STATE OF MICHIGAN

IN THE CIRCUIT COURT FOR THE COUNTY OF ANTRIM

WILLIAM BAILEY Plaintiff	Case No. 20-9238-CZ
v.	
ANTRIM COUNTY Defendant,	HON. KEVIN A. ELSENHEIMER
SECRETARY OF STATE JOCELYN BENSON Intervenor-Defendant,	

Matthew S. DePerno (P52622)
DEPERNO LAW OFFICE, PLLC
Attorney for Plaintiff
951 W. Milham Avenue
PO Box 1595
Portage, MI 49081
(269) 321-5064

Haider A. Kazim (P66146)
CUMMINGS, MCCLOREY, DAVIS & ACHO, PLC
Attorney for Defendant
319 West Front Street
Suite 221
Traverse City, MI 49684
(231) 922-1888

Heather S. Meingast (P55439)
Erik A. Grill (P64713)
Assistant Attorneys General
Attorneys for Proposed Intervenor-Defendant Benson
PO Box 30736
Lansing, MI 48909
(517) 335-7659

AFFIDAVIT OF BENJAMIN R. COTTON 8 JUNE 2021

I, Ben Cotton, being duly sworn, hereby depose and state as follows:

1) I am over the age of 18, and I understand and believe in the obligations of an oath. I make this affidavit of my own free will and based on first-hand information and my own personal observations.

2) I am the founder of CyFIR, LLC (CyFIR).

3) I have a master's degree in Information Technology Management from the University of Maryland University College. I have numerous technical certifications, including the Certified Information Systems Security Professional (CISSP), Microsoft Certified Professional (MCP), Network+, and Certified CyFIR Forensics and Incident Response Examiner.

4) I have over twenty-five (25) years of experience performing computer forensics and other digital systems analysis.

5) I have over eighteen (18) years of experience as an instructor of computer forensics and incident response. This experience includes thirteen (13) years of experience teaching students on the Guidance Software (now OpenText) EnCase Investigator and EnCase Enterprise software.

6) I have testified as an expert witness in state and federal courts and before the United States Congress.

7) I regularly lead engagements involving digital forensics for law firms, corporations, and government agencies.

8) In connection with this legal action I have had the opportunity to examine the following devices:

a) Antrim County Election Management Server Image. This image was acquired on 4 December 2020 by a firm named Sullivan and Strickler.

b) Thirty-eight (38) forensic images of the compact flash cards used in Antrim County during the November 2020 elections that were imaged on 4 December 2020 by a firm named Sullivan and Strickler.

c) One (1) SID-15v-Z37-A1R, commonly known as the Image Cast X (ICX), that was used in the November 2020 elections.

d) Two (2) thumb drives that were configured for a precinct using the ES&S DS400 tabulator that were used during the November 2020 election.

e) One ES&S server that was used in the November 2020 election.

9) **Internet Communications with the Dominion ICX.** I examined the forensic image of a Dominion ICX system utilized in the November 2020 election and discovered evidence of internet communications to a number of public and private IP addresses. Of specific concern was the presence of the IP address 120.125.201.101 in the unallocated space of the 10th partition of the device. This IP address resolves back to the Ministry of Education Computer Center, 12F, No 106, Sec.2,Hoping E. Rd.,Taipei Taiwan 106. This IP address is contextually in close proximity to data that would indicate that it was part of the socket configuration and stream of an TCP/IP communication session. Located at physical sector 958273, cluster 106264, sector offset 256, file offset 54407424 of the storage drive, the unallocated nature of the artifact precludes the exact definition of the date and time that this data was created. Also located in close proximity to the Ministry of Education IP address is the IP address 62.146.7.79. This IP address resolves to a cloud provider in Germany.

