply with the Georgia Election Code; and we think that they're reasonably usable to the point that we recommended consideration.

Q. Do you know where we can get a copy of that report? Excuse me. We'll go off the record for a second.

(Discussion held off the record.)

Q. Did you participate in writing Secretary of State department and election division policies about how the machines are to be used out in the polling places?

A. No, not directly.

Q. Or any of the policy directives of how machines are to be stored and things of that nature?

A. I've participated in a lot of conversations about that and I've participated in a lot of conversations here in the center when we were developing training materials and so forth about that but I've never actually written.

Q. Did you help write -- I believe you helped write certification policies, did you not, like during the 90's

and all leading up to this?

A. Yeah -- not for the Secretary of State but I was on the -- as I told you, I was on the FEC committee that wrote the FEC standards and I'm currently on the EAC committee that's developing EAC standards.

Q. And when were the policies that resulted in the eventual selection of the machines we use now, when were those policies created, those certification policies created; in what year?

A. These reports?

Q. The SOS certification policies. In other words, you ended up certifying seven machines.

A. I didn't. I don't certify machines. I evaluate machines. I wrote a report to the Secretary of State and the Secretary of State certifies the machine.

Q. Were you on the committee that developed the certification issues -- I mean the certification standards?

A. Well, there was no committee. My report is whether or not the machine complies with federal standards and state law.

Q. Is there something called rules of the Secretary of State?

A. Yes, there are rules of the Secretary of State.

Q. Did you help develop those?

A. I drafted -- I'm not sure I know what the current

ones are, but at one time I drafted proposed rules of the Secretary of State. I don't know the outcome of that.

MR. RITTER: For clarity, are we talking about rules and regulations of the Secretary of State or the State Election Board or both? Two different entities.

MR. FAVORITO: Secretary of State certification policy.

MR. RITTER: Well, let's be on the record just so we're clear for the purpose of the questions. Walker, I'm happy to have him answer but I just wanted to make sure that we're clear whether Dr. Williams is talking about regulations of the Secretary of State, regulations of the State Election Board or both.

MR. CHANDLER: Rules of the Secretary of State is, I think, the formal title.

THE WITNESS: Like I said, I at one time drafted some recommendations. If you would get me a copy of the current rules, I'll tell you whether or not they're the ones I helped draft.

BY MR. CHANDLER:

Q. Did you participate in writing the document that was called Electronic Voting Myth Versus Fact that was published by the Secretary of State's office? Are you

familiar with that?

A. I'm not sure I know what you're talking about.
There was a document out of Maryland with that title.

Q. Okay. Did you ever discuss audit capabilities of any of the piloted or purchased voting machines with representatives of Diebold?

A. No.

Q. Did you discuss the audit capabilities of any of the Diebold machines with Secretary of State Cox?

A. By audit trail what do you mean?

Q. The ability to produce a paper record.

A. Are we talking about just paper record?

Q. A paper record.

A. No. When we use the word audit trails we're talking about internal electronic time dated records of activities.

Q. But you did discuss those type of electronic audit trail capacities with Secretary of State Cox?

A. I don't recall ever discussing it with her.
That's a technical level of detail that she generally wouldn't be interested in, I wouldn't think.

Q. When the purchase or the entry into a contract with Diebold was close did you have any personal meetings with Secretary of State Cox to discuss the actual Diebold machines themselves?

A. I don't recall.

Q. Did you ever have any discussions about the audit trail and recount capacities of Diebold machines with any legislators prior to the selection of Diebold as the voting system that would be used?

A. I don't recall that either. Now, that commission that was formed that got referred to as the 21st Century Voting Commission or whatever it was, they did a lot of traveling around, talking to other jurisdictions and looking at voting systems and what have you and that's the group that came back with recommendations for an electronic voting system.

Q. Do you know why it did not contain -- that commission's final RFP did not contain a recommendation stating that the chosen system should have the capability to produce an independent paper audit trail of every ballot cast?

A. Do I know why they didn't recommend that?

Q. Yes.

A. No, I don't.

Q. Were you a party or a member of any commission that recommended dropping paper audit trails?

A. No.

Q. Do you remember whether or not the TrueVote system had an ability to produce paper audit trails?

A. Who makes that? That may be one of those two I can't recall.

Q. But you do remember that Avante produced them.

A. Uh-huh (affirmative).

Q. And you agree that the machines that we actually used -- ended up purchasing here in Georgia do not have the capability to produce an independent audit trail of each vote cast.

A. Paper audit trail?

Q. Yeah.

A. No.

Q. Independent of the machine. Do you agree with that, that they can't produce a paper audit trail?

A. Of each vote cast?

Q. Of each vote cast.

A. Yes.

Q. Now, there is a retrofit thing where they have this rollup system that was used in this recent pilot?

A. Yes, but that's not on our machine. That's an entirely separate machine.

Q. How is any audit trail independent from the vote recording equipment? Is there any independence of audit from the actual voting equipment?

A. I'm not sure I understand what you're trying to get at.

Q. What was the purpose of the 2006 audit trail pilot project?

A. I'm not sure I know what the purpose was. That was a product of the State Election Board and you'd need to ask them that question.

Q. Did you provide any assistance or evaluation help or what was your role?

A. Same as it is in everything. The machines that were proposed for use in that pilot project, I did the certification analysis of them.

Q. I believe there was a conclusory report at the end of the project; was there not?

A. I believe that's correct.

Q. Were you not a participant in that?

A. No.

Q. What group made those conclusions?

A. I don't know.

Q. Did you provide any advice to the Secretary of State or the Director of Elections concerning which machines should be used in the 2006 pilot project?

A. There wasn't a decision to be made there. There was only one machine that would integrate into our existing system that would produce those paper receipts.

Q. And that was a machine provided by Diebold.

A. That's correct.

(Discussion held off the record.)

(Brief recess.)

Q. All right. We're back on the record. The 21st Century Commission in 2002, didn't they recommend that there should be an independent paper trail, audit trail of every ballot cast?

A. I don't know.

Q. During an off-the-record break we looked at something called Certification of Voting Systems, which would be, I guess, Rule 590-8-1-.01. Did you have anything to do with the promulgation of those rules?

A. I did not write that document.

Q. I'm going to ask you if you agree with a definition or if we can establish a common definition here. An audit trail definition would be a record showing what operations a computer or computer user has performed in a specific period of time. Would you agree that that's --

A. We can use that as a definition of an audit trail.

MR. RITTER: Could you read that again?

MR. CHANDLER: It's a record showing what operations a computer or computer user has performed in a specific period of time.

MR. RITTER: Okay.

BY MR. CHANDLER:

Q. Now, it's my understanding that the machines that

we currently use are considered to have an audit trail because of electronic capacities to store information. Is this correct?

A. As a general statement, yes.

Q. So if the science department or whoever's checking on the machines wants to evaluate whether a machine recorded votes properly, they would be relying on electronic information stored in the machine, not printed on a piece of paper. Is this correct?

