McCullough Research

ANDREW NISBET
PRINCIPAL

Date: January 20, 2011

To: Voter Integrity Project

From: Andrew Nisbet
Robert McCullough

Subject: Electronic Security at Multnomah Elections Office

The level of security at the Multnomah County Election Division Office, although generally sound, has one vulnerability that is sufficient to render the election results suspect.

The location of the six tally machines and their relationship to the personal computer is critical to the credibility of the result. All seven machines are located in a locked room – the "Red Room". The tally machines are highly secured complete with printers to report both audits – changes to the machines – and results. The six tally machines are connected to a standard personal computer through Ethernet cables.

While the tally machines are highly secured, the personal computer that actually reports the results is not.

In 2007, the Multnomah County Auditor addressed the issue of Electronic Security at the Morrison facility:

> Additionally, at the request of an observer, Elections expanded the testing to include a comparison of printed totals from each tally machine to the compiled totals from the computer. Finally, they were responsive to our interim report on tally system programming and implemented several additional controls for this process, such as keeping

6123 REED COLLEGE PLACE • PORTLAND • OREGON • 97202 • 503-777-4616 • ANDREWN3@MRESEARCH.COM

> the sealed public certification results in the custody of someone other than the individual who runs the test.[1]

After 8 p.m. on the day of the election the personal computer is linked by Ethernet cables to the six ballot counting machines and totals are calculated. At the first public test of the ballot counting machines, staff was asked if the individual totals of six ballot counting machines were compared with the computer's results and the answer given was no. On the night of the election Janice Dysinger asked if she could have the totals from each of the six ballot counting machines so we could compare them with the computer's results the answer given was that the ballot counting machines don't generate totals. This statement would appear to contradict the 2007 Elections Audit quoted above.

When asked about post-election checking of tally machine totals against the results from the personal computer, Eric Sample of the elections staff indicated that this was not part of the procedure.

At the first public test of the ballot counting machines we were told that the network serving the tally machines and the personal computer was isolated. Andrew Nisbet asked if he could check to see if the system in the red room was actually isolated. He was told that this would have to wait until after the election.

It is not possible for observers or staff to monitor this part of the system, as the connections between the tally machines and the personal computer are not in plain sight. While it would be possible to tap into the network out of sight of the elections staff or election observers, this is not required to adjust the results of the tally machines.

The vulnerability of the connections pales when one considers that the unity machine has several unsecured USB ports.[2] What that means is that anyone who has had 30 seconds of unobserved access to the personal computer could adjust the programming or directly overwrite the election results. Best practices for mission critical equipment is to reduce

[1] Elections Office Audit, June 27, 2007, page 14.
[2] Universal Serial Bus (USB) is a standard communications capability available on almost all computers. USB "keys", "sticks", or "drives" are small devices routinely used to transfer files between computers. A USB "key" is easily carried. Standard USB devices are ½" by ¼" by 1".

access to the absolute minimum – often by using software to block unauthorized data transfers and physical elimination of data entry devices like USB ports.

The security of the elections process would be dramatically enhanced if:

1) The personal computer was physically secure in its own locked enclosure.
2) The software on the personal computer was checked before use. One option might be to secure the hard drive of the personal computer in a different location until needed.
3) The personal computer had an external audit log, preferably in hard copy, comparable to those on the tally machines. Absent an external audit log, the

operating system on the personal computer should be upgraded to Windows Server 2008 R2 and the operator should not be granted administrator status.[3]

4) The USB ports (and any other unneeded access ports) on the personal computer should be disabled.
5) The personal computer and the tally machines be subject to the testing as outlined in the 2007 Elections Office Audit.
6) The personal computer and the tally machines should be subject to video surveillance.
7) The Ethernet network – and the hub connecting its nodes – should be in plain sight.

Given the answers of the elections staff during the public tests of the tally machines, it is possible that the personal computer results would not be checked against the tally machines. Moreover, if the tally machines are "zeroed out" in subsequent tests, it might well be impossible to verify the election results against the tally machines at a later date.

We requested a report from the tally machines and compared it against the summary provide from the personal computer and saw no anomalies for the current election.

We would like to make it clear that the character of the elections staff is not in question. Their conduct of the election staff during the public tests of the tally machines was forthright and competent. Notwithstanding, reporting the results of the highly secured and tested tally machines on a relatively unsecured and untested personal computer is likely to provide a temptation for misbehavior. This is especially true when checks and balances suggested by the 2007 audit report appear not have been implemented three years later.

[3] The elections staff was unable to describe the degree of software security during the public tests. The standard Windows software is renowned for its lack of security. More sophisticated operating systems provide substantially upgraded safeguards against intrusion.