

EXHIBIT I
Comments, Questions and Witness Responses¹
Committee on House Administration
EAC Oversight Hearing, June 8, 2006

"CHA:" indicates a question from a member of the Committee on House Administration, while "EAC:" indicates a response from a Commissioner of the Elections Assistance Commission.

VOTER-VERIFIED PAPER RECORD REQUIREMENTS

CHA: One last quick question: there's a lot of support out there for voter-verified paper audit trails, as it's called, and we have a bill introduced in the congress to require that. What's your opinion of that? Is that the best way to ensure we can have a complete accurate audit, or have you conjured up or thought of some other approaches we might take to deal with that question?

EAC: The EAC has not taken a position on VVPAT per se. We have provided in our VVSG, standards and guidelines for the use of the VVPAT which is now mandated in 26 states across the nation ... Three years ago, there were no states, two years ago it was just the State of Nevada. So there has been a dramatic change. I think it's been a whole issue of independent verification of the voting process and of the balloting which one takes a look at. We set up procedures in the VVSG and in the management guidelines that we're going to issue this summer, to show election officials how they can secure a voting system from beginning to end, so people can have trust and confidence. Some states have decided to have VVPAT as part of that component, to trust the system that way. Other states have chosen not to because they feel comfortable in the system that's set up, because there is an audit requirement under HAVA. Electronic machines, even those that are not required to have a VVPAT, are required to produce audit trails of what is inside the machine, so that every ballot that's cast can be audited. So it can be trustworthy in a system whether it has VVPAT or not. We haven't taken a position on whether to advocate for that nationwide.

MEANINGFUL AUDITS WITHOUT VOTER VERIFICATION?

EAC: ...Some states have decided to have VVPAT as part of that component, to trust the system that way. Other states have chosen not to because they feel comfortable in the system that's set up, because there is an audit requirement under HAVA. Electronic machines, even those that are not required to have a VVPAT, are required to produce audit trails of what is inside the machine, so that every ballot that's cast can be audited. So it can be trustworthy in a system whether it has VVPAT or not. We haven't taken a position on whether to advocate for that nationwide.

HUMAN FACTORS

CHA: Let me ask also about human factors I pushed hard for that. Are you satisfied these were dealt with appropriately? For years I've heard "we have to train poll-workers better, train voters better..." I say that's utter nonsense. You can't expect people to remember from one session to another. Equipment and procedures should take account of that and be designed in such a way that no one should have to be trained, it should be so elementary anyone can do it without error. Has that goal been accomplished?

¹ Transcribed by Verified Voting from videotaped proceedings as posted at CHA website: <http://cha.house.gov/hearings/hearing.aspx?NewsID=1353>.

EAC: It's been worked on. We've increased from 29 to 120, made a good start. But right now, what they've done to meet VVPAT, for instance -- they've attached paper on the side of the equipment-- that's not useful to the judges. They are having issues, getting it attached and working properly. In our next iteration, that's one area we'll be looking into that a great deal. We've improved it, but not enough.

SECURITY VULNERABILITIES and CERTIFICATION

CHA: With the certification process that has been set up We read in the papers last week that Diebold has a great vulnerability I knew there would be, but to have such an obvious and simple one was surprising. Did that sneak through? Or was that particular model certified?

EAC: - Equipment was certified in the past by NASED. Our program will be far more vigorous. If a particular problem like that would be caught, I'm not for sure. When that was found, the individual went into an office and had access to the whole system and software. It's not like someone from outside found it.

COMPUTERS EASY TO HACK

CHA: One area I'm still very worried about is the lack of expertise of average Americans in dealing with computers... It's remarkably easy to hack into a computer and change things. I still want to keep an eye on the safeguards that are being developed to prevent that from happening.

RANDOM CHECKS

CHA: One other question, with the whole issue of this security Maryland I believe does random checks on its machines, is that right? [DD: Many states do.] I don't know why the states don't do that, and then this whole question of the security, like the slot machines, they have this whole system when they are manufactured and tested and then when in place, if it was required and at random, it would put it to rest and people would feel better about the security of these machines. Have you looked into that at all?

EAC: We are. In the draft we are developing our certification process, as described this morning. We are taking a look at doing random checks of voting equipment. As we look at certifying equipment, we're indeed taking a look at the EAC taking on a role of doing random checks of voting systems around the country.