A. That's correct.

Q. I would like for you to look at some e-mails, some prints of e-mails considered Exhibit A, B and C that have your name on them and ask if you recognize those.

A. I don't recognize A. I recognize B and C and D.

Q. Do you recall back in 2002 having e-mail contact with Garland Favorito?

A. Yeah. I just told you I recognize two of these, B and C and D -- three of them.

Q. Do you recall Mr. Favorito expressing concerns about the lack of external audit trails for the voting machines that were under evaluation?

A. I don't recall him specifically but I recall several people, a lot of people that did and I suppose he was one of them.

Q. I believe that you've already testified that there

was only one machine that had an external trail at that time.

A. To the best of my memory, yes.

Q. That was the AccuVote?

A. Avante.

Q. Avante. Excuse me. Do you recall Exhibit B?

Does that appear to be an e-mail in which you were involved?

A. Yeah.

Q. In that did you liken Mr. Favorito to a conspiracy theorist or call him one?

A. I sure did. At that time we were getting hit from all directions by people that basically didn't know what they were talking about and we were spending an enormous amount of time answering more or less frivolous complaints, and I subsequently apologized to him for that too.

MR. RITTER: Let me stop and ask a question. I want to allow any discovery that could lead to admissible evidence but I'm not sure how characterizing Mr. Favorito one way or the other is relevant. How is it relevant?

MR. CHANDLER: I think that it goes to the issue of the concern of the plaintiffs prior to the selection of the machines about the lack of an external audit capacity and the notice that was being given to the State of Georgia by the

plaintiffs or some of the plaintiffs that the machines under evaluation did not adequately protect the voting interests and the legal interests of the citizens of Georgia and so it goes to -- it would go to prior warning.

MR. RITTER: I hear what you're saying. I'm not sure that prior warning's relevant.

MR. CHANDLER: I understand that.

MR. RITTER: And I don't want to stop your conducting discovery on that. This is what I'm concerned about happening here is that it's really an attack on my witness, Mr. Williams, as supposedly defaming Mr. Favorito.

I think that Mr. Williams made it clear that he wasn't going to defame Mr. Favorito, wasn't trying to call him names. That is not our purpose. We're just defending this case.

So if we have questions that are about what happened, what was Mr. Williams thinking, so forth, I can understand that. Certainly in the broad scope of discovery I'm not going to object to that simply because it's discovery, but I want to avoid things that are going to be derogatory of anybody and so I would just ask us to focus our questions in that regard.

MR. CHANDLER: I think we're going to be --
we're not going to follow through with that
other than the issue of notice, and we accept
Mr. Williams' apology on that.

BY MR. CHANDLER:

Q. However, did you ever send any kind of a written
retraction to the Georgia Vine people?

A. I didn't send that to Georgia Vine. I sent it to
Judge Van Horn. It was between me and Mr. Favorito and I
apologized to him.

Q. Are you familiar with what the Georgia Vine is?

A. Vaguely. I've seen one or two of them. It's not
something I read.

Q. What are they?

A. I don't know. I see it every now and then.

Q. Is it like an electronic newsletter?

A. It seems to be, yeah.

Q. Did the Georgia Vine publish the letter that you
wrote to Judge Van Horn?

A. I don't know. I don't read that.

Q. Are you generally familiar with voting machine
reports that are issued in the United States in the last say
six or seven years concerning the voting systems?

A. Could you be more specific about voting machine
reports?

Q. Are you familiar with the following reports, the Princeton University Security Analysis of Diebold AccuVote-TS Voting Machine Report of September 13, 2006?

A. Yes.

Q. Do you agree with the analysis and the issues that were raised in that report?

A. Within a context.

Q. What is that context?

A. That is a report of something that some university professors and their students did in a laboratory. I have no problems with what they said they did in a laboratory. They conjecture that that same thing could be done in an election environment. I have a lot of problems with that.

Q. Johns Hopkins University had a thing called Analysis of an Electronic Voting System in February 27th of '04. Are you familiar with that report?

A. Is that the one written by Avi Rubin?

Q. Yes, sir.

A. Are you talking about the one published in the New York Times?

Q. I don't know if it's published there, sir, but it's a Johns Hopkins report by Mr. Rubin.

A. I think I'm familiar with the one you're talking about, yes.

Q. Do you have any issues with what was done in that

case, how it was done?

A. The same.

Q. When you say in a laboratory setting as opposed to the voting booth setting, are you saying that in the laboratory system they had a much lower scale of security that was involved?

A. Well, in Mr. Rubin's case he didn't even have an actual voting machine. He took the software and loaded it on a laptop computer and proceeded to work with it from there and based on that he made a lot of assumptions about election administration and all that just weren't true.

For example, in his report he says that he thinks it's so easy to fabricate a voter card that he thinks his janitor could do it, a completely asinine statement that even he himself later retracted.

Q. The California Secretary of State staff report called Investigation of Diebold Election Systems, Inc., April 20, 2004, are you familiar with that?

A. I don't recall that one offhand. Now, I probably did read it because all of these things that come out, we immediately get 15 copies of them from all of our friends and so I'm sure I read it but I don't recall it from that name.

Q. Did you read the Decertification and Withdrawal of Approval from the Secretary of State's office of California?

A. When was that?

Q. April 30th of 2004.

A. What was that title again?

Q. Decertification and Withdrawal of Approval.

A. I don't know if I read the actual report but I'm familiar with the contents of it.

Q. Do you know why they conducted some sort of a decertification? Are you familiar with that?

A. You know, I'd rather not do this from memory. I think I know but I'm not sure. There was an incident where the Diebold Corporation loaded some firmware in California that they had not previously certified.

Q. I see.

A. And I believe that's the basis of that report but I'm not sure.

Q. Are you familiar with the Ohio Secretary of State's DRE Technical Security Assessment Report of November of 2003?

A. No.

Q. How about the Maryland Legislative Services Trusted Agent Report of January 2004?

A. Who wrote that?

MR. FAVORITO: That was RABA Technologies.

THE WITNESS: Yes, I'm familiar with that and I'm also familiar with the other one, the

study that preceded that.

BY MR. CHANDLER:

Q. SAIC Risk Assessment Report?

A. Yes.

Q. How did those reports -- how do you think those relate to what we have here in Georgia now?

A. The RABA, not very much; the SAIC has a direct relationship.

Q. In what regard?

A. The SAIC, what they did, they took -- and you have Rubin's report, which had something like 67 or 68 separate things that he considered vulnerabilities in the Diebold system.

They went through them point by point by point by point and analyzed them as to whether they felt they were true vulnerabilities or not in an election environment. They came out with four recommendations. Diebold implemented those four recommendations into their system and that's the current system we run.

Q. Are you familiar with a Nevada Electronic Services Division Diebold Voting System Security Report?

A. No.

Q. Or any Nevada reports or problems that they might have had?

A. I wasn't even aware Nevada ran Diebold voting

systems. I thought Nevada had Sequoia systems.