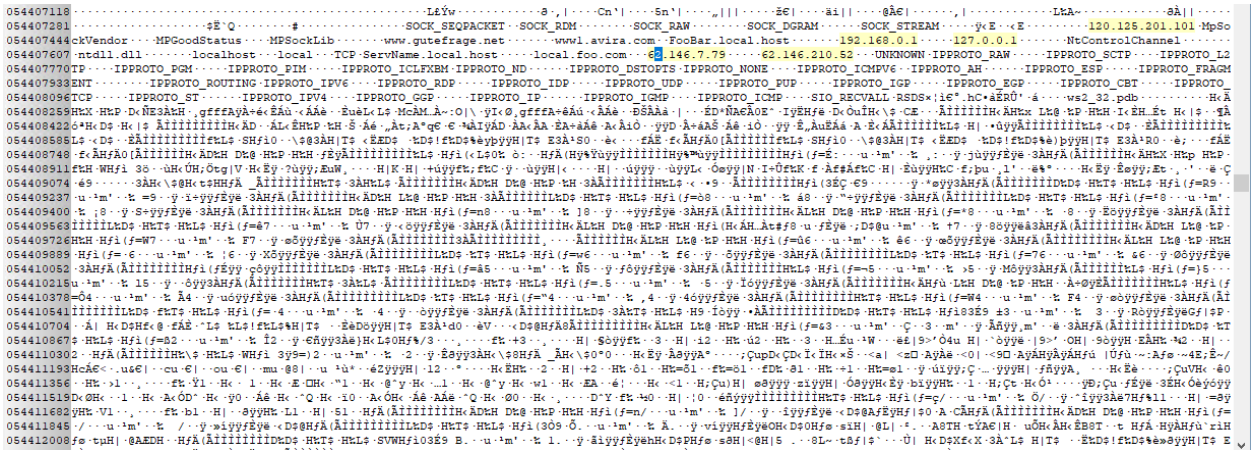


Figure 1-IP Addresses Located in Unallocated Space

Further examination of the ICX clearly indicates that this system is also actively configured to communicate on a private network of 10.114.192.x with FTP settings to connect to 10.114.192.12 and 10.114.192.25. Also apparent is that at one time this system was configured to have the IP address 192.168.1.50. This IP address is also a private IP range. These IP configurations and artifacts definitively identify two things, 1) the device has been actively used for network communications and 2) that this device has communicated to public IP addresses not located in the United States. Further analysis and additional devices would be required to determine the timeframe of these public IP communications.

10) **ESS DS400 Communications.** A careful examination of the ESS DS400 devices and thumb drives was conducted. This examination proved that each DS400 had a Verizon cellular wireless communications card installed and that the card was active on powerup, which meant that there is the ability to connect to the public internet on these devices as well. Both of the DS400 devices were configured to transmit election results to IP address 10.48.51.1. This is a private network, which means that it would only be accessible by the remote DS400 systems through leveraging the public internet and establishing a link to a communications gateway using a public IP or via a virtual private network (VPN). It is important to understand that this

communication can only occur if the cellular modems have access to the public internet. I did not have the entire communications infrastructure for the private network and given this lack of device production associated with the DS200, I cannot say which other devices may have connected to this private network nor the full extent of the communications of nor the remote accesses to the DS400 devices.

11) Contrary to published guidelines and best practices for computer security, a single password was shared for the EMSADMIN01, EMSADMIN, EMSUSER, ICCUSER01, ICCUSER02, and emsepsuser. These passwords were never changed from the time that they were created. There were two local administrative accounts that did not have a password. The security impacts of shared passwords and no passwords on computer security is well documented and dramatically increases the risk of unauthorized access. It is inconceivable that a system would have shared passwords or null passwords and still meet accreditation standards.

12) Contrary to published guidelines and best practices for sensitive systems, the hard disks on the Antrim EMS were not encrypted. This failure to follow best practices increases the vulnerability of the voter data and facilitates the easy of access to sensitive data for unauthorized users and should invalidate any accreditation of the system.

13) **Microsoft SQL Authentication was Set to Authenticate to Windows User Mode.**

This is a significant breach of sound practice for accessing the Microsoft SQL server. Simply put if an unauthorized user gains access to the system, that unauthorized user would have complete access to the Microsoft SQL server at the level of the compromised user. Given that the administrative accounts for the Antrim EMS server either used a shared password or did not have a password, full access to the SQL server would have resulted, exposing the contents of the database and the election results to manipulation by an unauthorized user.

