



# County of Allegheny Election Tabulation Network Analysis

## Findings and Recommendations Report

November 6, 2006

Prepared by:  
Brian Eckels, CISSP

Submitted to:  
Jason Ditzenberger

## Executive Summary

VigilantMinds was asked to verify that the election tabulation network and associated devices were not connected to any other networks. This was accomplished by:

- Viewing the switch management interface to verify that the switch was properly reporting the connected devices
- Checking Ethernet ports in the room where the equipment is located to verify they are disabled
- Verifying that none of the machines were connected to an external wireless network
- Tracing all cables connected to the election tabulation network's switch to verify they were connected to permitted devices

## Observations

VigilantMinds arrived on-site at approximately 8:00 AM on Nov. 6, 2006. At approximately 8:25 AM, the consultant entered the room where the election tabulation network is located. The only materials the consultant took into the room were a laptop and a notepad for recording observations. The consultant's laptop was not connected to the election network in any way; it was used only to verify that Ethernet ports in the room normally connected to other networks were not active (no link). The consultant left the room at approximately 10:00 AM on Nov. 6, 2006.

The following diagram shows the election tabulation network as it was configured at the time the consultant left the premises:

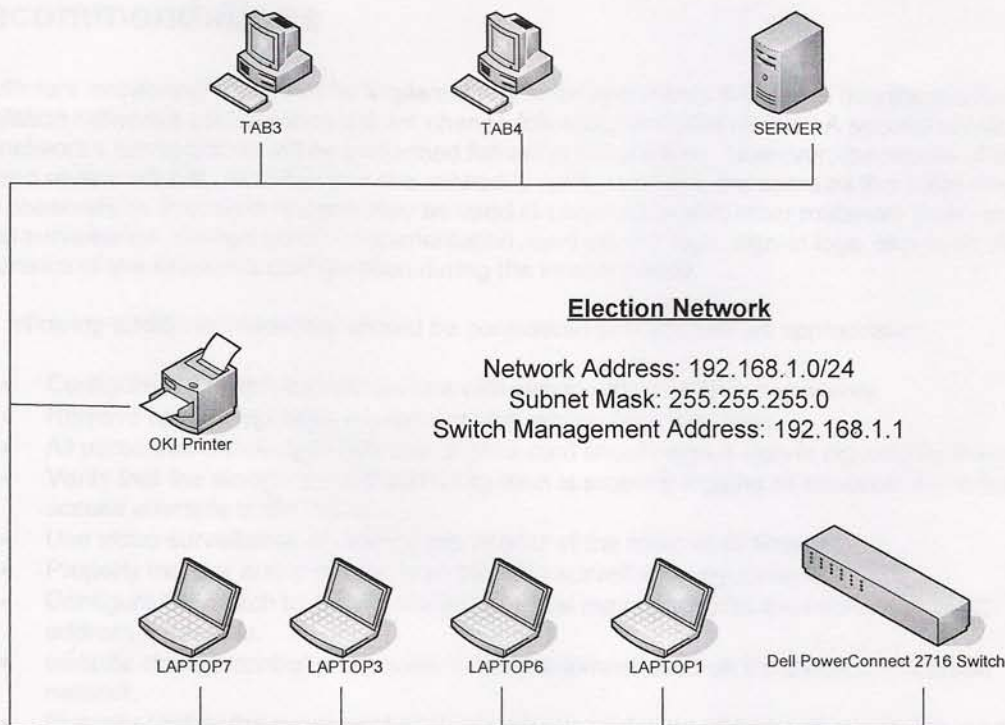


Figure 1 - Election Tabulation Network Configuration

VigilantMinds recorded the following observations about the network and facilities:

- All devices are connected via Ethernet to a Dell PowerConnect 2716 switch.
- All devices are on the same subnet (192.168.1.0/24).
- The Dell PowerConnect 2716 switch properly reports the number of attached devices.
- One cable was connected to the switch which was unused.
- One PC was found in the room which was off and was not connected to the election tabulation network.
- Miscellaneous cabling and equipment was present in the room.
- The room has external video surveillance as well as electronic card access control.
- The Dell PowerConnect switch was not properly configured and had to have its management interface address changed to 192.168.1.1 from the default of 192.168.2.1.
- The Dell PowerConnect switch has no logging capabilities and limited abilities to report on attached devices. As a result of this limitation it is not possible to conclusively identify changes to connections without constant video surveillance of the room's interior.
- All Ethernet ports in the walls (normally connected to other networks) were found to be inactive.
- No sign-in log was present for the room where the elections tabulation network is located.
- The Dell PowerConnect switch did not have an administrative password assigned to it.

VigilantMinds did not examine:

- Electronic card access system
- Video surveillance systems
- Configuration of systems connected to the election tabulation network
- The contents or security controls of an adjoining room

## Recommendations

Insufficient monitoring is present for VigilantMinds to independently determine that the election tabulation network's configuration did not change following the initial review. A second review of the network's configuration will be performed following the election. However, the results of the second review will only establish that the network's configuration is the same as the initial review. The observations from both reviews may be used in conjunction with other materials (such as video surveillance, change control documentation, card access logs, sign-in logs, etc) to provide assurance of the network's configuration during the interim period.

The following additional measures should be considered and adopted as appropriate:

- Configure the switch and all devices with strong administrative passwords.
- Remove any unnecessary equipment and cabling from the room.
- All personnel without an electronic access card should sign a sign-in log prior to entry.
- Verify that the electronic card access system is properly logging all successful and failed access attempts to the room.
- Use video surveillance to monitor the interior of the room at all times.
- Properly monitor and control access to video surveillance equipment.
- Configure the switch to restrict the devices that may connect to the network by MAC address if possible.
- Institute change control procedures for all equipment used on the election tabulation network.
- Properly control the movement of all equipment (including all types of removable media, such as flash/SD cards, floppy disks, CDs, DVDs, USB or 'thumb' drives, etc) into and



out of the room. Any equipment that enters or leaves should be recorded in a written log with the purpose of the equipment stated. Any removable media which enters or leaves should be scanned for viruses and have its contents verified.

## Conclusions

Assurance of the tabulation network's configuration can only be given if both reviews are used in conjunction with other records as noted above.

VigilantMinds appreciates this opportunity to work with the County of Allegheny and looks forward to future engagements.