STATE OF MICHIGAN
IN THE CIRCUIT COURT FOR THE COUNTY OF ANTRIM

WILLIAM BAILEY

Plaintiff

Case No. 20-9238-CZ

v.

ANTRIM COUNTY

HON. KEVIN A. ELSENHEIMER

Defendant

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

Timothy M. Perrone (P37940)
COHL, STOKER & TOSKEY, PC
Attorney for Livingston County Clerk
601 N. Capitol Ave.
Lansing, MI 48933
(517) 372-9000

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

Christopher D. Tholen (P76948)
GRAND TRAVERSE COUNTY, DEPUTY COUNSEL
Attorney for Grand Traverse County Clerk
324 Court Street
Traverse City, MI 49684
(231) 922-4600

Allan C. Vander Laan (P33893)
Kristen L. Rewa (P74043)
CUMMINGS, MCCLOREY, DAVIS & ACHO, PLC
Attorney for Barry County Clerk
2851 Charlevoix Drive SE, Ste. 327
Grand Rapids, MI 48546
(616) 975-7470

Frank Krycia (P35383)
MACOMB COUNTY, CORPORATION COUNSEL
Attorney for Macomb County Clerk
One S. Main, 8th Floor
Mount Clemens, MI 48043
(586) 469-6346

EXHIBITS 5-10

PLAINTIFF'S COLLECTIVE RESPONSE TO DEFENDANTS' and NON-PARTY COUNTIES' MOTIONS TO QUASH AND FOR PROTECTIVE ORDERS

Respectfully submitted

DePERNO LAW OFFICE, PLLC

Dated: April 9, 2021

/s/ Matthew S. DePerno
Matthew S. DePerno (P52622)
Attorney for Plaintiff

Exhibit 5

Barry County GOP resolution

BARRY COUNTY ELECTION INTEGRITY RESOLUTION

WHEREAS...all election violations (or potential violations) must be revealed, investigated, monitored, enforced and legally challenged through each County's administration;

WHEREAS...a "Constitutional Oath of Office" is required of all County governmental officials, employees, or those in service of the government, to secure loyalty of Constitutional law;

WHEREAS...,violations were clearly observed in Michigan during the November 3rd, 2020 election: i. e. TCF Center (Detroit) poll watchers and challengers overview was totally blocked; illegal mail-in ballots were counted by the thousands; hundreds of sworn witness affidavits of election fraud were totally ignored and MOST DISTURBING, *Dominion Voting Machines* were likely programmed to favor candidate Joe Biden;

WHEREAS...officials of the November 3rd, 2020 election in Antrim County, Michigan observed 6,000 votes for President Donald J. Trump AUTOMATICALLY switched to candidate Joe Biden;

WHEREAS...the Antrim County, Michigan Judge Elsenheimer authorized the release of a "Forensic Audit Report of Dominion Voting Systems", investigated and authored by the Allied Security Operations Group (ASOG);

WHEREAS...ASOG concluded: *"Dominion Voting System is INTENTIONALLY and PURPOSEFULLY designed with inherent errors to create systemic fraud to influence election results."* ;

WHEREAS...President Trump's personal attorney *Sidney Powell* stated, *Dominion Voting Systems* intentionally provided access to foreign infrastructures, for them to "*monitor and manipulate elections*";

WHEREAS...advocates claim *Dominion Voting System* and their partner *Smartmatic Software,* were developed, manufactured and distributed by dubious entities;

WHEREAS…*Dominion Voting Systems* is the election service contracted by Barry County for 10 years (2 years ago), which allows potential for manipulation and/or control of voting results for the next 8 years;

WHEREAS…*Dominion Voting Systems* are potentially a severe threat to the integrity, liberty and sovereignty of future elections for Barry County citizens;

WHEREAS…the next election will be in the year 2022. Barry County voters demand accurate and transparent election data results from *Dominion Voting Systems* to satisfy voter's desire for election integrity;

WHEREAS…the citizens of Barry County have lost confidence in future elections while *Dominion Voting Systems* remain in question and unchecked;

WHEREAS…the fiscal costs of a complete "forensic audit" of all *Dominion Voting Machines* of Barry County would be too burdensome for the County taxpayer and budget;

WHEREAS…the future of election stability in Barry County is endangered and will be until election integrity is confirmed and/or restored;

LET IT BE RESOLVED… "The Barry County GOP formally requests the Barry County Board of Commissioners select 4 to 6 voter precincts in various Townships throughout Barry County. Monitor and oversee a physical recount of paper ballots as compared to the *Dominion Voting Machine's* "tabulated" results. If the data from the two sources are compatible in each precincts, voter confidence will have been restored. If the data is not compatible, election integrity remains endangered, suggesting official activity is needed to restore voter confidence."

Exhibit 6

James Penrose report

April 9, 2021

Analyst: James Thomas Penrose, IV
Report Title: Preliminary Assessment of Wireless Communications Technology for Michigan Voting Systems

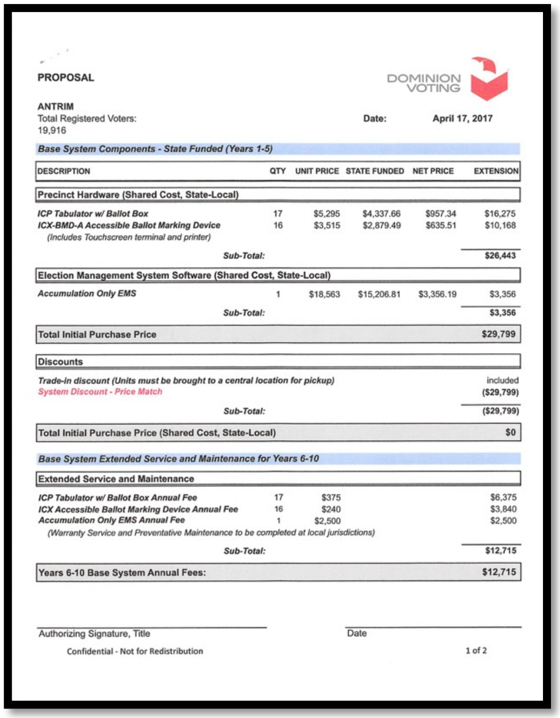
Executive Summary

Two versions of Michigan voting systems both Dominion and ESS have been found to have utilized wireless technology. The Dominion Voting Systems proposal for Antrim County shows a quote for wireless transmission capabilities, see Figure 1. Dominion representatives also confirmed issues with wireless transmission of vote totals and even went as far as disabling the saving of ballot images without explicit authorization.

The ESS Model DS200 was found to have an internal wireless card, that has a private network address that was designed to communicate with an ES&S Primary Host Server. These devices and servers are ostensibly designed to operate on a virtual private network (VPN) that does not allow routing to the Internet. While each of the devices do have private network Internet Protocol (IP) addresses, testing revealed that the SIM card used for the DS200 could be utilized in a generic device 4G wireless device and allow for access to the same access point name (APN). There is substantial risk to the ES&S APN connected machines from malicious actors that have access to any SIM card with pre-programmed access to the APN.

The manufacturer of the wireless 4G card used in the ES&S DS200 is a company named Telit. Telit is an internet of things company that has recently taken major investment from a Chinese investment fund that has ties to the Chinese Communist Party according to UK media reporting.

Antrim County Proposal for Wireless Results Transmission



PROPOSAL

DOMINION VOTING

ANTRIM
Total Registered Voters:
19,916

Date: April 17, 2017

Base System Components - State Funded (Years 1-5)

DESCRIPTION	QTY	UNIT PRICE	STATE FUNDED	NET PRICE	EXTENSION
Precinct Hardware (Shared Cost, State-Local)					
ICP Tabulator w/ Ballot Box	17	$5,295	$4,337.66	$957.34	$16,275
ICX-BMD-A Accessible Ballot Marking Device *(Includes Touchscreen terminal and printer)*	16	$3,515	$2,879.49	$635.51	$10,168
Sub-Total:					$26,443
Election Management System Software (Shared Cost, State-Local)					
Accumulation Only EMS	1	$18,563	$15,206.81	$3,356.19	$3,356
Sub-Total:					$3,356
Total Initial Purchase Price					$29,799
Discounts					
Trade-in discount (Units must be brought to a central location for pickup)					included
System Discount - Price Match					($29,799)
Sub-Total:					($29,799)
Total Initial Purchase Price (Shared Cost, State-Local)					$0

Base System Extended Service and Maintenance for Years 6-10

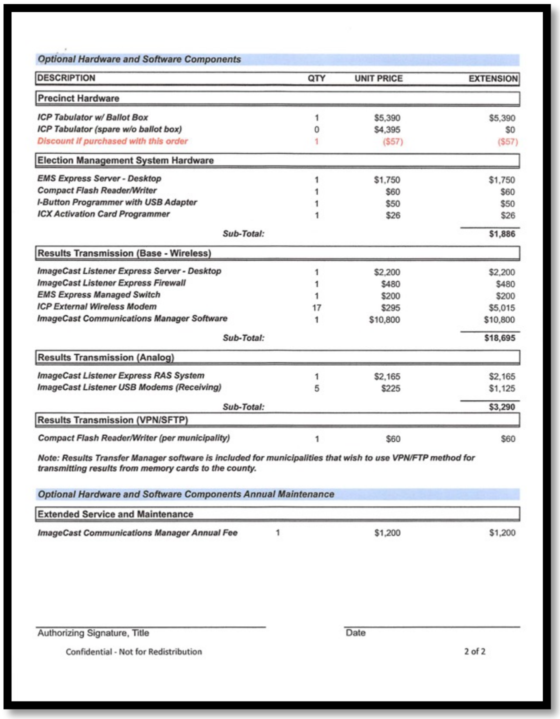
DESCRIPTION	QTY	UNIT PRICE	EXTENSION
Extended Service and Maintenance			
ICP Tabulator w/ Ballot Box Annual Fee	17	$375	$6,375
ICX Accessible Ballot Marking Device Annual Fee	16	$240	$3,840
Accumulation Only EMS Annual Fee *(Warranty Service and Preventative Maintenance to be completed at local jurisdictions)*	1	$2,500	$2,500
Sub-Total:			$12,715
Years 6-10 Base System Annual Fees:			$12,715

Authorizing Signature, Title

Date

Confidential - Not for Redistribution

1 of 2



Optional Hardware and Software Components

DESCRIPTION	QTY	UNIT PRICE	EXTENSION
Precinct Hardware			
ICP Tabulator w/ Ballot Box	1	$5,390	$5,390
ICP Tabulator (spare w/o ballot box)	0	$4,395	$0
Discount if purchased with this order	1	($57)	($57)
Election Management System Hardware			
EMS Express Server - Desktop	1	$1,750	$1,750
Compact Flash Reader/Writer	1	$60	$60
I-Button Programmer with USB Adapter	1	$50	$50
ICX Activation Card Programmer	1	$26	$26
Sub-Total:			$1,886
Results Transmission (Base - Wireless)			
ImageCast Listener Express Server - Desktop	1	$2,200	$2,200
ImageCast Listener Express Firewall	1	$480	$480
EMS Express Managed Switch	1	$200	$200
ICP External Wireless Modem	17	$295	$5,015
ImageCast Communications Manager Software	1	$10,800	$10,800
Sub-Total:			$18,695
Results Transmission (Analog)			
ImageCast Listener Express RAS System	1	$2,165	$2,165
ImageCast Listener USB Modems (Receiving)	5	$225	$1,125
Sub-Total:			$3,290
Results Transmission (VPN/SFTP)			
Compact Flash Reader/Writer (per municipality)	1	$60	$60

Note: Results Transfer Manager software is included for municipalities that wish to use VPN/FTP method for transmitting results from memory cards to the county.

Optional Hardware and Software Components Annual Maintenance

DESCRIPTION	QTY	UNIT PRICE	EXTENSION
Extended Service and Maintenance			
ImageCast Communications Manager Annual Fee	1	$1,200	$1,200

Authorizing Signature, Title

Date

Confidential - Not for Redistribution

2 of 2

Figure 1

Dominion Voting Systems ICX

In Michigan, the Dominion Voting Systems ICX is used to allow for touchscreen voting for disabled voters. During the forensics examination of an ICX machine there were two IP addresses discovered in unallocated space on the hard drive of the Linux operating system. The existence of these IPs in unallocated space implies the ICX had previous communication with one or both of the IPs.

The first IP address was: 120.125.201.101. This IP address is registered to Ministry of Education Computer Center located in Taipei, Taiwan.

The second IP address was: 62.146.7.95. This IP address is registered to EDV-BV GmbH QSC Subkunde located in Nurenberg, Germany.

The ICX machine itself appears to be manufactured in Taiwan and shipped to the United States via airfreight using China Airlines. See the photos of the shipping box in Figure 2.

