# County of Allegheny

## 2016 Pre/Post-Election Air Gap Analysis of Election Tabulation Network

Research and Recommendations Provided by:

solutions 4networks

*a network infrastructure company*

Jacob Winkle
Senior Consultant
jwinkle@s4nets.com
412.660.0867

**Table of Contents**

## Overview

The County of Allegheny has engaged solutions4networks to perform an "Air Gap" analysis of their elections tabulation network located in Pittsburgh, PA. solutions4networks has been tasked to verify the tabulation network is a stand-alone, isolated network and to assess the network's vulnerability to external access and/or tampering. In addition to the network, solutions4networks has been asked to assess and document the general physical security of the warehouse building.

An on site visit was made by Jacob Winkle of solutions4networks on April 25, 2016. The purpose of this document is to report the results of the assessment, identify security concerns and to make recommendations for the remediation of these concerns. A post-Election onsite visit was made on April 28, 2015. This report covers both the Pre-Election assessment and the Post-Election review. Post-Election Review updates will be noted in red.

### Site Contact

Elizabeth Dell
Elizabeth.Dell@AlleghenyCounty.US
412-350-6059

Robin Gigliotti
Robin.Gigliotti@AlleghenyCounty.US
412-629-7322

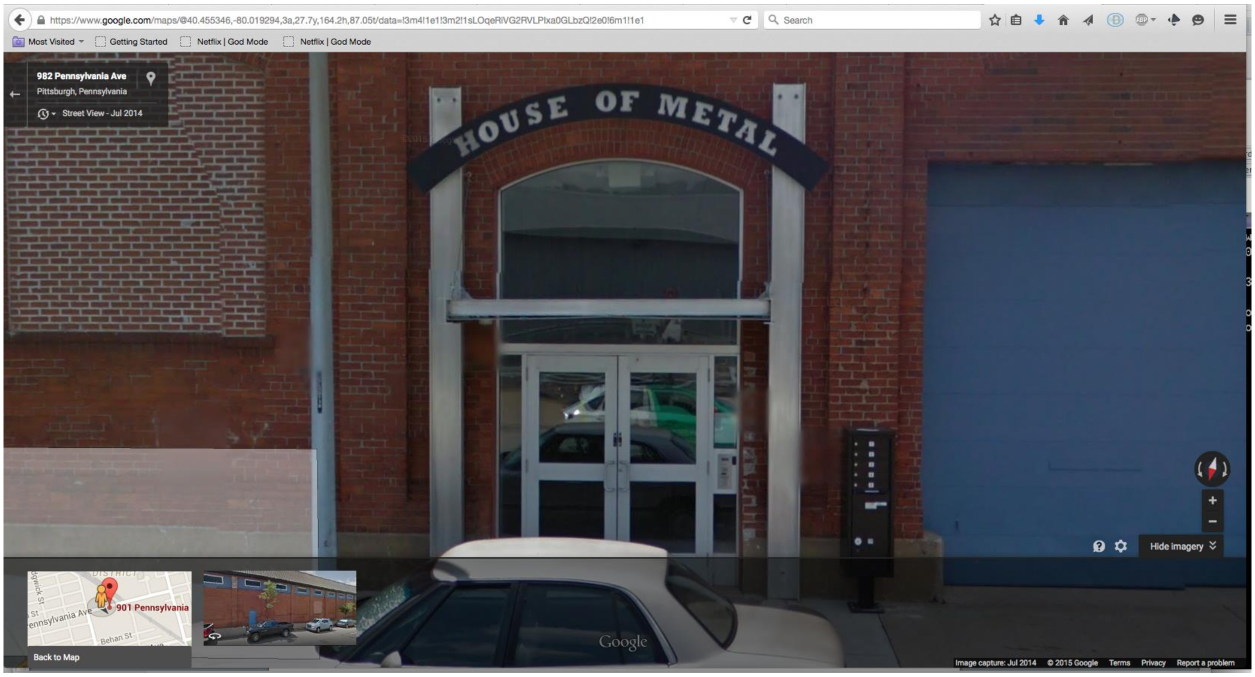
901 Pennsylvania Avenue
Pittsburgh, PA 15233