Q. Are you familiar with the University of California Security Analysis of the Diebold AccuBasic Interpreter Report of 2006?

A. Say that again.

Q. The University of California Security Analysis of the Diebold AccuBasic Interpreter.

A. I can't recall it.

Q. You agree that all of those that you have recalled and we have discussed just now have to do with the Diebold AccuVote-TS system.

A. Uh-huh (affirmative).

Q. And some of the reports identified security risks in vote results manipulation for the Diebold AccuVote-TS system. Now, don't you think that the vulnerabilities that these reports talk about could be ameliorated, if that's the right word, with external audit trails, that is to say with a concurrently produced paper ballot?

A. I don't know if I would go that far or not. Let me give you my personal feeling on the reliability of these paper audit trails. Okay?

Q. All right, sir.

A. From a technical point of view they're not necessary. We have established in many industries and in many situations the reliability and accuracy of electronic

systems. So from a technical point of view they're not necessary.

But having said that, it's extremely important in this country to maintain the voters' confidence in the election system and if that's what we've got to do to maintain the voters' confidence, to calm these waters of all these people that are raising all these issues, then that's what we need to do.

Q. All right, sir. I think that's very good. With regard to that, don't you think that's exactly what Mr. Favorito was trying to talk about back in 2002 when he was trying to have input prior to the adoption of a system?

A. That was his conclusion but his premise was wrong. He was basing it on a lot of vulnerabilities and things that just aren't there.

Q. Well, speaking of vulnerabilities, correct me if I'm wrong but one of the issues of voter confidence is, is it not, that the government itself could let's say monkey with the system and that people at the local precinct level would be deprived of the ability to know whether or not the machines were reporting accurately?

A. That's a frightening thought, that our government would deliberately subvert its own election process. If that happens, we've got a lot bigger problem than elections.

Q. Yes, sir, but you would agree that that is a

possibility.

A. Possibility, yes; probability, no.

Q. Yes, sir, under our current administration.

A. I'm not going to touch that.

Q. But you would agree, however, that under a system that produces an independent audit trail of every vote cast at the local precinct level during, for example, a recount those paper audits could be manually counted; is that correct?

A. Yes, sir. I also believe that anybody that's clever enough to subvert the system like that is clever enough to print those paper receipts any way they want them.

Q. If a machine prints a paper receipt, the voter can verify at the time before he puts it into a ballot box. Are you saying that that too could be subverted by, for example, a state government in Atlanta?

A. Not if the voters did, in fact, verify those receipts, but study after study has demonstrated that they don't, that less than 10 percent of the voters will actually verify their ballots.

And in fact, Ted Selker at MIT in a controlled study where he gave people a script to vote and he deliberately rigged the machine so that the printed receipt was wrong and only something like 10 or 15 percent of the people discovered that error.

So the paper receipt has its appeal but it's not foolproof. If it's being offered as a foolproof solution to the problem, it's not.

Q. I understand. Have there been -- can you name any independent study that upholds the accuracy of vote recording and tabulations of the Diebold machines purchased by Georgia?

A. We run accuracy audits after every election. We do parallel testing. We establish the accuracy of that machine during every single election.

Q. Does anybody else do that? Does anybody else --

A. I don't know. We're only responsible for Georgia.

Q. But you don't know of any independent study that upholds it independent of the state -- this group right here.

A. No, but I'm also not aware, including these studies you just mentioned, of any study that's challenging the accuracy of the machine. What they're saying is that the machines are vulnerable but I haven't seen a report yet that actually challenged the accuracy of the machine.

Q. I see. What's the difference between the terms blank voted and under voted as they're used on voting machine tally tapes?

A. A blank vote is a completely blank ballot, one that is not voted at all. An under voted ballot is one in

which some of the races were not voted.

Q. Under voting is rather common, isn't it?

A. Yeah.

Q. A lot of people just don't have an opinion and therefore don't vote on those other ones.

A. Exactly. And the further you get down the ticket, the more prevalent under voting is.

Q. Do you know what the term residual vote rate is?

A. Uh-huh (affirmative). That's used to refer to the number of under votes on the top race on the ticket. In a presidential race that would be the vote for President. In an off year that might be a senatorial race.

Q. So like, for example, in a presidential race there should be -- we should expect that there would be very little -- very few ballots that didn't have a selection for President.

A. Yeah. That's something you can't study because you can't -- because of the secrecy of the ballot you can't really go in and verify how people voted and whether they did it on purpose or not. But we think from anecdotal evidence that the under vote rate on the top of the ticket would be typically somewhere around one, one and a half percent at most.

Q. Might that just be, for example, because of voter ignorance?

A. It could be from a number of things. It can be from a poorly designed ballot. It can result from a voting system that's difficult to use. It can result from people not realizing, not verifying that they're on the summary screen. There are a number of issues there.

But there are also people who just don't vote the top of the ticket. When you get into rural Georgia, for instance, the sheriff is more important to those people than the President of the United States.

Q. I understand. Can you explain how ballot images can be recreated from -- well, first, can you identify the file formats that the voting machines, memory cards and servers use to record all records of votes cast?

A. No.

Q. Can you explain how ballot images can be recreated from the files after the votes are recorded?

A. Yes. Once the votes are recorded and uploaded into the GEMS server you can go into there and produce images of individual ballots and you can even do it in a format that you can read back on the scanner.

Q. For example, could you say that on any given machine voter number 2 cast his votes in a certain way?

A. No. You cannot identify from that. Those ballots are completely random.

Q. You mean as people vote then they're thrown in in

a random fashion.

A. That's right. That file is randomized as people vote beginning with about the fifth voter. Obviously if you only have one or two or three people vote on a machine -- and I don't know the exact algorithm on this, but as people vote this file is constantly randomized.

Q. All right. Are you familiar with the Volusia County, Florida elections and any problems they might have had on the voting machines down there in the 2000 presidential election?

A. In the 2000 election?

Q. Yes.

A. What was the voting system in Volusia County?

Q. Diebold, I believe.

MR. RITTER: In 2000? Are you talking about the punch card debacle in Florida in 2000?

MR. CHANDLER: No.

BY MR. CHANDLER:

Q. Do you know about a 16,000 negative votes that recorded in Volusia County in Florida in the 2000 election?

A. No.

Q. If a voting system recorded a portion of one candidate's votes for his opponent during an election, how would that be detected after the polls were closed?

A. It wouldn't. That's something that's got to be

prevented before the election. The machine's got to be properly set up and monitored and the accuracy established before the election. That's independent of the voting system. That's true of any voting system.

Q. If a county election official shifted votes in a central tabulator on election night from one candidate to another in the same race, how could that manipulation be detected?

A. When you close the polls in a precinct one of the things you do is print the results of that precinct and post them on the wall. That puts the results of that precinct in the public domain right there.