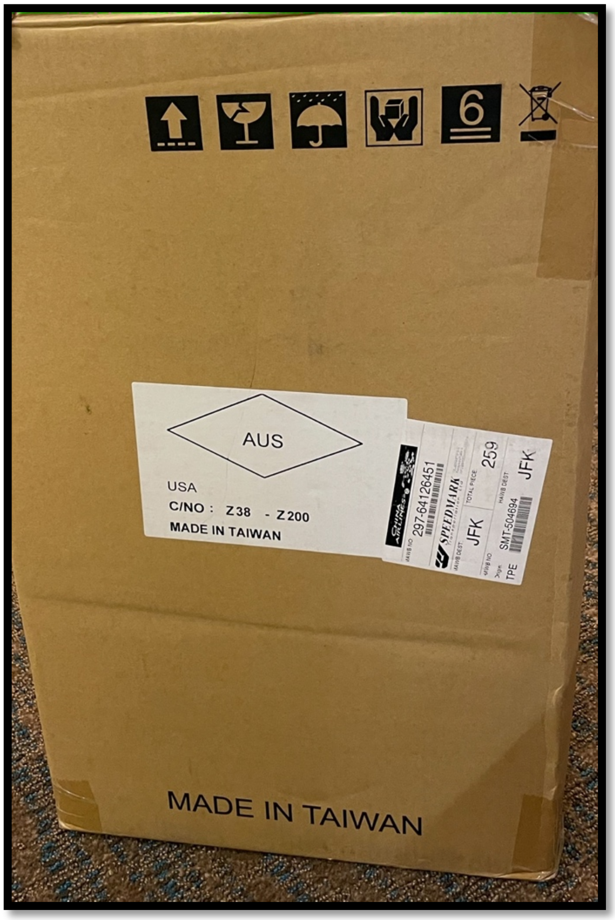
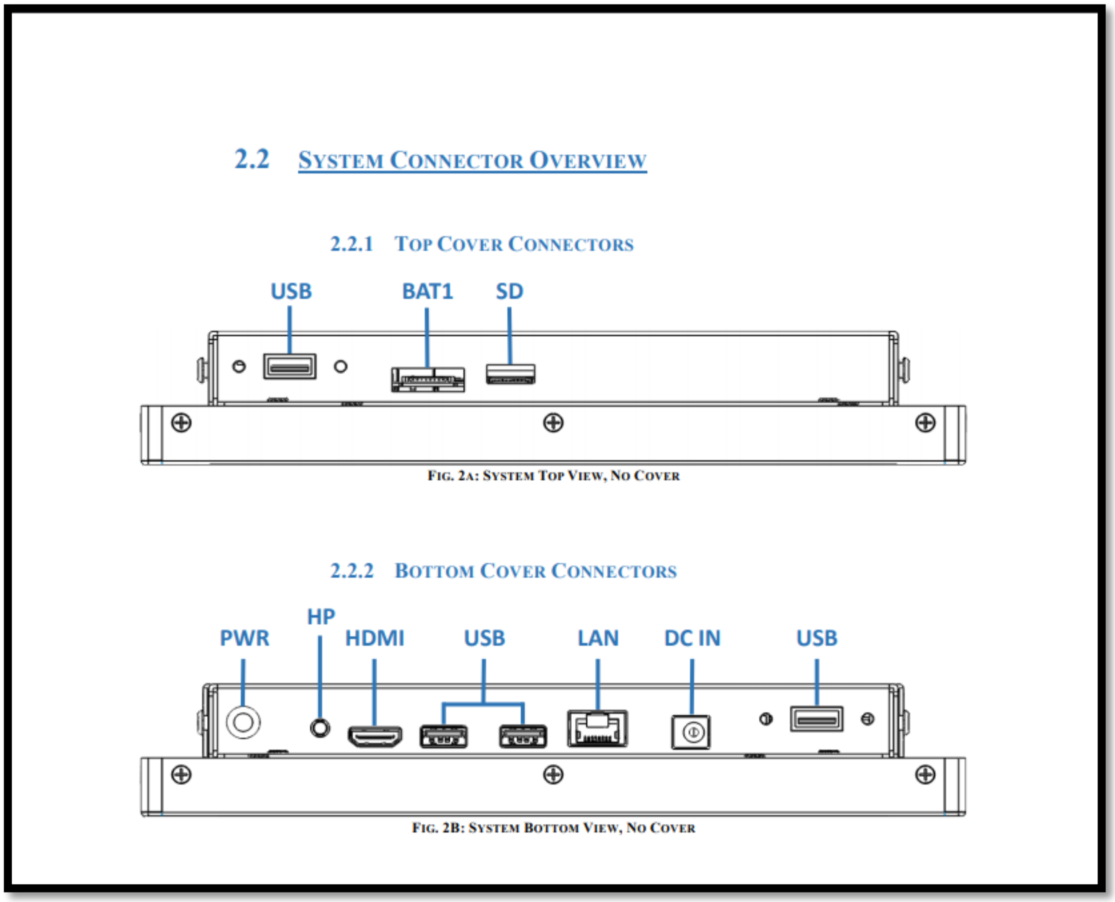


Figure 2

The ICX machine may also utilize an external wireless for communications modem with the central listener server for Dominion Democracy Suite. See the previously listed proposal from Dominion to Antrim County. The manual for the ICX also shows an Ethernet port for wired connectivity, see Figure 3.



2.2 System Connector Overview

2.2.1 Top Cover Connectors

Fig. 2A: System Top View, No Cover

2.2.2 Bottom Cover Connectors

Fig. 2B: System Bottom View, No Cover

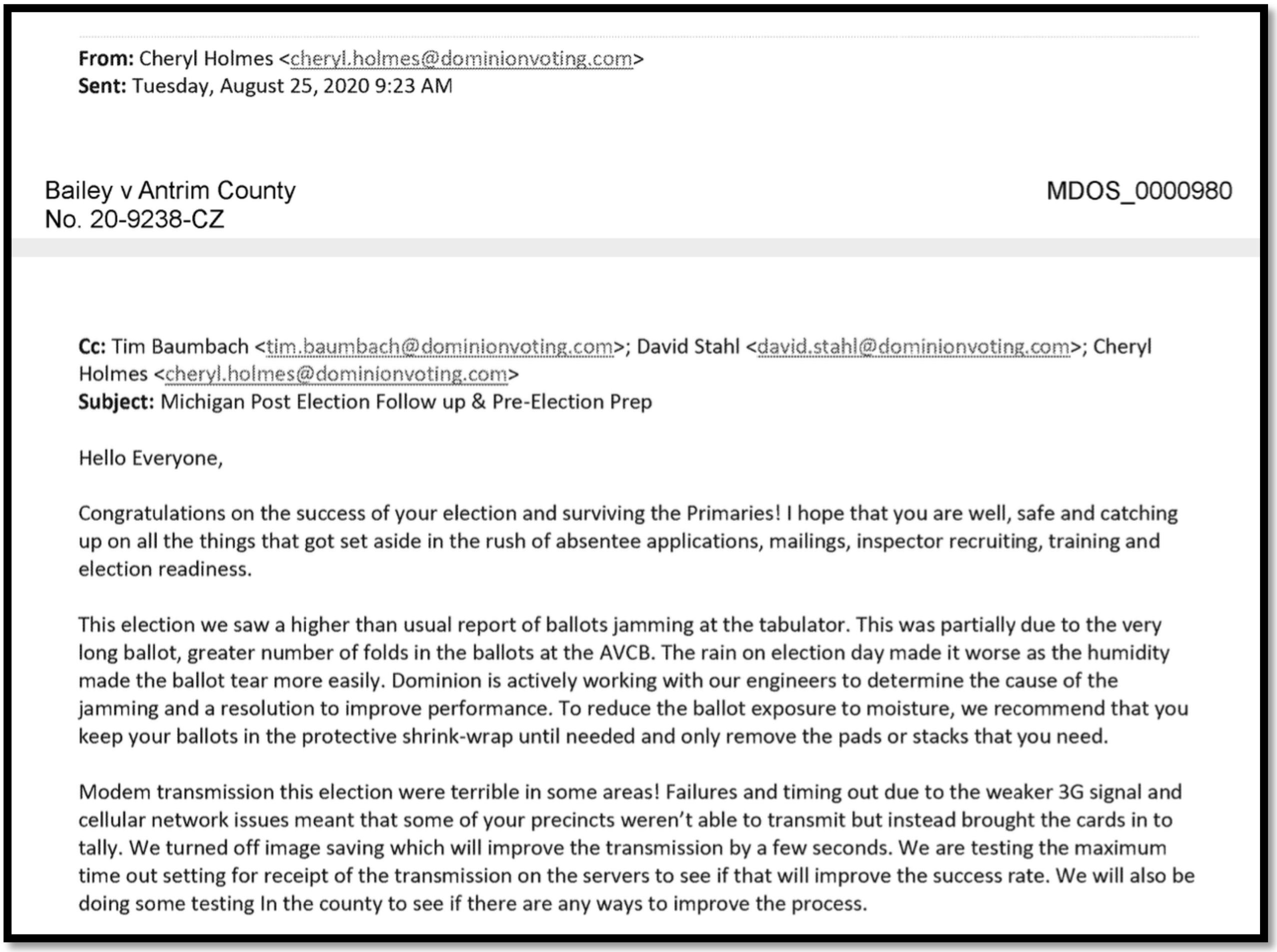
Figure 3

Dominion Summary Email to Michigan Counties

Dominion sent a summary email dated August 25, 2020 (Figure 4) after the primaries describing how the process of running the election went. Notably in this summary email from Cheryl Homes of Dominion Voting Systems she describes the following issues related to the transmission of vote totals via modems. In addition, Dominion turned off image saving without any authorization from the Secretary of State noted in the communication.

> ***"Modem transmission this election were (sic) terrible in some areas! Failures and timing out due to the weaker 3G signal and cellular network issues meant that some of your precincts weren't able to transmit but instead brought the cards in to tally. We turned off image saving which will improve the transmission by a few seconds. We are testing the maximum time out setting for receipt of the transmission on the servers to***

see if that will improve the success rate. We will also be doing some testing In the county to see if there are any ways to improve the process.”



From: Cheryl Holmes <cheryl.holmes@dominionvoting.com>
Sent: Tuesday, August 25, 2020 9:23 AM

Bailey v Antrim County
No. 20-9238-CZ

MDOS_0000980

Cc: Tim Baumbach <tim.baumbach@dominionvoting.com>; David Stahl <david.stahl@dominionvoting.com>; Cheryl Holmes <cheryl.holmes@dominionvoting.com>
Subject: Michigan Post Election Follow up & Pre-Election Prep

Hello Everyone,

Congratulations on the success of your election and surviving the Primaries! I hope that you are well, safe and catching up on all the things that got set aside in the rush of absentee applications, mailings, inspector recruiting, training and election readiness.

This election we saw a higher than usual report of ballots jamming at the tabulator. This was partially due to the very long ballot, greater number of folds in the ballots at the AVCB. The rain on election day made it worse as the humidity made the ballot tear more easily. Dominion is actively working with our engineers to determine the cause of the jamming and a resolution to improve performance. To reduce the ballot exposure to moisture, we recommend that you keep your ballots in the protective shrink-wrap until needed and only remove the pads or stacks that you need.

Modem transmission this election were terrible in some areas! Failures and timing out due to the weaker 3G signal and cellular network issues meant that some of your precincts weren’t able to transmit but instead brought the cards in to tally. We turned off image saving which will improve the transmission by a few seconds. We are testing the maximum time out setting for receipt of the transmission on the servers to see if that will improve the success rate. We will also be doing some testing In the county to see if there are any ways to improve the process.

Figure 4

ESS DS200 Machine

The DS200 machine was found to have a wireless 4G modem installed internally within the enclosure of the machine. The printed tapes that summarize the activity during the election show that the 4G modem was used to send the results to a central listener server via secure file transfer. The Telit LE910-SV1 in Figure 5 was found within the ES&S enclosure.

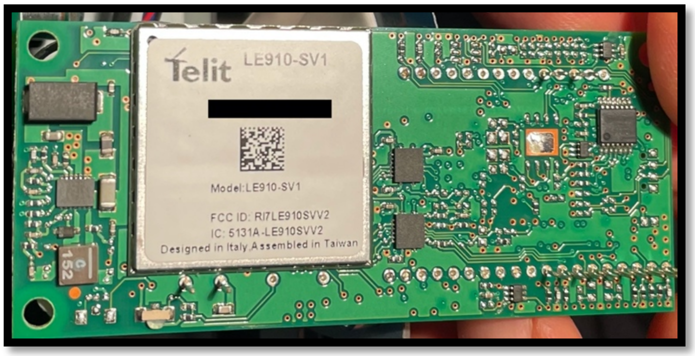
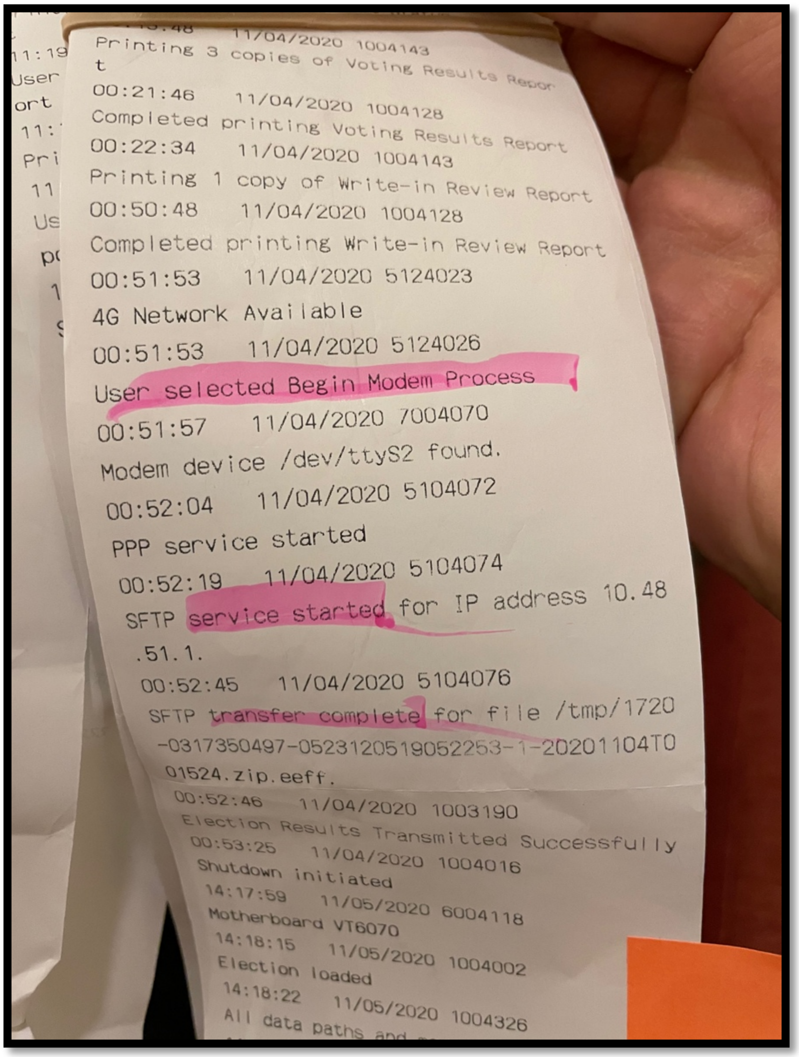


Figure 5

The printed summary tape from the ES&S machines also indicate that the submission of the vote totals occurred using the wireless 4G modem, see Figure 6.