## General Physical Security/Building Access

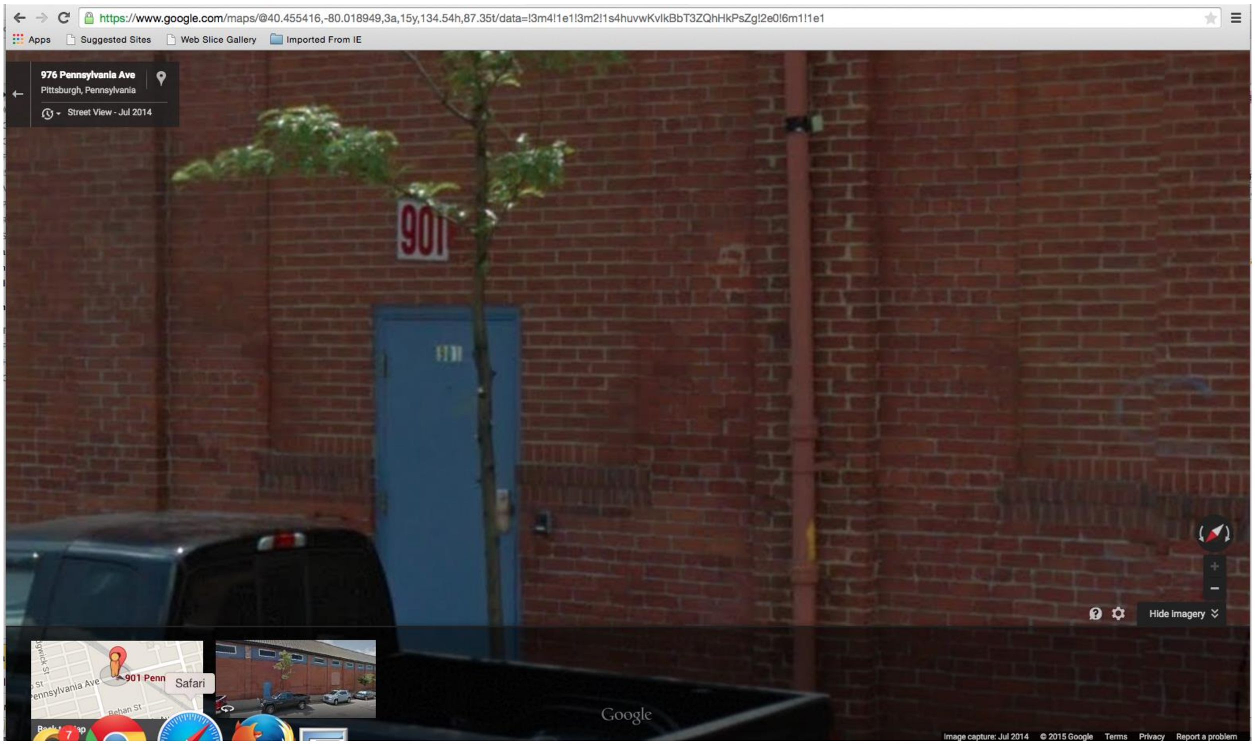
### Physical Security/Building Access - No Issues Found

There are several suites within the warehouse and there were no outside signs, which identified the County of Allegheny building space. The building phone at the main entrance also did not have any entries to dial for the County of Allegheny.

## Building Main Entrance:



## Suite 901:



solutions4networks was met at suite 901 by Robin Gigliotti after a call was placed to her cell phone and was asked to provide driver's license identification and a business card before access to the building was granted.

Entrance from the street required badge card access. The first door in the warehouse required a security code, but it was a physical, non-electronic lock.

Security cameras were observed over the street entrance and inside the computer room. Cell phones were not permitted into the computer room that contained the tabulation network.

Post-Election Review: All items indicated above remained the same.

# Election Tabulations Network

## Network Overview - Physical

A Network Topology diagram was provided to solutions4networks. The observed network topology was identical to the provided drawing.