14) **Out of Date Security Updates and Virus Definitions.** An analysis of the operating system and antivirus settings on the servers and computers provided to me was conducted. It was immediately apparent that these systems were extremely vulnerable to unauthorized remote access and manipulation. For example, none of the operating systems had been patched nor the antivirus definition files updated for years. The Antrim EMS operating system was last updated on 04/10/2019. Furthermore when the operating system was updated on 4/10/2019 the user did not apply the most recent patches, instead used a the 10.9.1 patch which was already 15 patches behind at that point in time. It is important to understand that these patches are critical to fixing vulnerabilities and protecting the system from unauthorized access. The fact that the operating system was not fully patched increases the dependency on the endpoint antivirus to protect the system. In this case however, the antivirus definitions were even more outdated than the operating system. The Antrim EMS was leveraging Windows Defender as the antivirus. The Windows Defender antivirus definition files were last updated on 7/16/2016. Given that this date matches the operating system installation date, the Windows Defender antivirus definitions had NEVER been updated after the system was installed. The other systems were in a similar state. This lack of security updating and basic cyber security practices has left these systems in an extremely vulnerable state to remote manipulation and hacking. Since 2016 more than ninety seven (97) critical updates have been issued for the Windows 10 operating system to prevent unauthorized access and hacking and weekly updates have been issued for the Windows Defender antivirus program. The fact that these systems are in such a state of vulnerability, coupled with the obvious public and private internet access, calls the integrity of the voting systems into question and should have negated the system accreditation.

15) **The Antrim EMS Server was Remotely Logged Into by Anonymous Logon.** The Antrim EMS failed to maintain windows security event logs before 4 November 2020. Consequently a full user logon activity analysis was not possible to perform. However, within the logs that were present on the system there were at least two successful logins to the EMS server by an Anonymous user. The first occurred on 11/5/2020 at 5:55:56 PM and the second occurred on 11/17/2020 at 5:16:49 PM EST. Both of these logons appeared to have escalated privileges at the time of logon. Given that this computer was supposed to be on a private network, this is very alarming. One would expect that any network logon, if authorized by the accreditation authority, would require specific usernames and passwords to be utilized, not anonymous users. Given the vulnerable state of the operating system and antivirus protections, this apparent unauthorized access is particularly alarming and certainly would not have been authorized on an accredited system.

16) **Opposing Counsel's Expert Validates the Weak Security Findings.** The Halderman report dated March 26, 2021 relating to this matter validates these findings. It also validates that the system is in a state such that an unauthorized user can easily bypass the passwords for the system and database to achieve unfettered access to the voting system in a matter of minutes. These manipulations and password bypass methodologies can be performed remotely if the unauthorized user gains access to the system through the private network or the public internet.

17) **Incomplete Compliance with the Subpoena for Digital Discovery.** Antrim County has apparently failed to produce all of the voting equipment for digital preservation and analysis. I examined the purchase documents produced by Antrim County with respect to the purchase of the Dominion Voting system and note that the following system components listed on the purchase documents were not produced:

(a) ImageCast Listener Express Server

(b) ImageCast Express Firewall

(c) EMS Express Managed Switch

(d) ICP Wireless Modems (17)

(e) Image Cast Communications Manager Server

(f) ImageCast Listener Express RAS (remote access server) System

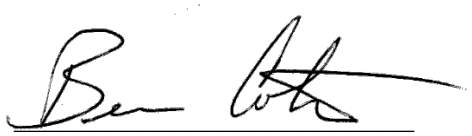
(g) ImageCast USB Modems (5)

(h) Network Netflow Data

(i) Router Configuration Data and Logs

Without these additional items and system components it will be impossible to determine the extent of public/private communications and the extent to which the proven anonymous remote access to the voting system components may have impacted the Antrim EMS databases and election results.

SIGNED UNDER THE PAINS AND PENALTIES OF PERJURY THIS 8th DAY OF June 2021.



Benjamin R. Cotton