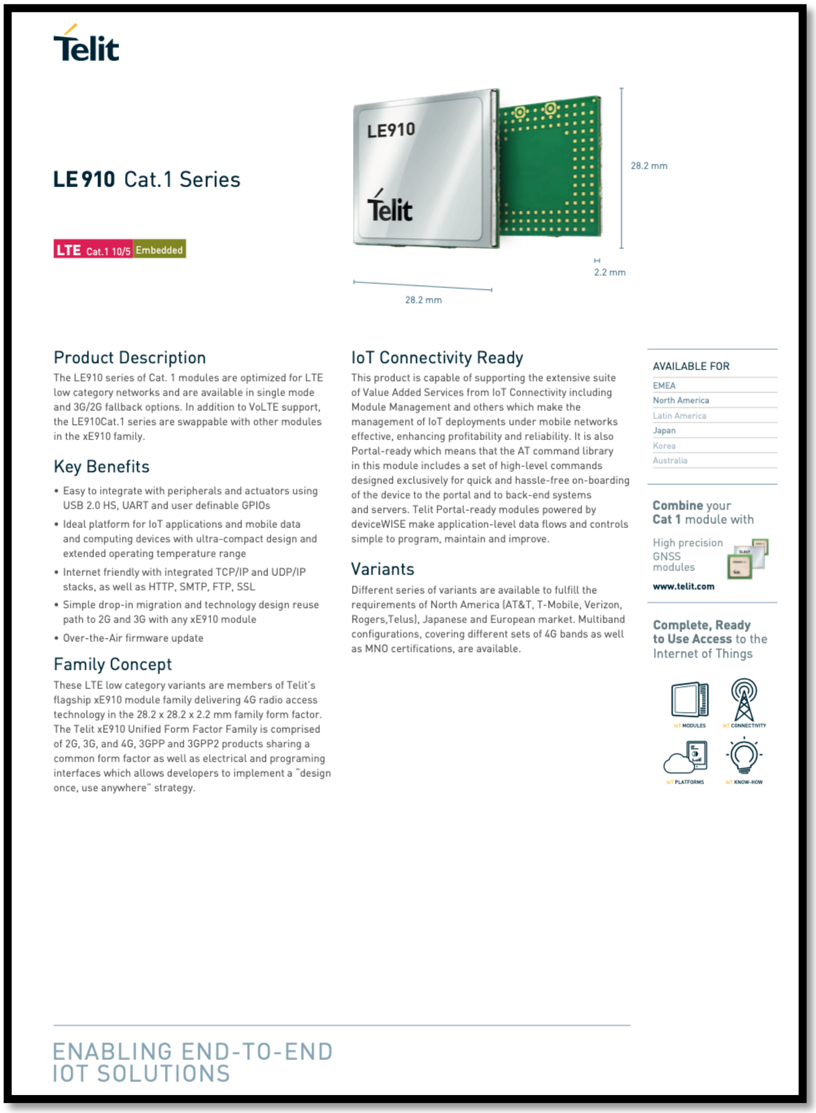
```
          11/04/2020 1004143
Printing 3 copies of Voting Results Repor
t
00:21:46    11/04/2020 1004128
Completed printing Voting Results Report
00:22:34    11/04/2020 1004143
Printing 1 copy of Write-in Review Report
00:50:48    11/04/2020 1004128
Completed printing Write-in Review Report
00:51:53    11/04/2020 5124023
4G Network Available
00:51:53    11/04/2020 5124026
User selected Begin Modem Process
00:51:57    11/04/2020 7004070
Modem device /dev/ttyS2 found.
00:52:04    11/04/2020 5104072
PPP service started
00:52:19    11/04/2020 5104074
SFTP service started for IP address 10.48
.51.1.
00:52:45    11/04/2020 5104076
SFTP transfer complete for file /tmp/1720
-0317350497-0523120519052253-1-20201104T0
01524.zip.eeff.
00:52:46    11/04/2020 1003190
Election Results Transmitted Successfully
00:53:25    11/04/2020 1004016
Shutdown initiated
14:17:59    11/05/2020 6004118
Motherboard VT6070
14:18:15    11/05/2020 1004002
Election loaded
14:18:22    11/05/2020 1004326
All data paths and
```

Figure 6

The Telit LE910-SV1 card installed in the ES&S device was utilizing a commercial Verizon SIM card with an APN configuration specific to the ES&S DS200 provisioning. Testing revealed that the same SIM card could be utilized in a separate wireless hotspot device and the device could then join the same APN as the ES&S voting machines. An unauthorized user could gain access to this APN by an extra SIM card pre-provisioned for this APN, or by removing a SIM from an operational device and using it in another device.

Telit LE910-SV1 Hardware Summary

According to the hardware summary specifications datasheet from Telit, the LE910-SV1 comes standard with "Internet friendly integrated TCP/IP and UDP/IP stacks, as well as HTTP, SMTP, FTP, SSL.” (Figure 7) These features are very useful to application programmers, but are also ripe for abuse by unauthorized users of the APN devoted to the ES&S machines.



Telit

LE910 Cat.1 Series

LTE Cat.1 10/5 Embedded

Product Description

The LE910 series of Cat. 1 modules are optimized for LTE low category networks and are available in single mode and 3G/2G fallback options. In addition to VoLTE support, the LE910Cat.1 series are swappable with other modules in the xE910 family.

Key Benefits

- Easy to integrate with peripherals and actuators using USB 2.0 HS, UART and user definable GPIOs
- Ideal platform for IoT applications and mobile data and computing devices with ultra-compact design and extended operating temperature range
- Internet friendly with integrated TCP/IP and UDP/IP stacks, as well as HTTP, SMTP, FTP, SSL
- Simple drop-in migration and technology design reuse path to 2G and 3G with any xE910 module
- Over-the-Air firmware update

Family Concept

These LTE low category variants are members of Telit’s flagship xE910 module family delivering 4G radio access technology in the 28.2 x 28.2 x 2.2 mm family form factor. The Telit xE910 Unified Form Factor Family is comprised of 2G, 3G, and 4G, 3GPP and 3GPP2 products sharing a common form factor as well as electrical and programing interfaces which allows developers to implement a “design once, use anywhere” strategy.

IoT Connectivity Ready

This product is capable of supporting the extensive suite of Value Added Services from IoT Connectivity including Module Management and others which make the management of IoT deployments under mobile networks effective, enhancing profitability and reliability. It is also Portal-ready which means that the AT command library in this module includes a set of high-level commands designed exclusively for quick and hassle-free on-boarding of the device to the portal and to back-end systems and servers. Telit Portal-ready modules powered by deviceWISE make application-level data flows and controls simple to program, maintain and improve.

Variants

Different series of variants are available to fulfill the requirements of North America (AT&T, T-Mobile, Verizon, Rogers,Telus), Japanese and European market. Multiband configurations, covering different sets of 4G bands as well as MNO certifications, are available.

AVAILABLE FOR

EMEA
North America
Latin America
Japan
Korea
Australia

Combine your
Cat 1 module with

High precision
GNSS
modules

www.telit.com

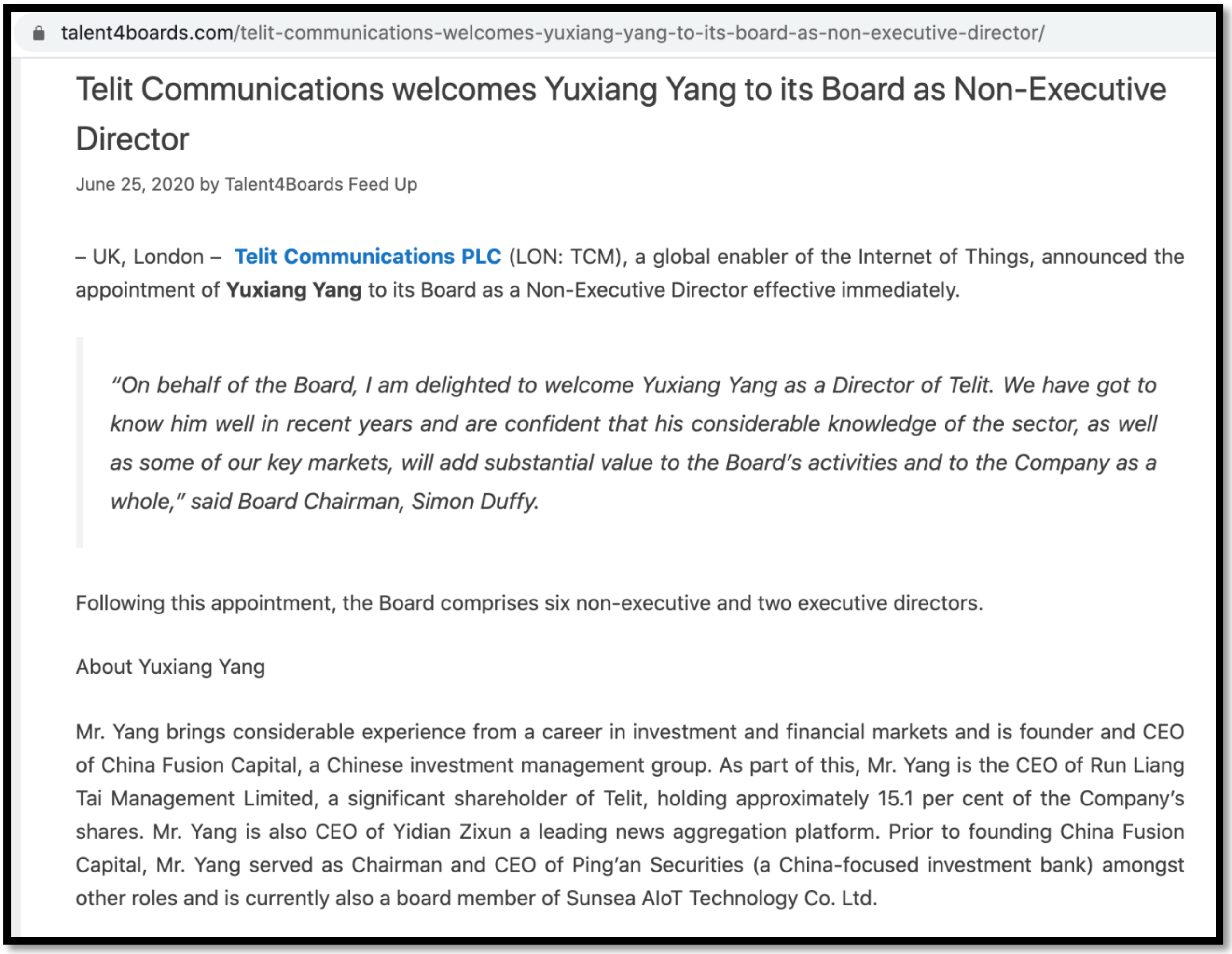
Complete, Ready
to Use Access to the
Internet of Things

ENABLING END-TO-END
IOT SOLUTIONS

Figure 7

Background on Telit

Telit is a publicly traded company Internet of Things (IoT) and Machine to Machine (M2M) company headquartered in London, UK with an operations unit in Trieste, Italy.
In late 2017, Run Liang Tai Management in Hong Kong built a 14 percent stake in Telit. Mr. Yuxiang Yang sits on the board of directors for Telit (see Figure 8) and is CEO of Run Liang Tai Management Limited.



talent4boards.com/telit-communications-welcomes-yuxiang-yang-to-its-board-as-non-executive-director/

Telit Communications welcomes Yuxiang Yang to its Board as Non-Executive Director

June 25, 2020 by Talent4Boards Feed Up

– UK, London – **Telit Communications PLC** (LON: TCM), a global enabler of the Internet of Things, announced the appointment of **Yuxiang Yang** to its Board as a Non-Executive Director effective immediately.

> *"On behalf of the Board, I am delighted to welcome Yuxiang Yang as a Director of Telit. We have got to know him well in recent years and are confident that his considerable knowledge of the sector, as well as some of our key markets, will add substantial value to the Board's activities and to the Company as a whole," said Board Chairman, Simon Duffy.*

Following this appointment, the Board comprises six non-executive and two executive directors.

About Yuxiang Yang

Mr. Yang brings considerable experience from a career in investment and financial markets and is founder and CEO of China Fusion Capital, a Chinese investment management group. As part of this, Mr. Yang is the CEO of Run Liang Tai Management Limited, a significant shareholder of Telit, holding approximately 15.1 per cent of the Company's shares. Mr. Yang is also CEO of Yidian Zixun a leading news aggregation platform. Prior to founding China Fusion Capital, Mr. Yang served as Chairman and CEO of Ping'an Securities (a China-focused investment bank) amongst other roles and is currently also a board member of Sunsea AIoT Technology Co. Ltd.

Figure 8

A media report from August 15, 2020 from the UK online publication *Financial Mail on Sunday* indicated that there were concerns raised about Chinese influence of the Telit firm within the UK government. Here is an excerpt from the news story located here: https://www.thisismoney.co.uk/money/markets/article-8630685/Chinese-close-UK-internet-things-pioneer.html

> ***…The maneuvering by powerful investors comes after secretive Chinese multi-millionaire banker Yuxiang Yang joined Telit's board earlier this summer.***

His appointment may raise concern in Westminster that a Chinese businessman with ties to his country's Communist government could be seeking to gain influence over the business.

Yang runs China Fusion Capital, the parent company of Run Liang Tai Management, a mysterious investment fund that has built a 15 per cent stake in Telit to become its largest shareholder.

Sources said some of the firms that have invested in Run Liang are giant Chinese companies, such as coal mining group Wintime Energy and Jiangsu Shuangliang, a manufacturer of air conditioners and boilers.

Run Liang also owns a stake in Sunsea Telecommunications, a Shenzhen-listed 'internet of things' provider that recently raised around $200million (£1.5million) by issuing shares to Zhjzgroup, a state-backed tourism firm. Yang also sits on the board of Sunsea. Speculation has been mounting that Run Liang is hoping to engineer a merger of some or all of Telit with China-based Sunsea.

Run Liang's move on Telit, which is listed on AIM, follows a period in which several other London-listed businesses have been bought by China-linked firms.

Imagination Technologies was bought by Canyon Bridge – a private equity fund bankrolled by Beijing – in 2017 for £550million. Concerns rose in the spring when Canyon Bridge tried to place four directors from China Reform Holdings on to Imagination's board.

Conservative MPs Tom Tugendhat, who now leads the China Research Group, and David Davis warned that Imagination's intellectual property could be shifted to China.

When asked about Telit, Bob Seely, chairman of the Foreign Affairs Select Committee, said: 'We do need a thorough review of investment security and we need an oversight board for purchases by high-risk vendors or from higher risk states.' Telit, which is due to unveil figures next week, declined to comment.

Exhibit 7

Cyber Ninjas report

4/9/2021

Antrim County, MI

Election Management System
Application Security Analysis

Cyber Ninjas
Phone: (941) 3-NINJAS
Fax: (941) 364-6527
www.CyberNinjas.com
5077 Fruitville Rd #109-421, Sarasota, FL 34232

1 Revision History

Date	Revision	Notes
01/10/2021	DRAFT	Initial Draft Created
01/11/2021	DRAFT	Revision 1.0 Completed
03/13/2021	DRAFT	Additional Findings Added
04/07/2021	DRAFT	Additional Findings
04/08/2021	DRAFT	Revision 2.0 Completed

2 Table of Contents

3 Executive Summary

The Antrim County Election Management System (EMS) environment is setup in a manner where it would potentially be possible for an individual to alter the results of the election without leaving much of a digital trail.

- Users of the computer have enough access rights and the needed tools installed to directly modify election results in the database. Official results are generated from this database.
- The master encryption key utilized to encrypt election results is stored in plain text in the database, and its value exists both at the county and with Election Source. If Election Source was hacked, or this value otherwise got into a malicious actor's hand; it would be possible to create malicious tabulator configurations or alter the result files from tabulators. Either of these could be used to change the results of an election.
- Log levels are such on the system that it would be possible to delete files, delete logs, or the similar; and it would be difficult to have the necessary details available to investigate the incident.
- Application and computer system accounts are generic and shared among multiple individuals making it near impossible to determine who performed an action even if proper logging was in place.
- Hard-coded credentials, failure to use cryptography properly, and other well-known bad practices are utilized throughout the software suggesting that exploitation of the software is very possible. These types of problems are documented to be reoccurring with this EMS going back over 10 years.
- Ballot images are missing from the Compact Flash data, making it difficult to audit how the software interpreted any given ballot.

These types of findings and departures from best practices utilized across multiple industries for over 10 years is inexplicable for a system that is both highly sensitive, and a likely target for nation state activity.