Q. Is that printed at the precinct?

A. At the precinct.

Q. Right there?

A. Right then in public view with poll watchers watching and candidates watching and anybody that wants to watch it, and those results are posted right on the wall and put in the public domain.

If subsequent to that back at the election office results begin to come in that disagreed with those, it would be detected immediately.

Q. And how would that be detected?

A. By candidates because they've got people out there at those polls looking at what's posted and if results start

coming in that are different than what's posted, they're going to raise a flag on that.

You see, the results are posted on election night as they come into the central installation center sent up to the State. They're posted on the website by precincts. So if those results are out of kilter with what those candidates saw in the polling place, we'd know it immediately.

Q. Can you identify any time that an audit for recording accuracy has been conducted on machines after votes were actually cast in an election other than on that pilot project?

A. We do that after every election. We run what's called parallel tests during every election and at the end of those parallel tests -- and I believe Ray Cobb probably described this process to you so I won't go into the details of the process, but one of those things he'd do is go in and print those ballot images you're talking about and actually manually count them and see if they agreed with the electronic results.

Q. Can you identify any recanvass of electronic votes in Georgia that has produced an electronic vote count different from the original count?

A. No. There are two voting systems that will give you the exact same answer on a recount as they do on the

original count and that's an electronic voting system and a lever machine.

Q. Do you know who Sam Barber was, a person that had to do with the company ACT?

A. No.

Q. Do you know who a Jeffrey W. Dean, who was a software programmer and senior vice president of Global Election Systems? Do you know anything about him or who he was?

A. No.

Q. Do the Diebold voting machines or their servers allow negative votes?

A. No.

Q. Does the State of Georgia use any independent testing authorities for any of its computer systems that you know of?

A. We require that the systems prior to use in the state be certified by the independent testing authorities that are doing the certifications previously for NASED and now for the EAC.

Q. Do you know a company called Cyber, C-Y-B-E-R?

A. Uh-huh (affirmative).

Q. Where is that company based?

A. It's a very large company. They've got a big office right here in Atlanta.

Q. And a company called Wylie, W-Y-L-I-E?

A. Uh-huh (affirmative).

Q. Do they perform any testing functions for the State of Georgia?

A. They have in the past but not for the State of Georgia. They did testing functions for NASED. They tested systems for compliance with the FEC standards for NASED, which then became systems that were used in Georgia.

Q. Do you know if either of those companies have any kind of financial relationship or are they owned by Diebold or a parent company of Diebold?

A. I have no idea but I'm confident that they're not. Wylie is a large defense contractor that is located in Huntsville, Alabama, and an office in California that does analysis primarily for the Department of Defense and NASA.

Q. So what organizations provide the funding sources for Cyber, Wylie and any other independent testing authorities used by Georgia?

A. Again, this is federal. This is not Georgia. When a voting system submits a system for certification under the federal guidelines they pay for the testing.

Q. So for example, if Diebold pays for the testing of its own equipment by whatever group it is --

A. By these certified labs. Cyber incidently is no longer a certified lab. Wylie is and there are two or three

other labs that have since been certified.

Q. Do you remember prior to us entering -- us, the State of Georgia entering into a contract with Diebold, do you know what company certified, ran their certifications prior to y'all's reevaluation?

A. Yeah. Wylie did what's called a hardware analysis, the so-called shake-and-bake test, the high temperature, low temperature, that sort of thing, and Cyber did the software and the functional testing.

Q. And did you say Cyber was no longer qualified or whatever?

A. I don't know that they're no longer qualified. We're in a transition period from NASED to the EAC and the labs that were certified under NASED have to be recertified under the EAC, and I know that Cyber has applied for that but I don't think their application has been completed yet. It hadn't been denied but it hadn't been completed.

Q. Would you define what a penetration analysis is in terms of the Diebold machines?

A. I don't know if I've heard that term before.

Q. Do you know if there was a checklist of analysis or things that had to be gone through on the precertification analysis?

A. Certification at the federal level or the state level?

Q. Federal.

A. All I can do there is refer you to the federal standards and say that these labs test to those standards. Now, if what you're calling a penetration analysis is in those standards, then yes, it's done. If it's not, it probably isn't.

Q. So you don't remember whether or not a penetration analysis was done on the Diebold machine; is that correct?

A. That's right.

Q. Do you remember when you started the certification process for the voting machines that were used in the 2002 elections?

A. That would have been the original procurement so the certification of those would have taken place prior to that procurement.

Q. In '01 is when it started, say May of '01 or something like that?

A. Well, all I can say is it had to be prior to that procurement. I don't know the exact dates.

Q. You don't remember when you completed certification of the voting machines used in that.

A. No.

Q. What software versions were certified for use in the 2002 elections?

A. I don't recall.

Q. Have you written any reports about Diebold concerning vendor noncompliance in the last five years?

A. Noncompliance?

Q. Noncompliance with any of its contractual obligations.

A. For the state?

Q. Yes.

A. That would not be my responsibility.

Q. So you have not written any reports of that sort.

A. No.

Q. Can you explain why no records exist in the Secretary of State's office in regards to certifying the software used on election day in 2002 according to a March 25, 2003 response from Cliff Tatum of legal affairs to a Freedom of Information Act request? That's a long question. I'm sorry.

MR. RITTER: There may be a document you want to show us.

MR. CHANDLER: I'm sorry.

MR. FAVORITO: I have a reproduction of the document.

MR. CHANDLER: We'll be off the record for a second.

(Discussion held off the record.)

- - -

BY MR. CHANDLER:

Q. We're back on the record. Do you certify voting systems?

A. No.

Q. Were you part of the contractual process that the Secretary of State entered into with Diebold?

A. No.

Q. Or any amendments to any contracts?

A. No.

Q. Were you familiar with the federal and state certifications of Diebold by other authorities or are you only concerned about whether or not Diebold machines met those certifications relative to what Georgia --

A. Just Georgia.

Q. So for example, did the federal government independently certify voting machines that could be used under HAVA? Do you follow my question?

A. I'm not sure. HAVA's very recent, you know.

Q. That's after 2002. Was there ever -- anywhere in this whole selection process was there ever a federal mandate that said for federal elections the following systems -- any of the following systems can be adopted?

A. No. These voting system standards are entirely voluntary and, in fact, until HAVA came along only about 36 states adopted these standards. There were 14 states that

didn't adopt them.

Q. Do you know why those states didn't?

A. No idea. Well, in the case of Florida, Florida felt that their state certification process was more rigorous than the federal.

Q. Do you have any let's say computer scientist knowledge of the way that the software -- the technical ways the software in Diebold machines works or are you more result oriented?

A. I'm what you'd call more result oriented.

Q. If Georgia had implemented voting machines that produced a verifiable paper ballot which could be used for verifying the machine counts and recounts, would we have needed to have used any testing and certification process at all?

A. Oh, absolutely.

Q. And why?

A. Because there are multiple dimensions to a voting system. You start with accuracy, security, reliability, availability and go right on down -- well, maintainability and finally affordability.

