October 5, 2005

Comment on WiFi Threats: http://vote.nist.gov/threats/papers/wifi_outsider.pdf
and http://vote.nist.gov/threats/papers/wifi_insider.pdf

I agree with Mr. Epstein concerning the threat WiFi equipped systems pose to electronic voting systems. I am somewhat concerned that this discussion is focused on WiFi and not Optical and RF in general. Any method of communicating with the voting system including optical or other RF communications systems presents an equivalent threat.

A number of existing voting systems are equipped with IrDA (Infrared Data Association) optical wireless ports. These systems support communications with the DRE voting systems at data rates up to 115 Kb/s.

In Diebold System's AccuVote TS systems these ports are supported using Microsoft's Windows CE with Winsock. This makes the application interface easy to program to, and all required drivers are already installed in the OS.

It is interesting that the VVSG currently under development, while mentioning this technology does nothing to restrict or prevent its use, not even on Election Day.

It is understandable that communications technology be used for pre election preparation, but is totally irresponsible and inexcusable to allow it to be used during an election. The presence of this technology makes it possible to upload to the voting system anything that is desired after the final "Logic and Accuracy" test have been performed, thus totally compromising the system. Even the ability to transmit as much as a single frame (even an error frame) of data could be sufficient to alter the approved behavior of the system.

I submitted a short paper discussing this issue to the TGDC entitled Comment on Wireless Requirements, at http://vote.nist.gov/ECPosStat.htm. I believe this to be a highly likely line of attack on voting systems unless the technical community is vocal in exposing this threat before it becomes accepted practice to install optical ports in voting systems. I hope that you will use your influence to draw attention to these flaws as well as to the threat of WiFi.

Thank You,
James C. Johnson