It is highly recommended that all components of the EMS software immediately go through a full code-review audit to determine the extent of the problems encountered and how easily other areas of the application may be exploitable. In addition, it is recommended that the following items be reviewed to have a better understanding of the full impact of some of these findings:

- Election Source should be required to provide a list of all personnel that have access to the Election Definition databases utilized for Antrim County, as well as provide documentation on any controls that are in place to detect and prevent a breach or modification of election data.
    - Should the controls be determined to be insufficient to detect a nation state level attack, at a bare minimum; all Michigan election projects, and compact flash cards should be forensically imaged and reviewed to determine if any alterations of the data or systems took place.
- Documentation should be requested on the reasoning for installing Microsoft SQL Management Tools onto the EMS Server and who performed this action. This software is not on the EAC's approved list for certified systems, and a legitimate purpose for its installation is not apparent. Yet this software greatly facilitates the changing of database values.
- Copies of the tabulator tape result output for all precincts should be provided, in addition to chain-of-custody documentation showing that these files have been properly cared for and have not been altered. These numbers should then be compared against the numbers read directly from the compact flash cards.
- File definitions should be provided by Dominion for the various results and configuration files held on the compact flash cards, so that the decrypted files can easily be read and confirmed to match the EMS Server and therefore no alteration took place.

4 Scope

Cyber Ninjas was engaged to evaluate the security of the Election Management System (EMS) utilized in Antrim County, MI in order to determine if cyber security related flaws, abuse of functionality, misconfiguration or purposely malicious actions or code could account for the voting irregularities demonstrated in the county during the November 2020 General Election.

A forensic image of the Antrim County Election Management System (EMS) gathered on December 6th, 2020 was converted to a bootable virtual machine. This machine was then utilized to allow the EMS to be utilized in a "live" environment to examine logs, configurations, and functionality of the applications. All analysis was performed within this virtual environment.

5 Background

The following section outlines background details and definitions useful in understanding the overall Election Management System (EMS) architecture and structure, as well as definitions that are utilized throughout the report. Architecture details came from publicly available documentation, as well as reviewing the deployment within Antrim County.

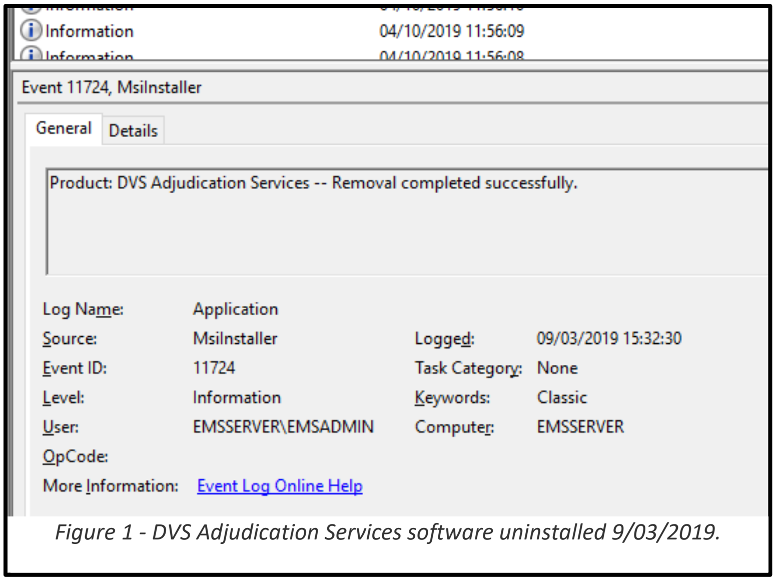
5.1 Architecture

The architecture of the Election Management System (EMS) in Antrim County consisted of one or more ImageCast Precinct (ICP) tabulators and an ImageCast X (ICX) Ballot Marking Device (BMD) at every precinct, as well as the EMS Server that was centrally located at the county. While the ICP devices support a number of different ways to remotely report results, Antrim County stated that they aggregated the results by collecting the compact flash cards and manually importing the results off of these compact flash cards.

5.1.1 Election Management System Server (EMS Server)

The EMS Server is the primary device utilized in Antrim County in order to run an election and serves as the central aggregator for all election results within the county. While the EMS Election Event Designer software can be utilized to build an entire election from scratch, documentation provided indicates that the initial election definition was created by Election Source and exported as a package for Antrim County to then import into their system. This configuration was then utilized by the county in order to build the compact flash cards utilized to configure the ImageCast Precinct (ICP) devices, and after the polls were closed these same compact flash cards were brought back to the EMS in order to attempt to import and publish the results. The EMS software also supports the manual entry of result files.

The EMS Server machine in smaller counties can at times also be utilized as the digital adjudication machine, but this software was not installed on the EMS Server image that was reviewed. Examining the Windows Event Logs shows that the DVS Adjudication Services software had been installed on April 10, 2019; but had later been removed on September 3rd, 2019. This explains the DVS Adjudication logs from 2019 referenced from the ASOG report, and also explains why there were not any adjudication logs for 2020. This is consistent with what the county has reported that all adjudication for 2020 was done manually.



Information 04/10/2019 11:56:09

Information 04/10/2019 11:56:08

Event 11724, MsiInstaller

Product: DVS Adjudication Services -- Removal completed successfully.

Log Name: Application

Source: MsiInstaller

Logged: 09/03/2019 15:32:30

Event ID: 11724

Task Category: None

Level: Information

Keywords: Classic

User: EMSSERVER\EMSADMIN

Computer: EMSSERVER

OpCode:

More Information: Event Log Online Help

Figure 1 - DVS Adjudication Services software uninstalled 9/03/2019.

5.1.2 IMAGECAST X (ICX) - BALLOT MARKING DEVICE (BMD)

ImageCast X (ICX) Ballot Marking Devices (BMD) are primarily utilized in Antrim County in order to support accessibility voting. With these devices an individual can vote via a touch screen or a number of specialized input devices, and this in turn prints out a ballot with a QR code which can then be fed into the ImageCast Precinct (ICP) tabulators where the votes are tabulated. These devices are configured utilizing USB drives created from the EMS Server.

5.1.3 IMAGECAST PRECINCT (ICP) – PRECINCT TABULATOR

ImageCast Precinct (ICP) devices are designed to handle the tabulation of ballots at a precinct level. These devices support both a standard hand-filled out bubble ballot, as well as the QR coded ballots created by the ICP device. As votes are cast the results are written simultaneously to two compact flash cards for redundancy. One of these compact flash cards also holds all the configuration for the ICP device. This configuration tells the ICP how to read and understand the various ballot types for the election. These compact flash cards are built on the EMS Server.

5.2 Definitions

The following section references various definitions to help clarify their meaning throughout the report, and to clear up some common misconceptions related to the systems reviewed.

5.2.1 Log Files

The term log files will be utilized for any place where an application or the operating system writes information about what happened as an audit trail, or to aid in debugging. This includes, but is not limited to, specialized and general Windows Event logs, the slog.txt files from the ICP tabulators, as well as the UserLog database table found within every election database.

5.2.2 Source Code

Source Code is the text which is written by a programmer which can be compiled into a program. The compiled program is then deployed onto a computer to perform the desired action. There was no source-code encountered on any of the compact flash drives, or on any of the forensic images captured. Only compiled programs were deployed on these systems.

6 Findings

The following sections outline the findings discovered over the course of the analysis. This included significant deviations from application security best practices, configurations that could allow the integrity of the system to be compromised, and suspicious actual usage of the EMS. This information is broken out by topic with sections that cover “Authentication & Authorization”, “Audit Logging & Tracking”, “Cryptography & Secrete Storage”, “Credential Management”, and “Tabulation Irregularities”.

6.1 Authentication & Authorization

The application did not follow best practices related with assigning least privilege to the users required to do the job or implement proper account management. This represents a large risk to the integrity of the election data. With the current setup it would be simple for a malicious admin to modify the vote in a manner where it would be difficult to determine who did it.

6.1.1 System Administrator utilized for all Access

The only user that has been utilized to login to the EMS Server machine for the entire history available in the Security Event Logs is the use EMSADMIN. This means that the EMSADMIN user is being utilized for normal, everyday use of the various applications associated with voting. This is a huge security risk and could easily be utilized to compromise or change the entire vote.

The EMSADMIN user is a full administrator on the machine in addition to being a full administrator on the Microsoft SQL Database utilized to store all election data. Furthermore, the EMSSERVER has the appropriate tools installed to make it simple to manually update any value in the database. This means that regardless of what level of access a user has within the EMS application they’d be able to change anything they wanted because they’re accessing the computer as an admin.

This could be utilized to:

- Change vote totals within the database affecting final results.
- Add, Edit, or Delete any user in the application, including changing passwords.
- Delete any sort of logs or audit trail that may exist on the computer, or in the database.

6.1.2 System and Application Shared Accounts

The application utilizes generic usernames and passwords rather than creating usernames for the individuals that will be utilizing the application. This likely means that more than one user has the credentials to the same account in order to perform various election related operations in the application. This defies best practice and makes it impossible for you to know who it was that performed a given operation within the application since multiple people have access to the same username. Best practices dictate that each user should always have his or her own username and password to the application. This increases accountability and helps avoid situations where credentials might be leaked.

6.2 Audit Logging & Tracking

The EMS server configuration fails to implement audit logs and controls that would be typical of a high-risk application. In many cases this would prevent the audit logs from existing that would be required to look into or detect a security incident.

6.2.1 No Ballot Images

None of the Compact Flash drives appeared to hold ballot images, and no ballot images had otherwise been imported into the EMS. Ballot images are a critical artifact and are essential for any type of system audit to determine how an electronic voting machine interpreted results and where it might be malfunctioning. Vendor training clearly state that ballot images should be imported into the EMS immediately following the election, but this was never done, and the images don't even seem to be present. Without ballot images its near impossible to match up and see the origin of where errors might be happening.

It is unclear how write-in candidates could have been properly handled without ballot images available for review.

6.2.2 Insufficient Audit Logs

Audit logs should be configured in a manner that all sensitive operations are logged, that the logs include all details necessary to investigate suspicious activity, and that the logs are difficult to tamper with. This was not the case with the Windows Event logs, nor the EMS Application logs.

The Windows Operating System is configured with the standard log level which does not log the access of sensitive files, the deletion of files, or other sensitive actions. This is atypical for a machine that is as sensitive as serving as the central aggregator of all the votes in the county.

The EMS logs found in the UserLog table are also completely deleted any time an election package is loaded within EED. Loading an election package in this way is a standard way that organizations such as Election Source provide the election event. However, this would mean it would be possible for someone to set a malicious device configuration, build the compact flash cards; and then reset the database and put things back to normal. This process would destroy all evidence of the change. Furthermore, the user, EMSADMIN, which is the main account utilized on the machine; has full access to edit the database and delete any log entries. Best practices dictate that an account utilized for normal use of a system not have access to edit or remove logs.

6.2.3 Manual Entries Do Not Require A Comment

The Result Tally and Reporting application can be utilized to insert manual vote count totals rather than automatically importing those results from the tabulator. These manual entries appear to be a way to override and replace the existing vote totals rather than allowing an interface where the numbers that are pulled in from a tabulator can be adjusted with some sort of audit trail. This interface does not log the username submitting the details, require a comment explaining the changes, or even display a timestamp so it was clear when the manual count was done.

These type of entries and comments are standard for any inventory or financial services application. It seems the sensitivity of an election system would be higher than that of these systems.

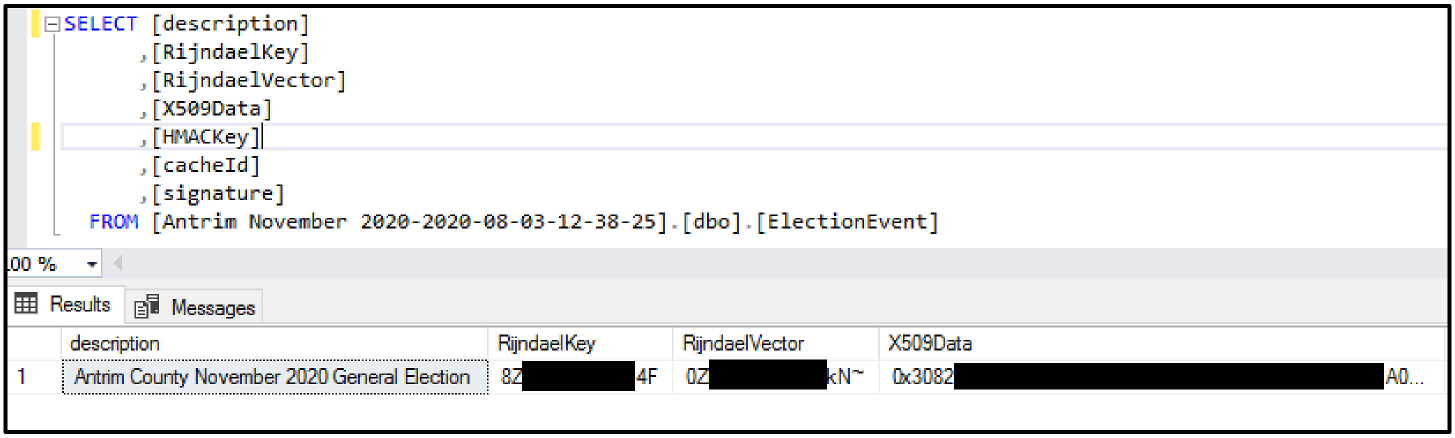
6.3 Cryptography & Secret Storage

The application did not appear to follow best practices for credential storage. The full extent of the problem cannot be fully determined without a review of the actual source code. However, simply by working with the files on the file system and looking in the database it was possible to find various sensitive details that are not properly stored. This included everything from the master encryption key to hard coded credentials.

6.3.1 Plaintext Cryptographic Keys

The master cryptographic key utilized to encrypt all voting results and configuration from the tabulators is stored in plain text in a table within the database for this election. With this key and knowledge about the file formats utilized; it would be possible to alter election results prior to those result files being loaded into the EMS Server, or to alter configurations for the tabulators to make them behave in a certain way. Furthermore, since Election Source originally built the election package utilized by the county and is the originator of the database; any employee at Election Source who had access to the county's database file, or any nation state that compromised one of their computers; would have the encryption key needed to adjust files on the compact flash cards.

Best practices would dictate that any encryption key utilized for election files would only exist on the County's EMS Server and stored in a hardware Trusted Platform Module (TPM). Since the compact flash cards for the tabulators are always built locally, there is no reason for this encryption key to exist anywhere except for the location where the cards are built. Failing to do so significantly reduces the overall security of the election.



```
SELECT [description]
      ,[RijndaelKey]
      ,[RijndaelVector]
      ,[X509Data]
      ,[HMACKey]
      ,[cacheId]
      ,[signature]
  FROM [Antrim November 2020-2020-08-03-12-38-25].[dbo].[ElectionEvent]
```

	description	RijndaelKey	RijndaelVector	X509Data
1	Antrim County November 2020 General Election	8Z[redacted]4F	0Z[redacted]kN~	0x3082[redacted]A0...

Figure 2 - Cryptographic keys are in plain-text in the databases. The values are redacted for security purposes.

6.3.2 Hard coded Credentials

Components of the EMS have hard-coded credentials compiled within the application itself. This is considered an extremely bad practice and is not something that should ever be done. Not only can credentials be exposed when they're hard coded in the application, but the fact that they're compiled in the application means that every single customer of this version of the EMS would utilize the same credentials. As a result, learning the credentials would allow you to attack them all.