So when you're looking at these systems you're looking at all of those, not just accuracy and security but you're looking at all of them. You're looking at maintainability. You're looking at reliability. You're

looking at availability. So the fact that it produces a paper record doesn't negate the importance of looking at all these different attributes.

Q. Can you explain why no state or federal certification confirmation existed for the Diebold machines on December 3rd, 2002, as indicated by the 29 point punch list sent by Robert Ray to Bob Urosevich?

MR. RITTER: Could you repeat that question?

BY MR. CHANDLER:

Q. Could you explain why no state or federal certification confirmation existed for the Diebold machines on December 3rd, 2002, as indicated by the 29 point punch list sent by Robert Ray to Bob Urosevich?

A. I'm not familiar with the punch list.

Q. Can you identify the names of the Diebold voting machine files that contain the four types of audit records described in the software requirements section of the 1990 voting system standards?

A. No.

Q. Approximately when were the voting machines delivered by Diebold, the mass of voting machines delivered by Diebold in 2002; what month, June, July?

A. I don't recall. The contract was signed roughly six months before the election so in that six months leading

up to November. In the last two months or so we were doing mostly acceptance testing so back off about three months and you're probably looking at the peak of the delivery.

Q. Were some patches, some software patches installed during that process before the election?

A. One.

Q. Do you know the name of that patch? Was it given a designation?

A. Not to my knowledge.

Q. Do you recall something of an 08-08 patch, which I believe would have been the August 8th patch?

A. Yeah; it's identified by the date, if that's what you mean, yeah.

Q. Is that the date of when it's applied to the machines?

A. I believe that's the date that appears on the operating system when you start up the machine, yeah.

Q. What was the purpose of that one patch that was installed?

A. When we were doing acceptance testing we were experiencing what we felt was an unsatisfactory level of what's called screen freezes. Now, the screen freeze is where you're voting on the machine -- and your laptop will do the same thing. All of a sudden the screen just locks up and none of the keys works; nothing happens.

Q. Yes, sir.

A. And we felt that the incident of this was unacceptable. Now, that was not an accuracy or any kind of a problem per se because you could reboot the machine and it would come right back up to where it was just like your personal computer and everything was fine so no votes were lost or anything like that. But that's not good psychology, to have voters all of a sudden standing there and the screen freeze.

So we looked into this and it turns out that it was caused by the operating system, not the Diebold software but by the Microsoft operating system, the way it updates its files, and it would get out of sync with the voting system and freeze the screen so a patch was developed for the operating system.

Q. By whom?

A. Diebold or their representatives. I think it's probably actually developed by Microsoft but came to us through Diebold, this patch that they said would fix it.

Now, at that point we were one month from the election. There was not time to go back through this federal certification program because that process takes time and we couldn't do it in a month.

So we brought the patch in here and examined it with our computer scientist and verified that yes, by golly,

it does cure these screen freezes and it has no impact on the voting system.

So we made the decision -- we made a command decision to implement that patch to solve that screen freeze problem on those machines.

Now, we examined it inhouse and we also got an unofficial reading from Cyber. We had our contact with Cyber look at it and give us his opinion, not official because we didn't have time to go through the official, but he agreed with us that yes, this did appear to solve the problem. It does not appear to impact the voting system negatively at all.

So based on all this input we installed the patch. We ran the election. We lived happily ever after. After the election we went back and went through the formal process to verify that it was okay, that we'd made the right decision.

Now, legally we were okay. We were on sound footing because if you'll read the Secretary of State's rules, the rules very clearly state that in the event that for whatever reason an ITA evaluation is not available by a certified lab that the Secretary of State can designate an organization to conduct those tests. They designated us. We conducted the test.

Q. Have there been any incidences of basically

machines in Georgia elections just simply failing and therefore any votes that were cast on that particular machine were just lost?

A. No. We've never lost a vote due to a machine failure.

Q. Can you explain why the State was unaware of the impact certification requirements and number of machines affected by the 08-08 patch as indicated by the same 12-3-02 punch list?

MR. RITTER: I object because the document's not in front of us and you're asking him about --

MR. FAVORITO: Here it is.

MR. RITTER: Well, let's mark it as an exhibit but in any regard, the way the question's phrased, it assumes that it's saying certain things.

The document's going to speak for itself. You know, if he has any knowledge about it, I'd be happy to have him testify about it, and I think maybe the first question we ought to ask is whether the witness has any knowledge about these documents. This is Exhibit H.

BY MR. CHANDLER:

Q. Do you have any knowledge of Exhibit H?

A. No.

Q. Are you familiar with Exhibit H?

A. Never seen it before.

Q. Do you know a Mr. Mark Radtke?

A. Yes.

Q. Who is Mark Radtke?

A. He's an executive with Diebold Corporation.

Q. Did Mark Radtke testify before the Election Assistance Commission?

A. I don't know. I'm sure he did. They've held a number of open hearings and invited a number of people including vendors to testify but I don't know personally whether he did or not.

Q. That patch was installed in the '02 election. Have other patches been installed since then?

A. No. That's the only time we got into a time crunch type of situation where we were not able to go through the full certification evaluations.

Q. Do you agree that patches can affect the efficiency of voting machines?

A. Patches can do most anything. That's why you test them.

Q. I believe you may have answered this before, but does state law allow a patch to be made to electronic voting machine operating systems without requiring certifications?

A. State law?

Q. Yes.

A. No.

Q. Are you familiar with a file that was used as a patch or some sort of an after-market addition called Rob-Georgia.zip?

A. Am I familiar with it?

Q. Yes.

A. No, I'm not familiar with the contents of that file.

Q. Are you familiar with any patches that Diebold did in the summer of '02?

A. No, other than the one we've talked about.

Q. Do you know what the purposes of the AccuBasic files used in the Diebold voting machines that Georgia has -- do you know what the purposes of those are?

A. No.

Q. You don't know any Rob-Georgia zip file that was a zip file of any kind that was installed by Diebold on the machines as a patch?

A. No.

Q. Do you know of any way that GEMS voting database of our Diebold machines can be altered using Microsoft Access, Notepad or a DOS command prompt without leaving any record of the alteration?

A. No.

Q. If such alterations could be done or were done, the equipment couldn't prevent manipulation of vote recordings; is that correct?

A. That's correct, but as we discussed earlier, any subsequent alteration of vote totals is going to be detected.

Q. I'll show you something marked Exhibit I and ask if you're at all familiar with that.

MR. RITTER: This is labeled part 2 and it looks like a page 52 of 115 pages. Do you have the whole report this relates to?

MR. FAVORITO: The State Election Board has that. They have all of those reports that we've referenced. I personally delivered them all.

MR. RITTER: I'll let him answer the questions the best he can but I'm just curious. I don't want to go hunting for this document. What's the name of the document?

MR. FAVORITO: This came from the Ohio --

MR. RITTER: Ohio Secretary of State?