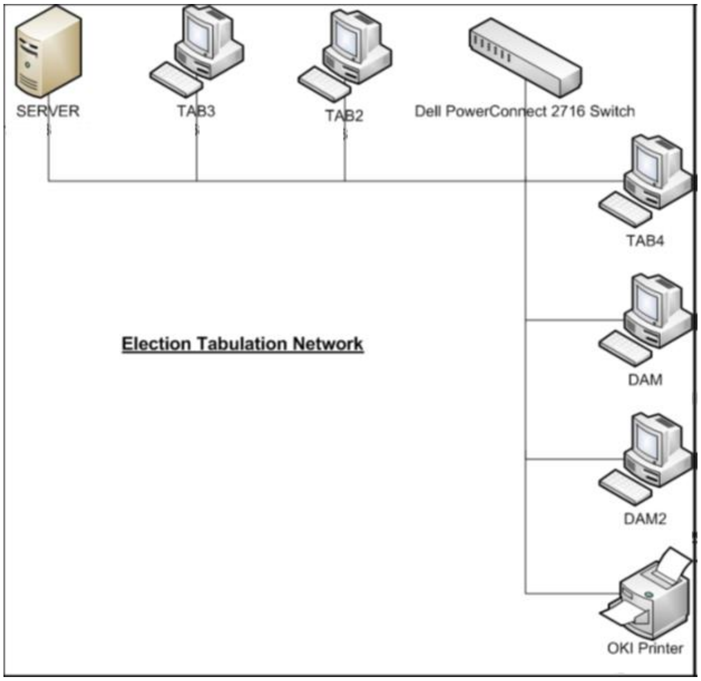


Figure 1 - Election Tabulation Network

The Election Tabulation Network consisted of the following devices:

- 1 Dell Powerconnect 2716 Ethernet Switch
- 1 Windows Server
- 5 Client PC's
  - Two DAM (Dial Access Modem) Servers
  - 3 Windows XP Clients
- 1 Printer

## Network Overview - Logical

All of the devices had an address from RFC1918 private network 192.168.1.0/24. The Windows Server with address 192.168.1.20 provided DHCP, DNS and WINS services. A default gateway of 192.168.1.1 was configured, but no such device was found on the network.

Post-Election Review: All items indicated above remained the same.

| Dell Server PE-SC1420 | Dell Optiplex GX520 | Dell Optiplex GX520 | Dell Optiplex GX520 | Dell Precision PWS690 | Dell Precision PWS690 |
|---|---|---|---|---|---|
| BOE.elections.local | TAB3.elections.local | TAB2.elections.local | TAB4.elections.local | DAM.elections.local | DAM2.elections.local |
| Provides DHCP, WINS, DNS Services | DHCP enabled | DHCP enabled | DHCP enabled | DHCP disabled, static address | DHCP enabled/DNS hard coded |
| Win2003 SP1 | WinXP SP3 | WinXP SP2 | WinXP SP2 | WinXP SP2 | WinXP SP2 |
| 2GB Ram | 1 GB Ram | 1 GB Ram | 1 GB Ram | 2 GB Ram | 2 GB Ram |
| 192.168.1.20 | 192.168.1.13 | 192.168.1.10 | 192.168.1.11 | 192.168.1.101 | 192.168.1.12 |
| 255.255.255.0 | 255.255.255.0 | 255.255.255.0 | 255.255.255.0 | 255.255.255.0 | 255.255.255.0 |
| gateway: 192.168.1.1 (doesn't exist) | gateway: 192.168.1.1 (doesn't exist) | gateway: 192.168.1.1 (doesn't exist) | gateway: 192.168.1.1 (doesn't exist) | N/A | gateway: 192.168.1.1 (doesn't exist) |
| N/A | DHCP Server: 192.168.1.20 | DHCP Server: 192.168.1.20 | DHCP Server: 192.168.1.20 | N/A | DHCP Server: 192.168.1.20 |
| N/A | DNS Server: 192.168.1.20 | DNS Server: 192.168.1.20 | DNS Server: 192.168.1.20 | DNS Server: 192.168.1.20 | DNS Server: 192.168.1.20 |
| N/A | Wins Server: 192.168.1.20 | Wins Server: 192.168.1.20 | Wins Server: 192.168.1.20 | N/A | Wins Server: 192.168.1.20 |
| Conexant 56k modem | N/A | N/A | N/A | N/A | N/A |
| 3.5 floppy disk | 3.5 floppy disk | 3.5 floppy disk | 3.5 floppy disk | 3.5 floppy disk | 3.5 floppy disk |
| cd drive | RW/DVD | RW/DVD | RW/DVD | RW/DVD | RW/DVD |
| tape drive | N/A | N/A | N/A | N/A | N/A |
| com1/com2/lpt1 | com1/com2/lpt1 | com1/com2/lpt1 | com1/com2/lpt1 | com1/com2/lpt1 | com1/com2/lpt1 |
| Dell PowerVault 100T DAT72 Tape drive | N/A | N/A | N/A | Zip Drive | Zip Drive |
| | | | | | |
| Remote Desktop Enabled. Allowed users ELECTIONS\SBS Remote Operators | Remote Assistance is enabled | Remote Assistance is enabled | Remote Assistance is enabled | Remote Assistance is enabled | Remote Assistance is enabled |
| No Automatic Updates Allowed | No Automatic Updates Allowed | No Automatic Updates Allowed | No Automatic Updates Allowed | Nothing is selected for Auto Updates | Auto Updates enabled for 3:00AM daily |
| Enterprise Symatec A/V installed and running, password protected | Symantec A/V: Parent Server BOE Definition File 5/8/2006 Rev. 35 | Symantec A/V: Parent Server BOE Definition File 5/8/2006 Rev. 35 | Symantec A/V: Parent Server BOE Definition File 5/8/2006 Rev. 35 | N/A | N/A |
| Windows Firewall is off, ICS service not running | Windows Firewall is off | Windows Firewall is off | Windows Firewall is off | Windows Firewall is on | Windows Firewall is on |
| **Physical Connections:** | **Physical Connections:** | **Physical Connections:** | **Physical Connections:** | **Physical Connections:** | **Physical Connections:** |
| ethernet | ethernet | ethernet | ethernet | ethernet | ethernet |
| ps/2 mouse | usb mouse | usb mouse | usb mouse | usb mouse | usb mouse |
| ps/2 keyboard | usb keyboard | usb keyboard | usb keyboard | usb keyboard | usb keyboard |
| monitor | monitor | monitor | monitor | monitor | monitor |
| | | External Zip drive | | | |
| power cord connected to APC Battery Backup | power cord | power cord | power cord | power cord | power cord |
| | Serial connection to the ESS (Elections System&Software) Hub. This is the cardridge that the voter data is on | Serial connection to the ESS (Elections System&Software) Hub. This is the cardridge that the voter data is on | Serial connection to the ESS (Elections System&Software) Hub. This is the cardridge that the voter data is on | Serial Bus connection going to a bank of v.92 modems - some are powered on | Serial Bus connection going to a bank of v.92 modems - some are powered on |