Hard coding of credentials into this application appears to go back to at least 2010, based on the following report:

https://www.eac.gov/sites/default/files/voting_system/files/Deficiency%20Report.pdf

NOTE: These were detected by utilizing grep to search the binaries for the string "password".

File Name(s)	Value

/Election Data Translator/DVS.DemocracySuite.DatabaseService.dll
/Election Event Designer/DVS.DemocracySuite.DatabaseService.dll
/Election Event Designer/DVS.DemocracySuite.DatabaseService.dll
	username="Techadvisor"
	password="YWanPlFl6ETqijhPNWFsyEjAy6eEzJM0A0DJ7O+YY4Q="

/Election Data Translator/DVS.DemocracySuite.DatabaseService.dll
/Election Event Designer/DVS.DemocracySuite.DatabaseService.dll
/Election Event Designer/DVS.DemocracySuite.DatabaseService.dll
	username="MRO01"
	password="YWanPlFl6ETqijhPNWFsyEjAy6eEzJM0A0DJ7O+YY4Q="

/Election Data Translator/DVS.DemocracySuite.DatabaseService.dll
/Election Event Designer/DVS.DemocracySuite.DatabaseService.dll
/Election Event Designer/DVS.DemocracySuite.DatabaseService.dll
	username="ROAdmin"
	password="YWanPlFl6ETqijhPNWFsyEjAy6eEzJM0A0DJ7O+YY4Q="

/Election Data Translator/DVS.DemocracySuite.DatabaseService.dll
/Election Event Designer/DVS.DemocracySuite.DatabaseService.dll
/Election Event Designer/DVS.DemocracySuite.DatabaseService.dll
	username="Admin"
	password="YWanPlFl6ETqijhPNWFsyEjAy6eEzJM0A0DJ7O+YY4Q="

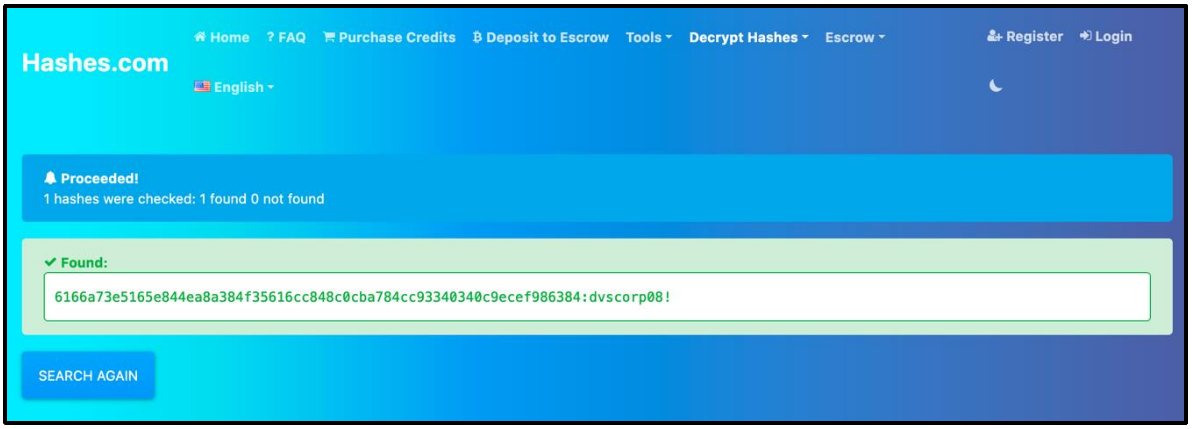
/Election Data Translator/DVS.DemocracySuite.DatabaseService.dll
/Election Event Designer/DVS.DemocracySuite.DatabaseService.dll
/Election Event Designer/DVS.DemocracySuite.DatabaseService.dll
	username="SAdmin"
	password="YWanPlFl6ETqijhPNWFsyEjAy6eEzJM0A0DJ7O+YY4Q="

/Election Data Translator/DVS.DemocracySuite.DatabaseService.dll
/Election Event Designer/DVS.DemocracySuite.DatabaseService.dll
/Election Event Designer/DVS.DemocracySuite.DatabaseService.dll
	username="Admin"
	password="oCFR3h+mPKykHkkE41o5cvyCSwY="

/Election Data Translator/DVS.DemocracySuite.DatabaseService.dll
/Election Event Designer/DVS.DemocracySuite.DatabaseService.dll
/Election Event Designer/DVS.DemocracySuite.DatabaseService.dll
	username="Admin"
	password="oCFR3h+mPKykHkkE41o5cvyCSwY="

6.3.3 Passwords Stored As An Unsalted Hash

Credentials to the EMS applications are stored within the Microsoft SQL Database utilizing the hashing algorithm SHA256. This is better than storing the credentials in the database as plain text, but industry best practices dictate that these passwords should also have a cryptographically random string tacked onto the front of them before being hashed. This is referred to as "salt"; and it prevents several common attacks that might allow an attacker to figure out the credentials. Because salt was not used, we were actually able to take the hash out of the database, 6166A73E5165E844EA8A384F35616CC848C0CBA784CC93340340C9ECEF986384, and run it through a database of pre-computed hashes at https://hashes.com/. This let us figure out that its value was, "dvscorp08!".



Proceeded!
1 hashes were checked: 1 found 0 not found

✓ Found:

```
6166a73e5165e844ea8a384f35616cc848c0cba784cc93340340c9ecef986384:dvscorp08!
```

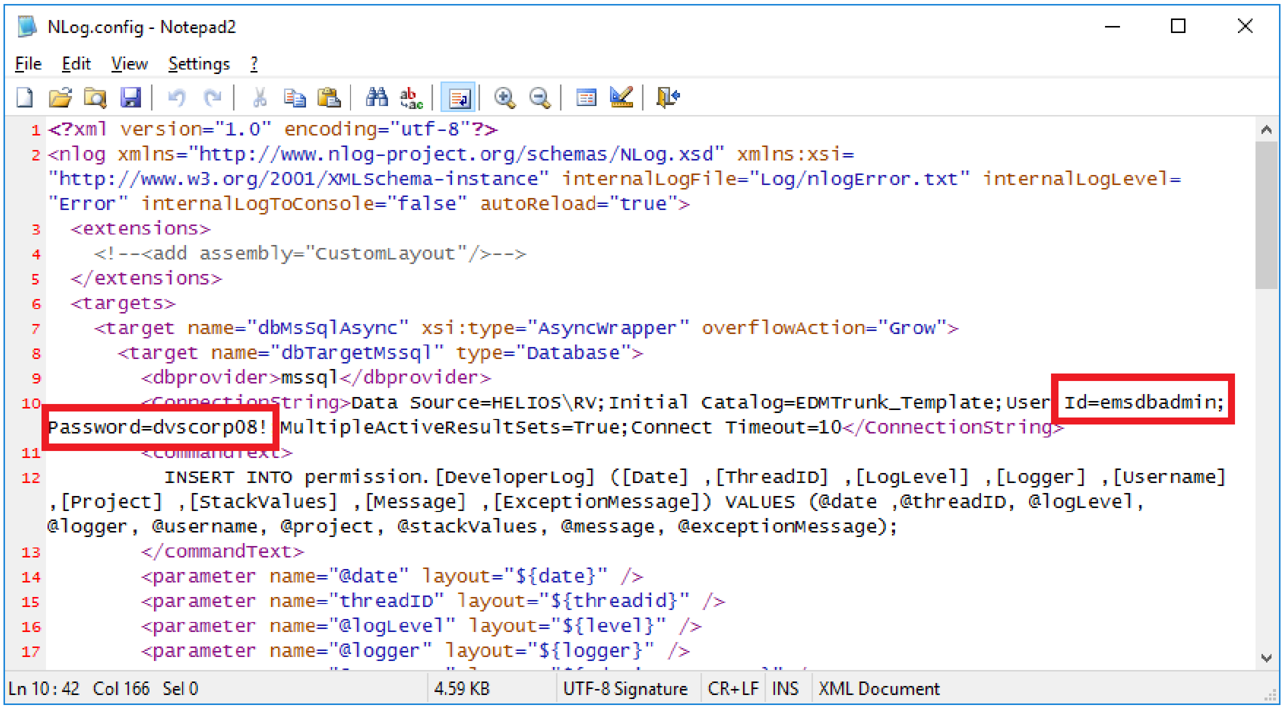
6.3.4 Credentials In Plain Text

The application has several places that included credentials in plain text hard coded within various locations and configuration files. Best practices dictate that credentials should always be encrypted whenever they are stored on the filesystem of a machine. Failing to do so can allow sensitive credentials to potentially be compromised and utilized to manipulate results. This is considered a basic security requirement that even low-risk applications should follow. The Election Management System would be considered a high-risk system.

6.3.4.1 C:\Program Files\Dominion Voting Systems\Smart Card Service\NLog.config

Database credentials are stored in plain text without any encryption within a configuration file for the Smart Card Service. The naming of this password suggests that this default password has gone unchanged since 2008. This is supported by a 2010 defect report that cited this same password as being hard coded within the application:

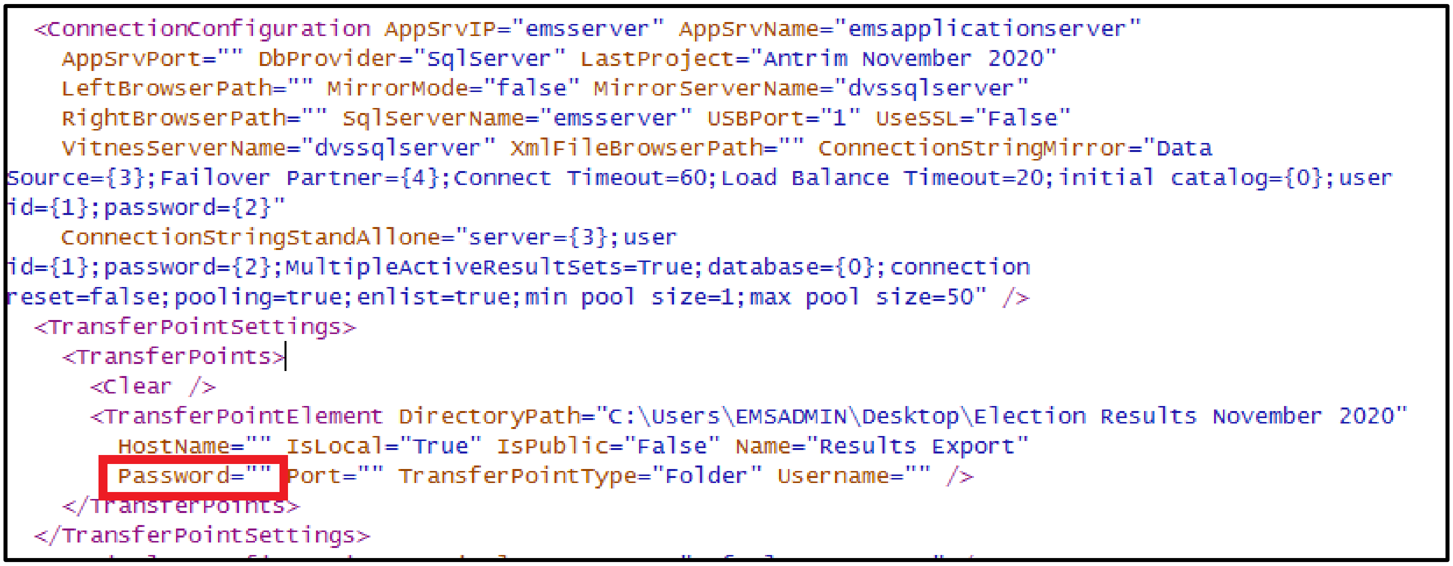
https://www.eac.gov/sites/default/files/voting_system/files/Deficiency%20Report.pdf



```
<?xml version="1.0" encoding="utf-8"?>
<nlog xmlns="http://www.nlog-project.org/schemas/NLog.xsd" xmlns:xsi=
"http://www.w3.org/2001/XMLSchema-instance" internalLogFile="Log/nlogError.txt" internalLogLevel=
"Error" internalLogToConsole="false" autoReload="true">
  <extensions>
    <!--<add assembly="CustomLayout"/>-->
  </extensions>
  <targets>
    <target name="dbMsSqlAsync" xsi:type="AsyncWrapper" overflowAction="Grow">
      <target name="dbTargetMssql" type="Database">
        <dbprovider>mssql</dbprovider>
        <connectionString>Data Source=HELIOS\RV;Initial Catalog=EDMTrunk_Template;User Id=emsdbadmin;
Password=dvscorp08! MultipleActiveResultSets=True;Connect Timeout=10</connectionString>
        <commandText>
          INSERT INTO permission.[DeveloperLog] ([Date] ,[ThreadID] ,[LogLevel] ,[Logger] ,[Username]
,[Project] ,[StackValues] ,[Message] ,[ExceptionMessage]) VALUES (@date ,@threadID, @logLevel,
@logger, @username, @project, @stackValues, @message, @exceptionMessage);
        </commandText>
        <parameter name="@date" layout="${date}" />
        <parameter name="threadID" layout="${threadid}" />
        <parameter name="@logLevel" layout="${level}" />
        <parameter name="@logger" layout="${logger}" />
```