MR. FAVORITO: DRE Technical Security Assessment Report from November 21, 2003. It's known as the Compuware report. We would contend that that is excerpted straight from that

report.

MR. RITTER: What's the question?

BY MR. CHANDLER:

Q. First the question is do you recognize Exhibit I.

A. No.

Q. How many pages long is this report?

A. 115.

MR. RITTER: Plus many exhibits and
whatever. This is labeled 115.

THE WITNESS: This is page 52 out of 115.

BY MR. CHANDLER:

Q. You're not familiar with this report?

A. I'm familiar with the CompuServe report in Ohio
but I don't recognize page 52.

Q. I see. Okay. So you do recognize the report. Do
you recall the physical testing evaluations that were done
as part of that test?

A. Not offhand.

Q. Do you remember that they suggest -- that that
report suggested that there was a risk that an unauthorized
person with access to the GEMS server could access the
database and change ballot definition files and election
results?

A. Yes.

Q. Do you think that that does not apply to the

Georgia machines that we have?

A. The key word there is unauthorized persons. We go to great extent to prevent unauthorized persons from gaining access to our servers.

Q. But by the same token, that means the people of Georgia have to trust their authorized persons; is that correct?

A. That's correct.

Q. Who hires and fires the authorized persons here in Georgia?

A. If you're talking about the GEMS -- access to the GEMS servers, you're talking about the county elections offices, the county election directors. That's where those GEMS servers are is in those county offices. And the State Election Board has a set of rules that they have to adhere to to ensure the physical security of those servers.

Q. All right.

MR. RITTER: Can I ask a question about I? I just want to know what's going on here. As I look at it on this printout there's two arrows at the bottom of I that are pointing upward with nothing written below them. Is there something that was redacted off of that?

MR. FAVORITO: No. The red arrows are to show the areas of concern that we wanted to ask

about. They were added to the report.

Nothing's been redacted, to my knowledge.

MR. RITTER: Were the red arrows added by you?

MR. FAVORITO: No, the red arrows were not added by me personally.

MR. CHANDLER: Who were they added by?

MR. FAVORITO: By wherever the report came from. I don't know the exact individual.

MR. CHANDLER: Do you want to go off the record here?

MR. RITTER: Sure. Why don't we go off the record.

(Discussion held off the record.)

BY MR. CHANDLER:

Q. Do you agree that it's possible that the software in Diebold machines could be altered using Microsoft Access, Notepad or a DOS command prompt without leaving any record of an alteration?

A. Read that again.

Q. Is it possible that a GEMS voting database used by our machines could be altered using Microsoft Access, Notepad or a DOS command prompt without leaving any record of that alteration?

A. I believe Access you could. I'm not sure about

Notepad or from a DOS command prompt but with Access you certainly could. It's possible.

Q. If the equipment -- how could the equipment prevent fraudulent manipulation of vote count recording and counting if it allows such alterations?

A. The equipment can't prevent it. This is one of those areas where you have to have external procedures to protect your equipment and that's the generic statement that applies to any voting system you're talking about. You have got to protect that system from unauthorized access or bad things are going to happen to you.

Q. Are you aware that Diebold machines have any hard coded passwords for administration access?

A. They did have. They do not anymore. That was one of the four recommendations of -- the SAIC report in Maryland recommended that those passwords be changed.

Q. Did they have them in 2002?

A. Yes.

Q. Did you consider it a security flaw also?

A. Yes.

Q. And that's why it has been changed.

MR. RITTER: Just for the record, maybe we want to explain what's meant. You said hard coded password?

MR. CHANDLER: Yes.

MR. RITTER: Let's explain what that means.

BY MR. CHANDLER:

Q. Will you explain what a hard coded password is?

A. Yeah. The Diebold touch screen uses a password as part of the security identification of a person authorized to do certain things on a machine. The password is a five-digit code or four -- I forget which -- but anyway, when the machine first came out that password was hard coded as 1111. It's since been changed so that you can and we do change them from election to election on a random basis. Now, with 159 counties I have to tell you that's an administrative nightmare but it is a security flaw that has been corrected.

Q. How are Diebold voting machines put into a test mode for logic and accuracy testing for certification?

A. There's two general modes on the machine, the voting station. One is what's called a test mode and the other is your general election mode and this is done with the administrator card and that password we were just talking about.

Q. Do you agree that a voting machine that we use could operate differently in a test mode than it would during a live election?

A. No; it uses the same software in test mode.

Q. Could it not have software altered to pretend that

it was working properly today and then in the actual election kick over to a different --

A. Again you're operating in the realm of possibility and, yes, that's theoretically possible.

Q. At the precinct level is there testing done at the machine right at the beginning of the election?

A. No. The testing's all done prior to the machine being delivered. What's done at the election, when you turn it on on the morning of election day the machine goes through some self-diagnostics like your laptop does when it boots up to be sure that internally it's healthy, and then it prints what's called a zero tape to show that there are no previous votes on the machine and then it goes into election mode.

Q. Again, this is just a realm of possibility and call me a conspiracy theorist if you would like to but couldn't the machine be -- couldn't the software in the machine basically report that the machine's all clear and ready to work but in fact the machine is ready to misrepresent the votes that are cast on it during the day?

A. If it had been altered to do that prior to 2002 and we hadn't caught it in all these five years of running it, that's a possibility.

Q. Or it's a possibility that it could be done in the future by an unscrupulous government administration; is that

correct?

A. It would be hard to do now even by an unscrupulous government administration because once we've got these things inhouse and got them tested we guard them pretty rigorously.

Q. Again, that's the we. I'm talking about if your successors-in-interest were --

A. Absolutely, yeah, certainly.

Q. -- were wanting to establish a police state, they could simply alter the software, could they not?

A. That's right, certainly, and my wife could kill me in my sleep but I try not to think about it.

Q. But does she think about it?

A. That's the reason I don't carry much insurance.

Q. How do you know that the software is the same for the test mode and the live elections?

A. Well, because there's just one set of software in there.

Q. Do the Diebold voting machines have dip switches that can be switched to allow the machines to be booted from inserted flash memory and external flash memory instead of the normal and the onboard flash memory?

A. Yes. Would you like to know what's involved in doing that?

Q. Yeah; sure.

A. You've got to turn the machine upside down, remove 17 screws, reset your dip switches, put the cover back on, replace the 17 screws, turn it right side up. Try doing that in a precinct with everybody watching.

Q. And if that was done, would the machine report that it had been done to it?

A. You would know it the minute you turned it on. You're quoting something from that Princeton study that you mentioned earlier.

Q. Do you agree that when one of our Diebold voting machines is booted differently than when certified it would also operate differently than when certified?

A. I'm not sure I know what you mean by booted differently.

Q. I'm not sure if I do either.

MR. FAVORITO: Want me to clarify it off the record?

(Discussion held off the record.)

