Venango County

Courthouse Annex

1174 Elk Street, Box 831

Franklin, PA 16323

814/432-9501 FAX 814/432-4741

Board of Elections

Craig Adams, Chair

Martha Breene, Vice-Chair

Eleanora Miller

Chief Clerk

Denise Jones

November 29, 2011

Honorable Carol Aichele
Secretary of the Commonwealth
302 North Office Building_
Harrisburg, PA 17120

Dear Secretary Aichele,

As you may know, since between May of 2006 and May of 2011, voting in Venango County was carried out using an election system provided by ES&S. Most votes were cast using iVotronic DRE (direct recording electronic) voting terminals; absentee ballots were scanned using an M100 optical scanner; ballot preparation and tabulation have relied on the Unity software suite. It is our understanding that the elements of this system were certified by your office in 2006.

Recently questions have arisen about the security and auditability of the iVotronic DRE's. We wish to request information and guidance from your office to inform the decision-making process of the Venango County Board of Elections.

First, with respect to the security of machines running the Unity ballot preparation and tabulation software, we request clarification of language in the certification documents. The original iVotronic certification document (December 22, 2005) includes this language (bold-face type is in the original document):

> Unity runs on an ordinary Windows laptop or desktop. Such a machine could be connected to the Internet, have a wireless card or Bluetooth interface, or be attached to a local or wide area network. All of these represent security risks of varying risk. Unity makes no effort to restrict, or even monitor, these possible connections. The configuration of the Unity computer is therefore uncontrolled and unauditable. That is, after an election, it is impossible to determine what modifications might have been made by an intruder, a virus, spyware or other species of malicious code. […] **The Secretary requires that Unity be operated as a standalone system without network connection, local or otherwise.**

The amended certification (April 7, 2006) appears to reaffirm the above requirement ("Conditions for Certification, page 5).

We wish to understand the precise meaning of the Secretary's requirement, in particular the ban on

network connections is temporary (while Unity is actually in operation), or whether it is permanent, i.e., from the time that Unity is installed on a computer until the time it is uninstalled, no network connections of any kind, even a wired Ethernet within a single room, are permitted.

Second, an anomaly was observed during analysis of a "log" file produced by Unity, in particular the EL68A "System Log", which is documented by the vendor as reporting "every action performed in your election system in chronological order." In particular, between "log" records indicating activity taking place on May 13 and May 16, there appear "log" records indicating activity on July 9. As you might expect, this observation is perplexing to us and is a cause for concern. We request information and guidance from the Secretary as follows:

Is the Secretary's office aware of other instances in which the contents of the EL68A "System Log," or other "log" files produced by Unity, appear not to be in chronological order? If so, is an explanation available for this situation? As we understand it, the contents of the EL68A "System Log" represent a report on data stored within Unity in a proprietary data format which is not publicly documented. If this is the case, is the Secretary's office able to suggest to us whether the sort of anomaly we have observed is due to incorrect data stored within Unity, incorrect conversion of the data to the human-readable EL68A "System Log," or due to some other known reason?

Third, as you may be aware, two in-depth studies of the iVotronic software took place after the Secretary's 2006 certification. The "SAIT study", commissioned by the Florida Department of State and published in February of 2007, disclosed that version 8.0.1.2 of the iVotronic software contained multiple security vulnerabilities, including "several software defects that could allow an attacker to introduce a virus into the voting system" (Section 7.11) and an "undocumented backdoor" which allows all password checks to be bypassed using a device called a "Factory Test PEB" (Appendix D). The "EVEREST Report", commissioned by the Ohio Secretary of State and published in December of 2007, found that "a particular challenge in securing the iVotronic DRE terminal is the large number of precinct-based attack vectors whose exploitation must be prevented" (Chapter 4). The study includes a picture of an iVotronic being compromised by the "Factory Test PEB" vulnerability, carried out using a widely available palmtop computer (Figure 7.1). The EVEREST study examined iVotronic firmware versions 9.1.6.2 and 9.1.6.4.

We are seeking guidance on the following questions related to the results of these studies.

1. Because we do not have access to the source code for the iVotronic firmware certified for use in Pennsylvania, version 9.1.4.1, we do not know which vulnerabilities reported by the SAIT study and the EVEREST study are present in the iVotronics owned by Venango County. Likewise, the EVEREST study identified vulnerabilities in Unity 3.0.1.1; we do not know which of those vulnerabilities is present in the version of Unity certified for use in Pennsylvania, 3.0.1.0. We request any information that the Secretary has on which vulnerabilities are present in voting system hardware, firmware, and software in use in Venango County which are certified by the Secretary's office. If the Secretary's office does not presently possess information on which, if any, of the publicly identified vulnerabilities are present in systems certified by the Secretary's office, we request that the Secretary investigate and issue a public report.
2. Based on the information in the reports cited above which became available after the Secretary's certification of ES&S voting-system equipment, does the Secretary affirm the existing certification of this equipment for use in Pennsylvania elections?