6.3.4.2 C:\Program Files\Dominion Voting Systems\Results Tally and Reporting\ DVS.DemocracySuite.ResultTally.exe.Config

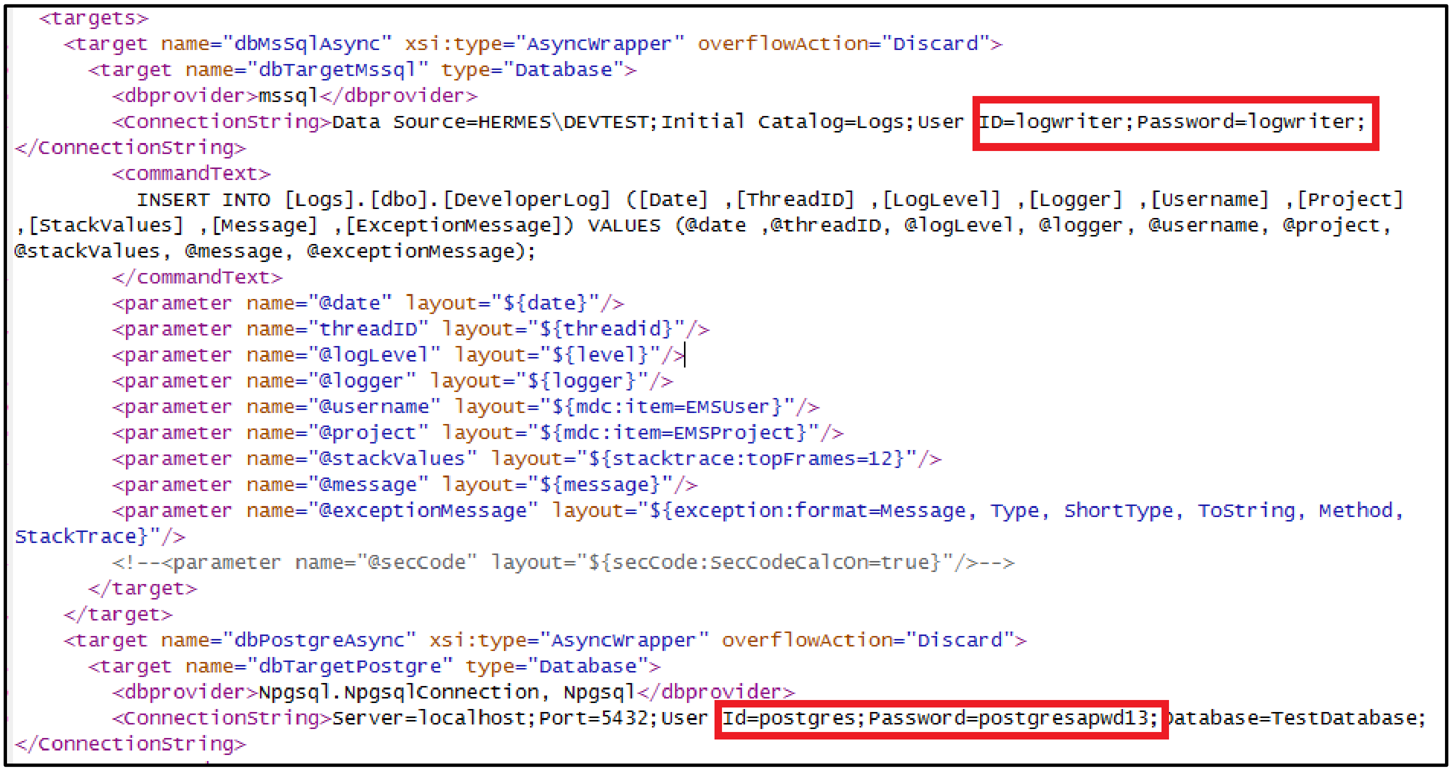
The configuration for the Results Tally and Reporting Application has a location where a password would be stored in plain text. Since Antrim writes the results to the local file system rather than a network machine; this entry does not directly represent a risk to Antrim County. However, this shows a pattern of not following well recognized industry best practices.



```
  <ConnectionConfiguration AppSrvIP="emsserver" AppSrvName="emsapplicationserver"
    AppSrvPort="" DbProvider="SqlServer" LastProject="Antrim November 2020"
    LeftBrowserPath="" MirrorMode="false" MirrorServerName="dvssqlserver"
    RightBrowserPath="" SqlServerName="emsserver" USBPort="1" UseSSL="False"
    VitnesServerName="dvssqlserver" XmlFileBrowserPath="" ConnectionStringMirror="Data
Source={3};Failover Partner={4};Connect Timeout=60;Load Balance Timeout=20;initial catalog={0};user
id={1};password={2}"
    ConnectionStringStandAllone="server={3};user
id={1};password={2};MultipleActiveResultSets=True;database={0};connection
reset=false;pooling=true;enlist=true;min pool size=1;max pool size=50" />
  <TransferPointSettings>
    <TransferPoints>
      <Clear />
      <TransferPointElement DirectoryPath="C:\Users\EMSADMIN\Desktop\Election Results November 2020"
        HostName="" IsLocal="True" IsPublic="False" Name="Results Export"
        Password="" Port="" TransferPointType="Folder" Username="" />
    </TransferPoints>
  </TransferPointSettings>
```

6.3.5 C:\Program Files\Dominion Voting Systems\Results Tally and Reporting\NSLog.config

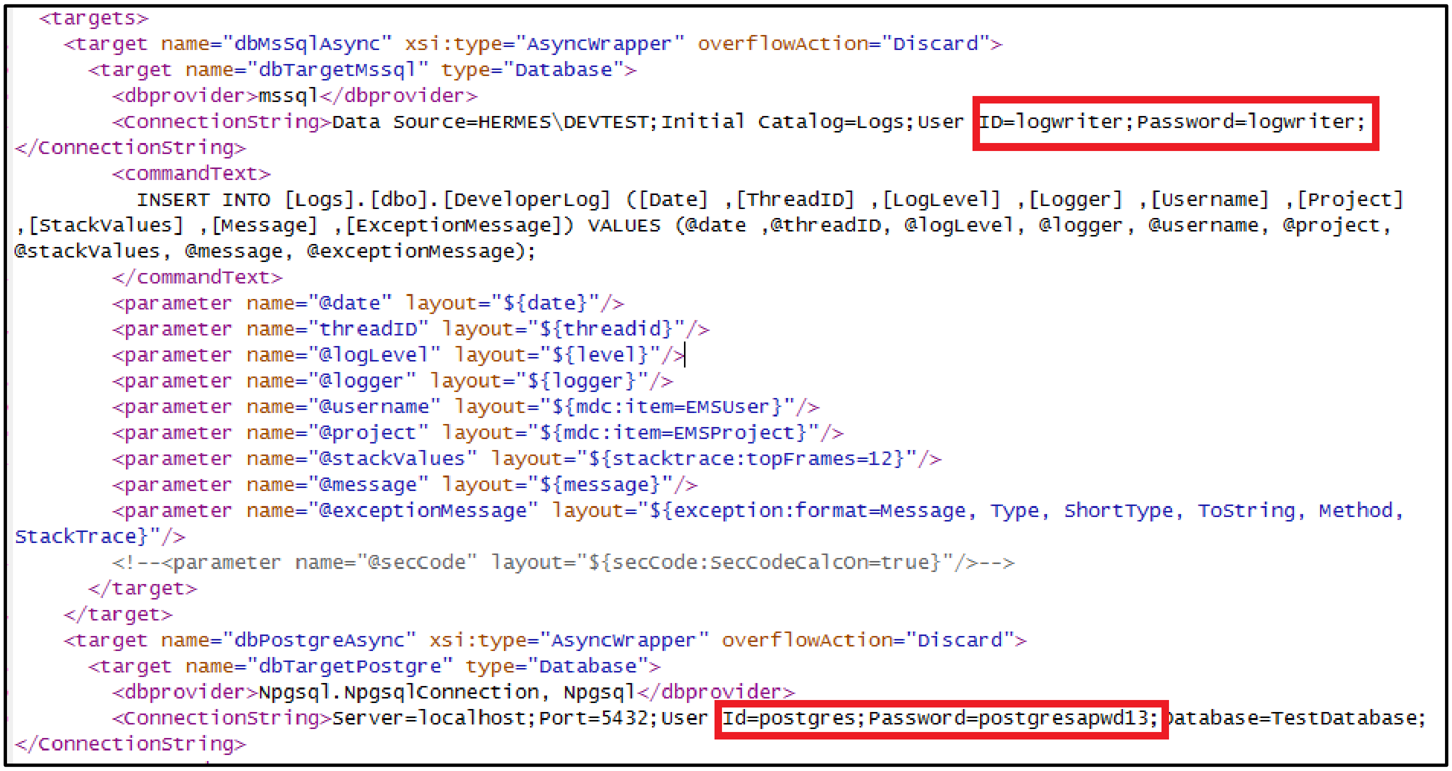
The NSLog.Config for the Results Tally and Reporting has multiple database connections hard coded within the configuration file. Giving the naming and database types listed with the connections string, it's unclear if these are currently in-use in the application. However, it further demonstrates that storing passwords in plain text is common within the application suite.



```
  <targets>
    <target name="dbMsSqlAsync" xsi:type="AsyncWrapper" overflowAction="Discard">
      <target name="dbTargetMssql" type="Database">
        <dbprovider>mssql</dbprovider>
        <ConnectionString>Data Source=HERMES\DEVTEST;Initial Catalog=Logs;User ID=logwriter;Password=logwriter;
</ConnectionString>
        <commandText>
          INSERT INTO [Logs].[dbo].[DeveloperLog] ([Date] ,[ThreadID] ,[LogLevel] ,[Logger] ,[Username] ,[Project]
,[StackValues] ,[Message] ,[ExceptionMessage]) VALUES (@date ,@threadID, @logLevel, @logger, @username, @project,
@stackValues, @message, @exceptionMessage);
        </commandText>
        <parameter name="@date" layout="${date}"/>
        <parameter name="threadID" layout="${threadid}"/>
        <parameter name="@logLevel" layout="${level}"/>
        <parameter name="@logger" layout="${logger}"/>
        <parameter name="@username" layout="${mdc:item=EMSUser}"/>
        <parameter name="@project" layout="${mdc:item=EMSProject}"/>
        <parameter name="@stackValues" layout="${stacktrace:topFrames=12}"/>
        <parameter name="@message" layout="${message}"/>
        <parameter name="@exceptionMessage" layout="${exception:format=Message, Type, ShortType, ToString, Method,
StackTrace}"/>
        <!--<parameter name="@secCode" layout="${secCode:SecCodeCalcOn=true}"/>-->
      </target>
    </target>
    <target name="dbPostgreAsync" xsi:type="AsyncWrapper" overflowAction="Discard">
      <target name="dbTargetPostgre" type="Database">
        <dbprovider>Npgsql.NpgsqlConnection, Npgsql</dbprovider>
        <ConnectionString>Server=localhost;Port=5432;User Id=postgres;Password=postgresapwd13;Database=TestDatabase;
</ConnectionString>
```

6.3.6 C:\Program Files\Dominion Voting Systems\Election Event Designer\NSLog.config

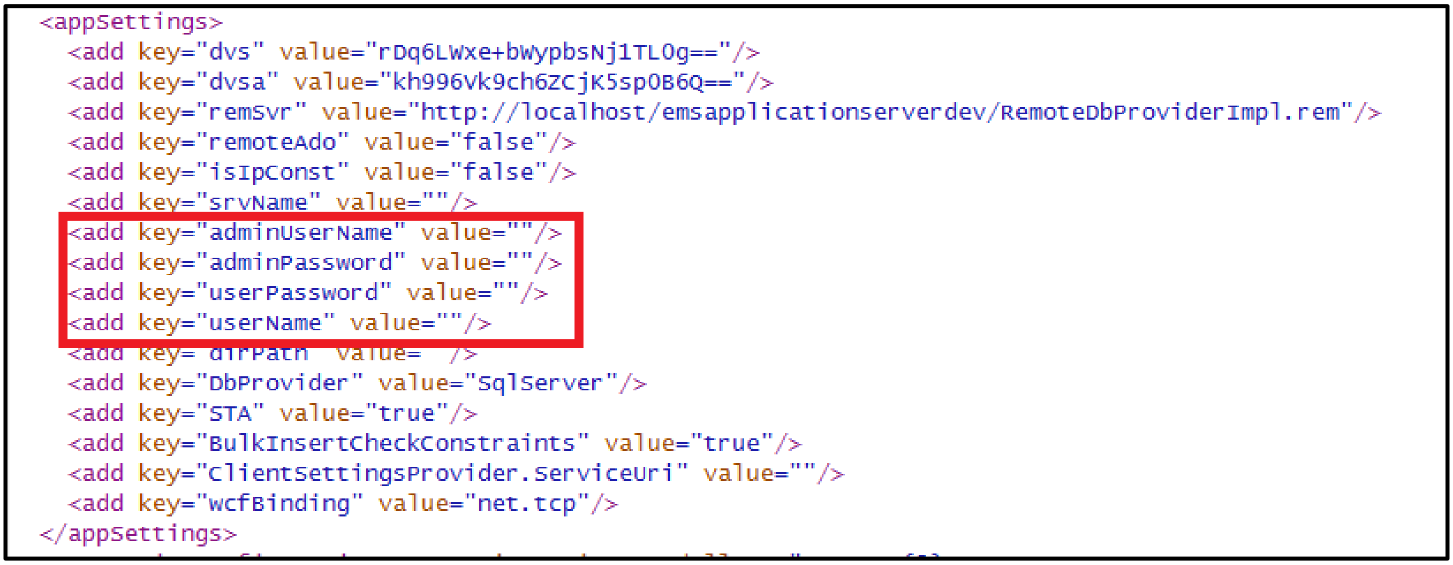
The NSLog.Config for the Election Event Designer has multiple database connections hard coded within the configuration file. Giving the naming and database types listed with the connections string, it's unclear if these are currently in-use in the application. However, it further demonstrates that storing passwords in plain text is common within the application suite.



```
  <targets>
    <target name="dbMsSqlAsync" xsi:type="AsyncWrapper" overflowAction="Discard">
      <target name="dbTargetMssql" type="Database">
        <dbprovider>mssql</dbprovider>
        <ConnectionString>Data Source=HERMES\DEVTEST;Initial Catalog=Logs;User ID=logwriter;Password=logwriter;
</ConnectionString>
        <commandText>
          INSERT INTO [Logs].[dbo].[DeveloperLog] ([Date] ,[ThreadID] ,[LogLevel] ,[Logger] ,[Username] ,[Project]
,[StackValues] ,[Message] ,[ExceptionMessage]) VALUES (@date ,@threadID, @logLevel, @logger, @username, @project,
@stackValues, @message, @exceptionMessage);
        </commandText>
        <parameter name="@date" layout="${date}"/>
        <parameter name="threadID" layout="${threadid}"/>
        <parameter name="@logLevel" layout="${level}"/>
        <parameter name="@logger" layout="${logger}"/>
        <parameter name="@username" layout="${mdc:item=EMSUser}"/>
        <parameter name="@project" layout="${mdc:item=EMSProject}"/>
        <parameter name="@stackValues" layout="${stacktrace:topFrames=12}"/>
        <parameter name="@message" layout="${message}"/>
        <parameter name="@exceptionMessage" layout="${exception:format=Message, Type, ShortType, ToString, Method,
StackTrace}"/>
        <!--<parameter name="@secCode" layout="${secCode:SecCodeCalcOn=true}"/>-->
      </target>
    </target>
    <target name="dbPostgreAsync" xsi:type="AsyncWrapper" overflowAction="Discard">
      <target name="dbTargetPostgre" type="Database">
        <dbprovider>Npgsql.NpgsqlConnection, Npgsql</dbprovider>
        <ConnectionString>Server=localhost;Port=5432;User Id=postgres;Password=postgresapwd13;Database=TestDatabase;
</ConnectionString>
```

6.3.7 C:\PROGRAM FILES\DOMINION VOTING SYSTEMS\ELECTION DATA TRANSLATOR\ DVS.BRIDGING.IMPORTADAPTER.EXE.CONFIG

The DVS.Bridging.ImportAdapter.exe.config for the Election Data Translator has multiple locations for credentials hard coded within the configuration file. It does not appear that Antrim utilizes this feature, so these appear to be blank. However, it further demonstrates that storing passwords in plain text is common within the application suite.



```
<appSettings>
  <add key="dvs" value="rDq6LWxe+bWypbsNj1TL0g=="/>
  <add key="dvsa" value="kh996Vk9ch6ZCjK5sp0B6Q=="/>
  <add key="remSvr" value="http://localhost/emsapplicationserverdev/RemoteDbProviderImpl.rem"/>
  <add key="remoteAdo" value="false"/>
  <add key="isIpConst" value="false"/>
  <add key="srvName" value=""/>
  <add key="adminUserName" value=""/>
  <add key="adminPassword" value=""/>
  <add key="userPassword" value=""/>
  <add key="userName" value=""/>
  <add key="dirPath" value=""/>
  <add key="DbProvider" value="SqlServer"/>
  <add key="STA" value="true"/>
  <add key="BulkInsertCheckConstraints" value="true"/>
  <add key="ClientSettingsProvider.ServiceUri" value=""/>
  <add key="wcfBinding" value="net.tcp"/>
</appSettings>
```

6.4 Credential Management

Credential reuse appears to be relatively common across the organization, and across multiple deployments of the application. The password dvscorp08!, which was in use in Antrim County has showed up in prior deficiency reports, and in breach data associated with employees of the EMS vendor. Based on its naming, this password is over 12 years old and still in use today. The continued use of this password makes it easy for a potential attacker to guess a password and get into the system to manipulate data.