BY MR. CHANDLER:

Q. All right. We're back on the record. I was just going to ask you if somebody wanted to defraud an election -- that is to say, for example, the Secretary of State decides that she wants to get reelected -- what would be the best way for her to make sure that she got reelected?

A. I'm not going to put that into public record for

security reasons.

Q. But there is a way?

A. There's always a way.

Q. And would you agree that if a way was found in an electronic system that there would be no way to have a recount other than it would yield the same result over and over and over?

A. If it got that far, but we believe that that would be detected before it got that far. We really believe that with the rigor that we protect these systems, the testing we do on these systems, the testing we do before an election, during an election and after an election, that we think that the probability that anybody could alter one of them in any way that was undetected by some of those tests that we do is minuscule.

Now, if that did happen, then we'd just have to take it to the nearest judge and say, "Look here, Judge; here's what happened. Now what's the remedy? Do you want us to rehold the election or what?"

Q. Do you agree that the Diebold voting machines use a customized version of a Windows CE operating system?

A. Yeah.

Q. Is that Windows CE operating system customized for use on voting machines?

A. It's not so much customized as it just doesn't

have all the features. They take out some of the features that are not necessary. They don't alter it any.

Q. Is there any documentation that exists showing that the Windows CE source code changes were examined prior to the 2002 elections?

A. No. Microsoft does not release their source code.

(Discussion held off the record.)

Q. We're back on the record. Are you familiar with a draft produced by the Technical Guidelines Development Committee of the Election Assistance Commission where it states that the NIST and the STS do not know how to write testable requirements to satisfy that the software in a DRE is correct?

A. Yeah, I'm aware of the document.

MR. RITTER: Let me just be clear. You've handed him the document. Why don't we mark it.

MR. CHANDLER: We may as well mark it.

MR. FAVORITO: I think that's K.

BY MR. CHANDLER:

Q. We'll mark it K, and off the record you had a time to kind of review this and all. Do you agree that it states that?

A. What it says is NIST and the STS do not know how to write testable requirements to satisfy that the software in a DRE is correct. That was written probably by Ron Rivas

to his chairman of that STS subcommittee and if he thinks NIST and the STS don't know how to write those requirements, then I don't have any reason to think they can.

Q. Do you agree with the first conclusion in Section 6 of the draft produced by the Technical Guidelines Development Committee when it states, "Software-independent approaches to voting systems are an effective approach to providing comprehensive and precise audits of voting system records."

A. Yes, sir, I do agree with that statement. Now, the problem, though, is how do you develop software-independent approaches, and that's a research topic right now. That is not something that is implemented in a voting system.

But what you're looking at there is a long-range future goal that's probably eight to ten years out in the future because the research is not even done much less the development or implementation.

Q. Since it's a goal, do you agree that that goal is a goal toward which our government in Georgia should strive?

A. Oh, yes.

Q. You said earlier that the issue of voter confidence -- do you think that the issue of voter confidence is integrally tied in with the idea that we need to have -- with that goal?

A. Not in Georgia. We have not had any evidence in Georgia that we have an issue with voter confidence; in fact, just the opposite. Every survey that's been done by the University of Georgia during an election has shown that in Georgia over 80 percent of the voters have confidence in our voting system.

MR. CHANDLER: Let's take a break. We'll step out in the little kitchen, confer and then have a few followup questions.

MR. RITTER: We'll step out and let you guys stay in here.

(Brief recess.)

BY MR. CHANDLER:

Q. All right. We talked about voter confidence just a moment ago. Are you familiar with the Atlanta Journal-Constitution poll that was conducted in 2006 about voter confidence in voter machines?

A. I don't recall what you're referring to.

Q. So are you aware of a 2006 AJC poll that stated that 88 percent of the Georgia voting public considered voting machine security as a top issue in the 2006 election?

A. I don't recall that, no.

Q. All right. What evidence do you have from actual elections that has demonstrated that your security testing is successful?

A. Say that again.

Q. What evidence do you have from actual elections that demonstrates that your security testing is successful?

A. Okay. In the election we do preelection testing and post-election testing and then parallel testing during the election, and in all of those we're comparing known vote patterns against what comes up on the machine, and in all of that testing we have yet to find a discrepancy.

Q. Do you ever have testing that involves like video cameras --

A. Yes.

Q. -- watching what's going on?

A. Yes. That's part of the parallel testing.

Q. If there was a failure of security, how would you know?

A. Well, by the results of these tests. It would show up in one or more of these various tests.

Q. Is there any way to know if vote tampering has been carried over into the ballot images?

A. What ballot images?

Q. I guess the ballot image where people are touching the screen in a particular spot.

A. The electronic image?

Q. Yes; during the parallel process, the parallel checking.

A. Didn't Ray Cobb describe the parallel test to you in detail?

Q. I believe he did some.

A. Well, then I'll go into it a little bit more. I'm not the expert on that. Ray's the guy you really need to talk to.

But basically on parallel testing what we do is we randomly select precincts and randomly select machines and set them up in the back room back here and during election using the actual -- the same database, election database that's used in those counties and in those precincts, we conduct a controlled vote where voters are given a script to vote and two people stand there. One calls it out and watches what's happening and the other one votes as a check that it's entered accurately.

And the video cameras record that and then at the end of the day we close the polls. We print those ballot images out and have an independent person count those ballot images manually. We don't tell them what the answer is.

And when they get them counted then we compare that to the electronic record and they've got to match a hundred percent.

I believe one time -- now, this is from memory so this may not be a hundred -- there may have been another one, but to my knowledge, there was only one time that there

was a one vote difference and we went back to the video cameras and actually found where one of the voters had hit the wrong button. So yes, that is an independent record of the vote.

Q. And then post-election checking, how is that carried out in a way that we know that ballot tampering has not occurred?

A. Well, what you're doing preelection and post election is you're verifying that the machine is functioning properly, and if the machine is functioning properly, then it's accurate.

Q. All right. This kind of goes back to something earlier and then we're almost finished.

When the NASED certification was completed for our system in 2002 who in Georgia received that documentation that the machines were certified?

A. Well, the documentation would be the reports from the ITA's and I would get those. The fact that that system is certified would be posted on the NASED website.

Q. Can you explain why as of March 3, 2003, NASED certification documentation had not been received --

MR. RITTER: Assuming it hadn't.

BY MR. CHANDLER:

Q. -- by the State?

A. I didn't know it hadn't.

MR. CHANDLER: All right. I think that's all the questions we have. Did you have some things you wanted to ask?

MR. RITTER: Yes. Thanks, Walker.

First let me say we may have an affidavit later from Mr. Williams. He has not been identified by us as an expert and not been prepared by us as an expert but I do have just a couple questions to follow up and clarify some testimony right now.

- - -

EXAMINATION

BY MR. RITTER:

Q. First, Dr. Williams, let me take you back to your testimony, which I think was that it was possible that Microsoft Access could be used to possibly change some of the software without leaving a trail.