"Air Gap" Analysis – No Issues Found

### No External Connections Found

The only outside connections found on the network were the dial-up modems on the DAM servers which are part of the application. No other external connections were found on the network. The 7 connections on the Dell 2716 switch were traced to valid devices. No other cables were connected to the Dell Switch and no loose cables were observed in the vicinity of the switch. solutions4networks asked if there was a valid login for the Dell 2716 switch but was told that no one was aware of one.

### No Wireless Adapters or Bluetooth Capability Found on Client Devices

Each PC was physically inspected for the presence of a wireless adapter or Bluetooth adapter and none were found.

The Windows "Device Manager" of each device was also inspected for the presence of any wireless devices.

### No Wireless Keyboards and Mice

The keyboards and mice all had physical wires connected to the computers.

Post-Election Review: All items indicated above remained the same.

## "Air Gap" Network Intact - Recommendations for Improvement

solutions4networks did not find any problems with the Election Tabulation Network, but have these recommendations to improve security of the network:

### Client Operating Systems – Update the Clients to a supported OS.

The clients PC's were found to be running Windows XP which is no longer supported by Microsoft. These may be more vulnerable to attack if the network was compromised. The clients also had their internal Firewall disabled. They did have Symantec Anti-virus installed, but the definitions were out of date.

### Server Operating System – Update the Server Operating System.

The server operating system is running Windows Server 2003, which is end of life July 2015. Any OS that is end of life is more vulnerable to attack if the network is compromised as it is no longer updated with any security patches.

### Remote Assistance Enabled.

Remote Assistance is enabled on the 3 clients and 2 DAM servers. This serves no positive purpose in a closed network environment where each machine is physically accessible and should be disabled in the event the network is compromised.

### Remote Desktop is Enabled.

Remoted Desktop is enabled on the BOE server. Once again this does not serve any positive purpose in a closed local network and should be disabled in the event the network may be compromised.

### Windows Update Enabled/None Selected.

The two DAM servers are configured differently from the rest of the computers on the network. Consistency should be the norm. All other computers have Auto Updates turned off. DAM1 has nothing selected and DAM2 has Auto Updates enabled and set for 3:00AM.

### Lock Physical Access to the Dell PowerConnect 2716

The Dell switch is easily accessible on the countertop. A locked cabinet would make it more difficult to connect an external cable. It is also recommended to disable any unused ports on the Dell Switch or move the unused ports to a different VLAN from the production network.

### Remove the Default Gateway Option

The DHCP server is giving the clients a default gateway of 192.168.1.1 even though no device exists. Removing the default gateway completely would make it more difficult for the clients to communicate with external networks. There is some inconsistency on the network in that not all of the clients are set up for DHCP. Either set them all up for DHCP or set them all up for Static. For a more secure environment it would be better to disable DHCP on the BOE server entirely and configure static IPs on all of the clients that way if someone were to ever connect to the Dell switch they would never obtain a DHCP address but would have to know the network addressing to hard code their PC.