6.4.1 PASSWORD REUSE

Reviewing the passwords utilized for Antrim County going back to August 2018; it appears that the password "dvscorp08!" has been utilized for at least one account since 2018 and in many cases that same password was utilized for most if not all the accounts.

An 2012 EAC report, "WYLE TEST REPORT NO. T57381-01APPENDIX A.11DEFICIENCY REPORT", reported on page 10 the **dvscorp08!** Password was hardcoded into the system and first reported on 2010-08-16 14:28.

https://www.eac.gov/sites/default/files/voting_system/files/Deficiency%20Report.pdf

6.4.2 Breach Data

A search of breach data associated with the EMS vendor’s domains shows regular use of the password “dvscorp08!”.

2017-07-19 Breach
EMAIL | SHA-1 | CLEAR PASS
masha.REDACTED@dominionvoting.com | a02151de1fa63caca41e4904e35a3972fc824b06 | dvscorp08!

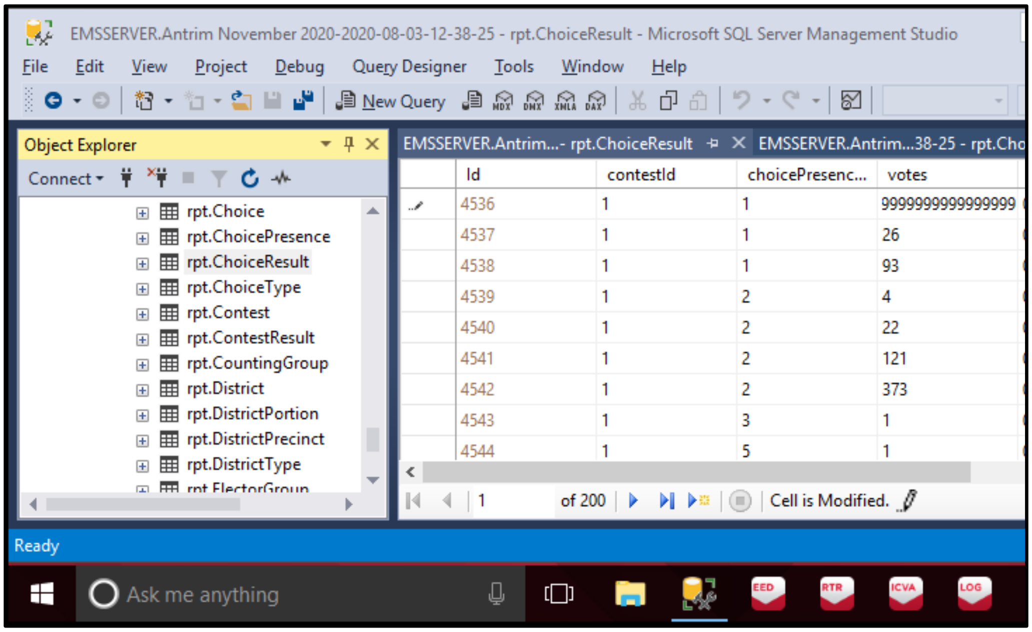
2017-12-11 Breach

masha.REDACTED@dominionvoting.com:dvscorp08!
masha.REDACTED@dvscorp.com:dvscorp08!
masha.REDACTED@gmail.com:dvscorp08!

6.5 Certification

The Election Assistance Commission’s (EAC) list of approved software for the EMS does not appear to include Microsoft SQL Server Management Studio, but this software is installed on the machine. Microsoft SQL Server Management Studio is a database administration tool which makes it easy to directly edit entries within the database. This could potentially be utilized to change vote values.

Since this tool is a separate install from Microsoft SQL Server, it is our understanding that it would be required to explicitly mentioned on the list of certified software in order to be allowed to exist on an EAC certified configuration (See pages 4-13):
https://www.eac.gov/sites/default/files/voting_system/files/Dominion_Voting_Systems_D-Suite_5.5-B_Test_Plan-Rev._02.pdf



Id	contestId	choicePresenc...	votes
4536	1	1	9999999999999999
4537	1	1	26
4538	1	1	93
4539	1	2	4
4540	1	2	22
4541	1	2	121
4542	1	2	373
4543	1	3	1
4544	1	5	1

Cell is Modified.

Figure 3 - SQL Management Tools allows the easy editing of a vote.

7 AFFIRMATION

I declare that I am over the age of 18, and I understand and believe in the obligations of an oath. Under penalty of perjury laws of the State of Michigan and the United States I attest that the foregoing report is true and correct, and that this report was executed this 9th day of April, 2021.

Douglas Logan

8 ABOUT CYBER NINJAS

Cyber Ninjas is an application security consulting company specializing in code review, ethical hacking, training and security program development. Our staff represents decades of experience in a variety of areas including application support, development, product management, and application security. This experience across all areas of the software development life cycle gives us a unique perspective on how to build security into your existing processes. We can help you build a software security program, expand the capabilities of your existing staff, or simply perform a security assessment of your software or your company. With everything we do, our goal is to build the knowledge within your organization. We strongly believe that "Security comes with knowledge." ™; and that it is our job as Cyber Ninjas to train and teach through every engagement in order to build up capabilities within your organization.

APPENDIX A: BIO – DOUGLAS LOGAN

Douglas Logan has handled Cyber Security for major companies and organizations around the country, such as the Federal Communications Commission, JP Morgan Chase, Bank of America, Citibank, Sally Mae, and more. In 2015, he was named a winner of the prestigious SANS 2015 Difference Makers Award.

Mr. Logan (CISSP, GWAPT, GCIH) is the CEO and Principal Consultant for Cyber Ninjas, a Sarasota, Florida-based company. Mr. Logan is responsible for working with organizations to evaluate their current cyber security risks, educate stakeholders on the nature and causes of those risks and establish policies, programs, and procedures that provide long-term protection.

Mr. Logan founded Cyber Ninjas under the mission of building organizations' cyber security capabilities by developing their people and processes, providing them with the opportunity to eventually handle their own security requirements. His solution-focused services include enterprise threat analysis and modeling, security program development, secure software development life-cycle (sSDLC) creation, malicious code detection, training, staff mentoring, code review and ethical hacking. "We believe there is no point in breaking something if you can't offer a reasonable way to fix it," he says**.**

Prior to founding Cyber Ninjas in 2013, Mr. Logan was a Senior Consultant for Cigital where, among other responsibilites, he helped launch the Bloomington, Indiana office. Under Mr. Logan's technical leadership, Cigital was able to scale their Vulnerability Assessement Managed Service in less than a year from three people conducting roughly 10 assessments a month, to about 20 individuals performing 250 assessments a month. Mr. Logan's process oriented methodology allowed him to place new hires straight out of college to billable work in under 10 days, and had those same individuals leading teams within 60 days. After a year of building people and processes, the entire system Mr. Logan built was self-propetuating and completely self-sufficient, allowing him to step into other projects.

Mr. Logan was also involved in many other areas of Cigital's business, including mobile threat modeling and threat analysis, red team enterprise risk assessments, advanced penetration testing, and instructor lead training. He is the author of Cigital's Android Penetration Testing class, and co-author and team-lead responsible for creating the iOS Penetration Testing class.

Before Cigital, Mr. Logan had 12 years combined experience in the IT field, including roles as Server Administration, Development, and Product Management.

His broad experience not only gives him a deep technical backing, but allows him to design solutions that integrate with normal day-to-day IT processes.

Outside of work Mr. Logan volunteers for the US Cyber Challenge; a non-profit organization dedicated to finding America's brightest and getting them plugged into the Cyber Security field. In that role he helps shape America's future cyber warriors to help defend our nation.

Mr. Logan holds Bachelors degrees in both Business Management and Accounting from Guilford College in Greensboro, NC.

Exhibit 8

Benjamin Cotton affidavit

STATE OF MICHIGAN

IN THE CIRCUIT COURT FOR THE COUNTY OF ANTRIM

WILLIAM BAILEY

Plaintiff

Case No. 20-9238-CZ

v.

ANTRIM COUNTY

HON. KEVIN A. ELSENHEIMER

Defendant,

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 APRIL 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.

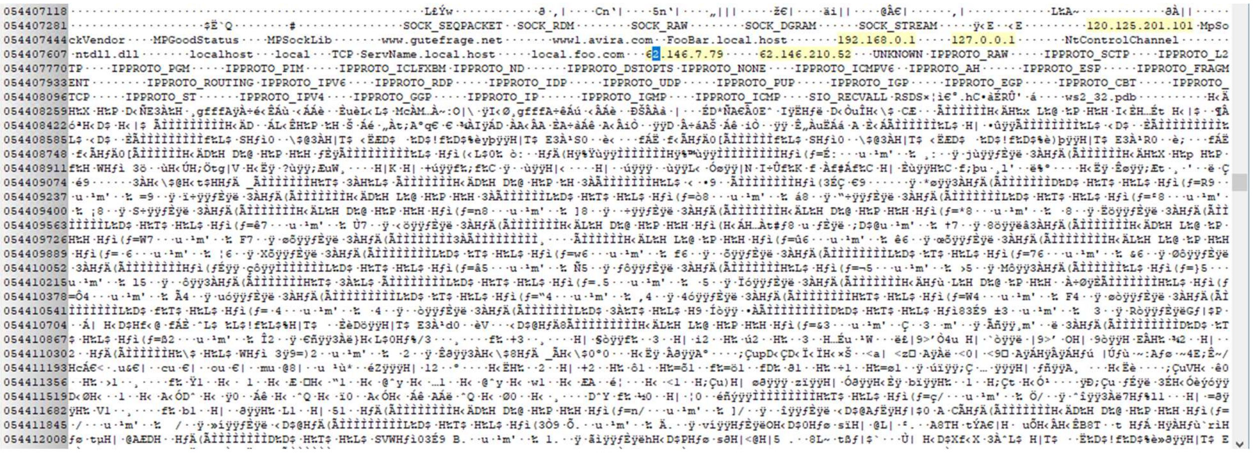
b) Thirty eight (38) forensic images of the compact flash cards used in Antrim County during the November 2020 elections that were imaged on 4 December 2020 by a firm named Sullivan and Strickler.

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) Thumbdrives 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.



```
054407118 ·····································L£Ýw···········∂·,|····Cn'|····5n'|····„|||·····ž€|····äi||····@Â€|······,|············LŁA~············∂À||·····
054407281 ·················$Ë`Q·······#···············SOCK_SEQPACKET··SOCK_RDM········SOCK_RAW········SOCK_DGRAM······SOCK_STREAM·····ÿ‹E··‹E·········120.125.201.101·MpSo
054407444ckVendor····MPGoodStatus····MPSockLib·······www.gutefrage.net·······www1.avira.com··FooBar.local.host·······192.168.0.1·····127.0.0.1·······NtControlChannel········
054407607 ntdll.dll·······localhost····local····TCP·ServName.local.host·····local.foo.com···62.146.7.79·····62.146.210.52···UNKNOWN·IPPROTO_RAW·····IPPROTO_SCTP····IPPROTO_L2
054407770TP····IPPROTO_PGM·····IPPROTO_PIM·····IPPROTO_ICLFXBM·IPPROTO_ND······IPPROTO_DSTOPTS·IPPROTO_NONE····IPPROTO_ICMPV6··IPPROTO_AH······IPPROTO_ESP·····IPPROTO_FRAGM
054407933ENT········IPPROTO_ROUTING·IPPROTO_IPV6····IPPROTO_RDP·····IPPROTO_IDP·····IPPROTO_UDP·····IPPROTO_PUP·····IPPROTO_IGP·····IPPROTO_EGP·····IPPROTO_CBT·····IPPROTO_
054408096TCP·····IPPROTO_ST······IPPROTO_IPV4····IPPROTO_GGP·····IPPROTO_IP······IPPROTO_IGMP····IPPROTO_ICMP····SIO_RECVALL·RSDS×¦ì€°.hC•àÉRÛ'·á····ws2_32.pdb··········H‹Ä
```

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) **<u>ESS DS400 Communications.</u>** 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 can not 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) **Out of Date Security Updates and Virus Definitions.** An analysis of 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 was last updated in 2016. The other systems were in a similar state. This lack of security updating 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. 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. The Halderman report dated March 26, 2021 relating to this matter validates this finding. 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.

12) **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)

Without these system components it will be impossible to determine the extent of public and private communications, the extent to which remote access to the voting system components is possible and to determine if or when unauthorized access occurred.

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

Ben Cotton

Benjamin R. Cotton

Exhibit 9

J. Alex Halderman affidavit

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

DONNA CURLING, ET AL., **Plaintiffs,** **v.** **BRAD RAFFENSPERGER, ET AL.,** **Defendants.**	**DECLARATION OF** **J. ALEX HALDERMAN IN SUPPORT OF MOTION FOR PRELIMINARY INJUNCTION** **Civil Action No. 1:17-CV-2989-AT**

Pursuant to 28 U.S.C. § 1746, J. ALEX HALDERMAN declares under penalty of perjury that the following is true and correct:

1. I hereby incorporate my previous declarations as if fully stated herein. I have personal knowledge of the facts in this declaration and, if called to testify as a witness, I would testify under oath to these facts.

<u>Georgia's Current Election Technology</u>

2. Georgia recently deployed new voting equipment and software manufactured by Dominion Voting Systems, Inc. ("Dominion"). These components include ImageCast X Prime ("ICX") ballot marking devices ("BMDs"), ImageCast Precinct ("ICP") precinct-count scanners, ImageCast Central ("ICC") central-count scanners, and the Democracy Suite election management system ("EMS"). Georgia

Secretary of State Brad Raffensperger certified these components in August 2019,[1] and they were first used statewide during the June 20, 2020 election.[2]

3. Under this new system (the "BMD-based Election System"), Georgia generally requires all in-person voters to select candidates on Dominion ICX BMDs. These devices are computer tablets connected to off-the-shelf laser printers. They do not record votes but instead print paper records that are supposed to contain the voter's selections in both human-readable text and as a type of machine-readable barcode called a QR code. Voters insert these printouts into Dominion ICP optical scanners, which read the barcodes and count the votes encoded in them.[3]

4. Absentee voters do not use BMDs but instead complete hand-marked paper ballots ("HMPBs"), which are tabulated at central locations by Dominion ICC scanners. While Georgia's precinct-based ICP scanners have the capability to count hand-marked paper ballots,[4] the State only uses them to count BMD printouts.

[1] Georgia Dominion certification (Aug. 9, 2019), https://sos.ga.gov/admin/uploads/Dominion_Certification.pdf.