A. Uh-huh (affirmative).

Q. Can you describe for us how probable you think that is?

A. Well, it's extremely improbable. If you go back through all of these various studies -- and that's one of them you're referring to that Ms. Harris has sponsored, that Princeton -- all of these different studies, they are all based on open access to the entire system. They have the

source code. They have access to -- free access to the machines.

That's not the way you run an election. In an election you have elaborate controls all around the whole process. When you walked in out here you had to sign in. You may not realize it but any time you're in this building you're escorted, particularly -- if you come down to this end of the building, maybe not, but if you try to go to the other end of the building, you'll find out very quickly that it don't work because that's where we've got servers; we've got software.

So we go to elaborate lengths, probably way overkill to protect the integrity of the system. And if you go around the country talking to the various election officials and election directors and you go up to Washington and you talk to the EAC, you'll find that Georgia is the envy of the nation when it comes to the way we manage and control our voting system.

MR. CHANDLER: Do Diebold employees have access to the machines during an election?

THE WITNESS: No.

MR. CHANDLER: Do county election officials have access to the GEMS voting database?

THE WITNESS: It's on their machine. Yeah, they have access to the database.

MR. RITTER: You're asking about the database, not the overall GEMS software; is that right?

MR. CHANDLER: Yes.

MR. RITTER: And that's what your question relates to?

MR. CHANDLER: Yes.

BY MR. RITTER:

Q. Now, let me move on. I've got a couple other quick followup questions. Let me turn to Exhibit J. I don't think this was ever identified so first let me ask you to identify what Exhibit J was.

A. Are you asking me to identify it?

Q. Yes.

A. What it is or where it came from?

Q. Well, what it is. What is it a picture of?

A. That's a picture of the internal mother board on a touch screen voting system.

Q. And I think you were asked about Exhibit J when they were talking about dip switches. Can you explain for the court what a dip switch is?

A. Well, it's a little switch that's basically a two-way switch that if you switched one way it gives you one outcome; if it switched another way it gives you another. Here in the middle of this exhibit is the list of dip

switches they're talking about and what they're saying is --

Q. Just a moment. Let me -- just so that we're clear because we're creating a transcript here that'll probably be read by the court and I'd like the judge to be able to understand, could we mark on Exhibit J where the dip switch is, like draw an arrow to that just so that the judge could look at that and see where the dip switches are.

A. (Complying). There's three of them and if you set them a certain way you can boot either from an EPROM or an external flash or an internal flash. Now, where are the switches? Let's see how they're set.

Let me say this about this study. If you go back and read -- this is a picture from the Princeton study. If you go back and read that study, you'll see that what they're saying here is all conjecture. They did not change those switches and insert a flash card and boot from that flash card.

They're saying looking at the settings on this board it looks like you might be able to do that. But nowhere did they actually boot from a flash card and change software in the system. This is all pure conjecture. And if you go through all of those studies, you'll pretty much find the same thing.

And the only ones that have been able to successfully change anything are those where they got inside

and used that Access database to make changes in that Access database. That's entirely possible and that's why you put rigorous physical security around those systems.

Q. My understanding is that the dip switches -- one of the things they will do is change the way that data can be input into the machine.

A. No, it changes the boot. These that they're talking about here changes the device that you boot from. You can boot from your normal boot routine or you can boot from -- this isn't a complete picture. It doesn't have the slots on it. You can boot from a flash that's inserted in one of these slots. If you want to take 17 screws out of the back of one of those things, I'll show you what this is talking about.

Q. Sure, but we need to explain this for the record. So that the judge will understand, what do you mean by boot?

A. When you start it up it looks somewhere to see what it's supposed to be running.

Q. It's turning on the computer.

A. Right. When you turn your computer on it looks out there on your disk to see what it's supposed to be -- to a boot record to see what it's supposed to be running and it says ah, there's Windows XP so it brings up Windows XP. Now, this controls which device it looks to for that boot.

Q. Whether it would look to a storage card like a

flash card or look to a hard drive?

A. Right, or whether it would look to a PC card stuck in an external slot or to a flash card put in one of those slots internally or what.

So what you could do is change the physical device that the machine boots from. Now, you still haven't changed the machine. You're just changing where it boots from. Now you've got to go onto that device and be clever enough to put whatever changes or software or what have you you want on that. These things are not trivial and it's no accident or no oversight that they didn't actually do that in this study.

Q. Now, why would you change where it boots from if you were trying to alter --

A. If you had your own little system on a flash card, then you could put yours in that slot and change the dip switches so it would boot from your system instead of its system.

Q. So that way you could try to create a sort of fake election or fake election results with that.

A. That's right. And if you want to change an election, doing that in the State of Georgia you would have to take some significant portion of those 26,000 voting machines, take the 17 screws out of the back of them, change your thing, put the 17 screws back and get them back where

they were without being noticed.

Then you're not through because you've got a record of your crime sitting out there so after the election you've got to repeat that process to get all those things out of there and set those switches back where they were.

See, this is the sort of thing that is the difference between possible and likely. Possible, yes; likely, absolutely not.

Q. And that's where I was going with this. You're saying -- and explain for us -- that to change the way it boots and therefore reads to create this election you've got to change the dip switch on every single machine you're trying to effect.

A. That's correct.

Q. Which would involve unscrewing the 17 screws, turning it over, then going inside, changing the dip switch and then installing the improper software.

A. That's correct.

Q. And then you have to after the election go back and undo all that to remove the evidence.

A. That's correct.

MR. RITTER: All right. I think that's all the questions I have for the moment.

- - -

FURTHER EXAMINATION

BY MR. CHANDLER:

Q. Just one followup question. In the parallel testing you described is there public access to the evidence created by that testing?

A. I'm confident there is. I mean, you know, elections are one of the most public things you'll ever see. You can observe just about any portion of an election. These things you're talking about where people are modifying this GEMS system, that's public. When they're in those county offices, when they're running those results on election night, that is very public and there's usually a lot of people standing around there watching. So I'm sure this is all public information.

Q. All right.

- - -

(Deposition concluded at 1:25 p.m.)

- - -

C E R T I F I C A T E

STATE OF GEORGIA:

COUNTY OF CHEROKEE:

I hereby certify that the foregoing transcript was taken down as stated in the caption, that the witness was first duly sworn, and the questions and answers thereto were reduced to typewriting under my direction; that the foregoing transcript is a true and correct record of the evidence given, and I further certify that I am not a relative or counsel to the parties in this case, am not in the regular employ of counsel for any of said parties, nor am I in anywise interested in the result of said case.

Disclosure pursuant to OCGA 9-11-28(d): The party taking this deposition will receive the original and one copy based on our standard and customary per page charges. Copies to other parties will likewise be furnished at our standard and customary per page charges. Applicable incidental expenses of production may be charged to any party.

This, the 2nd day of August, 2007.

Sharon J. Ruschell, RMR, CRR, CCR B-1179

My Commission Expires 2-19-2008