3. Based on the information in the reports cited above which became available after the Secretary's certification of ES&S voting-system equipment, are particular precautions or checks warranted, suggested, or required in order for this voting-system equipment to be used securely and accurately in Pennsylvania elections?
4. Enclosed below please find a two-page letter written by Steven M. Pearson of ES&S. The letter is not dated, but because it was included as an attachment to electronic mail, dated May 14, 2007, sent by Harry VanSickle, then of the Secretary's office, to Mark Wolosik, Manager of the Elections Division of the Allegheny County Department of Administrative Services, we assume the letter was written no later than May of 2007. The letter makes reference to a new version of iVotronic firmware without the "Factory Test PEB" vulnerability, expected to achieve Pennsylvania certification "later this year" (presumably 2007).

Was new iVotronic firmware submitted for Pennsylvania certification in 2007 or since then? To the extent of your knowledge, is new iVotronic firmware for Pennsylvania imminent? If so, is it likely to be available before the April 2012 primary election?

The conclusions reached by the authors of the SAIT and EVEREST reports, both commissioned by secretaries of state, concern us. Because we are not in a position to evaluate whether those conclusions apply to the software certified by your office, we have requested your input on the issues raised above.

Finally, after the May 2011 election, we received multiple troubling reports from voters that specific candidates were missing from ballot display screens while they were voting. Thus far we have been unable to conclusively determine exactly what those voters experienced or why. Has your office received similar reports from voters? If so, could you summarize any investigative efforts carried out by your office and any results of any such efforts? Can you suggest any ways to "audit" the ballot displays seen by voters using iVotronic DRE terminals?

We appreciate any light you can shed on these matters.

Sincerely,

Venango County Board of Elections

Craig Adams, chair Martha Breene, vice-chair Eleanora Miller

Enclosure: letter from Steven M. Pearson of ES&S

Cc: Shannon Royer
Deputy Secretary For External Affairs and Elections
Bureau of Commissions, Elections and Legislation
210 North Office Building
Harrisburg, PA 17120

Election Systems & Software
MAINTAINING VOTER CONFIDENCE. ENHANCING THE VOTING EXPERIENCE.
EXPERIENCE
RELIABILITY
SECURITY
INNOVATION
11208 John Galt Boulevard · Omaha, NE 68137 USA
Phone: 402.593.0101 · Toll-Free: 1.800.247.8683 · Fax: 402.593.8107
www.essvote.com

Harry A. VanSickle
Commissioner
Department of State
Bureau of Commissions, Elections and Legislation
210 North Office Building
Harrisburg, PA 17120

Commissioner VanSickle,

Thank you for the opportunity to provide you with important information regarding ES&S voting technology. As you know, we are fully committed to providing jurisdictions with voting systems that are secure, reliable, and accurate. Further, we are constantly seeking ways to enhance our voting technology. That is why we have very carefully reviewed the extensive, independent technical analysis conducted by the Security and Assurance in Information Technology Laboratory at Florida State University (FSU).

The team of experts conducting the FSU review unanimously determined that there were no software malfunctions that would have contributed to the 13th congressional district undervote total in that county. Their findings, along with the results of audits and parallel tests conducted by the Florida Department of State, a mandatory recount of the race (because of the small margin in results), local audits and post-election testing, court consideration of allegations that the voting equipment did not function properly, and other expert, independent assessments demonstrate that Sarasota County's voting system performed properly.

In addition to their primary task of investigating the congressional race, the FSU team also provided some feedback about potential technical enhancements that could be made to the iVotronic. One of the areas of focus included a hypothetical scenario involving use of a "factory test" PEB to attempt to override security features that require passwords for numerous functions of the technology.

Implementation of such a plan would require a fatal breakdown of standard protocols in Allegheny County's election security procedures. Specifically, the plan would require;

- the construction or acquisition of a highly sophisticated "factory test PEB;"
- prolonged access to voting equipment, unnoticed by any election official; and
- a sophisticated and extensive knowledge of the iVotronic system, including knowledge of the system's proprietary software and hardware.

In reality, such an effort is extraordinarily unlikely. Established election processes and procedures, including those already in use throughout Pennsylvania, would identify and prevent this type of security threat. The Department of State, Allegheny County, and

citizens of Allegheny County should be assured their election equipment and election procedures are secure.

Further, we have already made enhancements to the iVotronic firmware that completely eliminate the already remote possibility of such a threat. In fact, the next release of iVotronic firmware, which we expect to complete the EAC federal testing and state certification processes later this year, eliminates this capability entirely.

Again, thank you for the opportunity to provide this information. If you have any questions, please contact me.

Sincerely,

Steven M. Pearson
Vice President, Certification
Election Systems & Software