[2] Mark Niesse, "How Georgia's new voting machines work," *The Atlanta Journal-Constitution* (June 9, 2020), https://www.ajc.com/news/state--regional-govt--politics/how-georgia-new-electronic-voting-machines-work/RyIOJuHYQgktcCNGL9sEoK/.

[3] Decl. of Dr. Eric Coomer, Dckt. 658-2, at 10.

[4] *Id* at 9.

5. Pre- and post-election procedures in the BMD-based election system closely parallel those under the old DRE-based election system. Before every election, the Secretary of State's office prepares election programming files using Dominion EMS software, which is a collection of client and server programs that run on commercial-off-the-shelf (COTS) computers and servers. The Secretary of State transmits the election programming files to county officials, who use another instance of the Dominion EMS to prepare memory cards and USB sticks for every scanner and ballot marking device used in the county. These removable media contain the ballot design, including the names of the races and candidates, and rules for counting the ballots. Election workers install a memory card or USB stick into each BMD and ICP scanner prior to the start of voting.

6. After polls close, election workers remove the memory cards from every ICP scanner and return them to the county. At that point, the memory cards contain a digital image of each scan as well as the scanner's interpretation of the votes contained in the barcode. County workers use the Dominion EMS to retrieve data from the cards and prepare the final election results based on the barcode readings.

Attacks Against the BMD-based Election System

7. Attackers could alter election outcomes under Georgia's BMD-based election system in several ways:

(a) Attacks on the BMDs could cause them to print barcodes that differ from voters' selections. These changes would be undetectable to voters, who cannot read the encrypted barcodes. Since the barcodes are the only thing the scanners count, the impact would be a change to the election results. The only known safeguard that can reliably detect such an attack is to rigorously audit both the human-readable portion of the printouts and the barcodes, which Georgia does not currently do.

(b) Attacks on the BMDs could also change *both* the barcode and the human-readable text on some of the printouts. Research shows that few voters carefully review their BMD printouts, and, consequently, changes to enough printouts to change the winner of a close race would likely go undetected. No audit or recount could detect this fraud, since both the digital and paper records of the votes would reflect the same selections but not the ones the voters intended.

(c) Attacks on the scanners could also cause fraudulent election results by changing the digital records of the votes. The only known safeguard that can reliably detect such an attack is a sufficiently rigorous manual audit or recount of the paper records, which Georgia does not currently require.

8. One way that attackers could carry out attacks against the BMD-based election system is by infecting the election equipment with malicious software ("malware"). Malware could potentially be introduced in several ways, including: (a) with physical access to any of the many electronic components that compose the system, (b) through an attack on the hardware or software supply-chain, or (c) by spreading virally via the election management systems to polling place equipment during routine pre-election procedures.

9. Components of Georgia's election system that are not directly connected to the Internet might nonetheless be targeted by attackers. Nation-state attackers have developed a variety of techniques for infiltrating non-Internet-connected systems, including by spreading malware on removable media that workers use to copy files in and out.[5] Attackers could employ this method to infect the state or county EMS and spread from there to scanners and BMDs when workers program them for the next election. In this way, an attack could potentially spread from a single point of infection to scanners and BMDs across entire counties or the whole

[5] A well-known example of this ability, which is known as "jumping an air gap," is the Stuxnet computer virus, which was created to sabotage Iran's nuclear centrifuge program by attacking factory equipment that was not directly connected to the Internet. Kim Zetter, "An Unprecedented Look at Stuxnet, the World's First Digital Weapon," *Wired* (Nov. 3, 2014), https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/.

state, in the same way that malware could have spread through the old DRE system, which was not effectively air-gapped or otherwise reasonably secured.

10. The BMD-based election system is at further heightened risk of attack because of the legacy of poor security in Georgia's old DRE-based election system and its associated computers and networks. If attackers infiltrated the DRE-based system, they likely did so by first infiltrating components such as the Secretary of State's computer network, the voter registration database software developed by PCC, Inc., or the non-"air gapped" computers and removable media used by state and county workers and outside contractors to transfer data into and out of the EMS. The record in this matter contains abundant evidence about vulnerabilities in all these components, some of which were unmitigated for years and may still be unmitigated. Responsibility for their security continues to rest with many of the same technicians and managers who oversaw the security of the old system and were unable or unwilling to implement effective security measures.

11. These components continue to be used with the new voting system, including to process data that is copied to polling-place equipment. If attackers breached any of them to attack the DRE-based system, those attackers may continue to have such access under the BMD-based system. Technologies that the State has highlighted as key defenses for these legacy components, such as anti-malware

scans, anti-virus scans, and endpoint protection, provide little defense against sophisticated attackers like hostile foreign governments.

12. Importantly, apart from the examinations Fortalice conducted that found significant vulnerabilities with the Secretary of State's information technology infrastructure including components of the election management network, there is no indication that Georgia has ever forensically or otherwise rigorously examined the current election system, including components from the prior DRE-based system that are used with the current BMD-based system. In an environment of advanced persistent threats to both election systems, coupled with the critical known vulnerabilities with those systems, the lack of any such examination raises serious concerns about the reliability of the current system and election outcomes.

Georgia's New Dominion Equipment has Critical Security Flaws

13. Dominion does not dispute that its products can be hacked by sufficiently capable adversaries.[6]

14. One reason why this is true is the complexity of the software, which far exceeds the complexity of the DRE-based system. The Dominion software used in

[6] Decl. of Dr. Eric Coomer, Director of Product Strategy and Security for Dominion ¶ 13, Dckt. No. 658-2 ("all computers can be hacked with enough time and access").

Georgia contains nearly 2.75 million lines of source code (equivalent to about 45,000 printed pages), excluding the Windows and Android operating systems and other off-the-shelf software packages.[7] The ICP scanner alone contains about 475,000 lines of source code, and its software is written in C/C++,[8] a programming language that is particularly susceptible to some of the most dangerous types of vulnerabilities.

15. Software of the size and complexity of the Dominion code inevitably has exploitable vulnerabilities. As a source-code review team working for the California Secretary of State concluded in a study of a voting system with only 10% as much code as Dominion's, "If the [system] were secure, it would be the first computing system of this complexity that is fully secure."[9] Nation-state attackers often discover and exploit novel vulnerabilities in complex software.[10]

[7] SLI Compliance, "Dominion Democracy Suite 5.10 Voting System Software Test Report for California Secretary of State" (Aug. 2019), https://votingsystems.cdn.sos.ca.gov/vendors/dominion/dvs510software-report.pdf.

[8] *Id.*

[9] Joseph A. Calandrino, Ariel J. Feldman, J. Alex Halderman, David Wagner, Harlan Yu, and William Zeller, "Source Code Review of the Diebold Voting System," in *California Secretary of State's Top-to-Bottom Review of Voting Systems* (July 20, 2007), https://votingsystems.cdn.sos.ca.gov/oversight/ttbr/diebold-source-public-jul29.pdf.

[10] Andrew Springall, *Nation-State Attackers and their Effects on Computer Security* (2019), Ph.D. dissertation, University of Michigan, https://deepblue.lib.umich.edu/handle/2027.42/143907.

16. In addition to its complexity, the Dominion software used in Georgia utilizes a wide range of outdated off-the-shelf software modules, including some that perform essential security functions, such as the operating system and modules that process files an attacker might have manipulated.[11] The oldest third-party software components appear not to have been updated in more than 15 years. This is unfortunately consistent with the DRE-based system, which relied on software so out of date that the manufacturer stopped providing updates and patches more than a decade ago.

17. Outdated software components are a security risk because they frequently contain known, publicly documented vulnerabilities that have been corrected in later versions. Old or outdated software used in Georgia's Dominion equipment includes a version of Microsoft SQL Server dating from 2016, Adobe Acrobat from around 2015, barcode scanner software from 2015, μClinux operating system software from 2007, COLILO bootloader software from 2004, and a version of the Apache Avalon component framework dating from 2002. Georgia's BMDs

[11] SLI Compliance, "Dominion Voting Systems Democracy Suite 5.5-A Certification Test Plan" 16-19 (Dec. 2018), https://www.eac.gov/sites/default/files/voting_system/files/DVS_Democracy_D-Suite_5.5-A_Modification_Test_Plan_v1.2.pdf.

use the Android 5.1.1 operating system,[12] which is almost six years old and has not received security updates since March 2018; as of August 2020, it contained 254 documented vulnerabilities.[13]

18. Georgia certified the Dominion system without performing its own security testing or source-code review. The certification was preceded by tests that were limited to checking functional compliance with Georgia requirements.[14] The test report states that the testing "was not intended to result in exhaustive tests of system hardware and software attributes."[15] The term "security" does not appear in the report.

19. Several months before Georgia certified the Dominion system, the State of Texas performed its own certification tests. The Texas certification was more comprehensive and included test reports from five examiners appointed by the Texas

[12] Certificate of Conformance, Dominion Voting Systems Democracy Suite 5.5-A (Jan. 30, 2019) at pp. 3-4, https://www.eac.gov/file.aspx?A=TQycVTA%2BOLpxoCbwCFjQJmJdRP1dq9sFO3oVUWJl5u4%3D.

[13] CVE Details, "Google Android 5.1.1 Security Vulnerabilities," https://www.cvedetails.com/vulnerability-list/vendor_id-1224/product_id-19997/version_id-186573/Google-Android-5.1.1.html (last visited Aug. 19, 2020).

[14] Pro V&V, "Test Report: Dominion Voting Systems D-Suite 5.5-A Voting System Georgia State Certification Testing" (Aug. 7, 2019), https://sos.ga.gov/admin/uploads/Dominion_Test_Cert_Report.pdf.

[15] *Id*. at 3.

Secretary of State.[16] All of the examiners highlighted deficiencies with the Dominion system, including issues affecting its reliability, accessibility, and security. These problems led Texas to deny certification of the Dominion system in 2019.[17]

20. Several of the serious deficiencies noted by the Texas examiners affect system components used in Georgia, including the BMDs. One examiner noted that "the ICXs [BMDs] are built with a [commercial off-the-shelf] tablet and printer. The Android OS versions used on the tablets are several years old[;] therefore they do not have the latest security feature [*sic*.] as later Android releases."[18] A second examiner found that "[t]he doors covering data and power ports on the [BMD] tablets do not provide sufficient protection. […] a bad actor could add a USB device to the tablet while powered down that could remain undetected until after the election had ended."[19] A third examiner concluded that "[t]he ICX [BMD] also presented problems during the accessibility testing portion of the exam which demonstrate that it may not be suitable as an accessible voting system."[20]

[16] "Examiner Reports of Dominion Voting System Democracy Suite 5.5" (Jan. 16-17, 2019), https://www.sos.state.tx.us/elections/laws/jan2019_dominion.shtml.
[17] "Report of Review of Dominion Voting Systems Democracy Suite 5.5" (June 20, 2019), https://www.sos.state.tx.us/elections/forms/sysexam/dominion-democracy-suite-5.5.pdf
[18] Report of Texas examiner Tom Watson.
[19] Report of Texas examiner Brian Mechler.
[20] Report of Texas examiner Chuck Pinney.

21. Around the same time that Georgia certified the Dominion system, the State of California performed tests on a more recent version of the Dominion software, version 5.10, as part of its own certification process.[21]

22. In contrast to Georgia's tests, California's included some source code review and security testing. Like all security testing, the California tests were necessarily limited in scope and could not be expected to find all exploitable vulnerabilities. Nevertheless, they did uncover several serious flaws. These problems very likely apply to the version of the Dominion system used in Georgia given that it precedes the version tested in California.

23. The California testers found that attackers could modify the Dominion software installation files and believed that "it would be possible to inject more lethal payloads into the installers given the opportunity."[22] This implies that attackers could modify the Dominion installation files to infect election system components with malicious software.

[21] SLI Compliance, "Dominion Democracy Suite 5.10 Security and Telecommunications Test Report" (Aug. 2019), https://votingsystems.cdn.sos.ca.gov/vendors/dominion/dvs510security-report.pdf ("California Certification Security and Telecomm Test Report").
[22] *Id*. at 25.

24. Furthermore, the California testers found that the Dominion system's antivirus protection was insufficient or non-existent. "[O]n the EMS server, the AVAST Antivirus (AV) File Shield (the real time AV monitor) was only able to detect and clean one of the four [test] files. This potentially leaves the system open to zipped and double zipped viruses as well as infection strings in plain text."[23] Moreover, the ICX BMD and ICP scanner have no antivirus software at all.[24] As a result, malware that infected the Dominion components could evade antivirus detection.

25. One of the ways that attackers might affect election equipment is by physically accessing the devices. In the case of the Dominion BMD, the California source code reviewers found a vulnerability that can be exploited with physical access to the USB port that "would be open to a variety of actors including a voter, a poll worker, an election official insider, and a vendor insider."[25] This implies that no passwords or keys would be needed to exploit the problem, given physical access. California testers also found that "the ICX device does not provide monitoring of

[23] *Id*. at 19-20.

[24] *Id*. at 20.

[25] California Secretary of State's Office of Voting Systems Technology Assessment, "Dominion Voting Systems Democracy Suite 5.10 Staff Report" (Aug. 19, 2019) at 29, https://votingsystems.cdn.sos.ca.gov/vendors/dominion/dvs510staff-report.pdf.

physical security,"[26] and that, for all the polling place devices, including the ICX, "[s]ecurity seals, locks, and security screws can be circumvented."[27]

26. Other weaknesses found in the California tests include that "a number of passwords were able to be recovered that were stored in plain text,"[28] that the network switch used to connect EMS clients and servers was "determined to have twelve medium [severity] vulnerabilities and four low [severity] vulnerabilities,"[29] and that, if an authentication device used by poll workers and administrators was lost or stolen shortly before an election, revoking its access would require a logistically difficult process to reprogram the election files for the polling place devices throughout the jurisdiction.[30] These problems indicate that the Dominion system was designed without sufficient attention to security.

27. Although California ultimately permitted the Dominion system to be used, its certification requirements impose much more stringent security conditions

[26] California Certification Security and Telecomm Test Report at 11.
[27] *Id*. at 17.
[28] *Id*. at 15.
[29] *Id*. at 30.
[30] *Id*. at 15.

than those in Georgia, and no California jurisdiction uses Dominion BMDs for all voters as Georgia does.[31]

28. Dominion's response to Georgia's RFP lists among "key personnel" a "Chief Security Officer" (CSO) whose responsibilities for the voting system project were to be "Oversight of key security development and implementation."[32] Appointing a C-level executive to oversee a company's security posture is widely regarded as an industry best practice. However, at the time of the RFP, the CSO position was vacant, and to my knowledge Dominion has yet to fill the role.

BMDs and Ballot Barcodes Create Elevated Hacking Risks

29. Georgia's optical scanners use barcodes as the exclusive means of reading voters' choices. This increases the likelihood that attackers will be able to manipulate election results. The use of barcodes makes it possible for attackers to change how votes are recorded by hacking *either* the scanners or the BMDs. This

[31] California Secretary of State, "Conditional Approval of Dominion Voting Systems, Inc. Democracy Suite Version 5.10 Voting System" (Oct. 18, 2019), https://votingsystems.cdn.sos.ca.gov/vendors/dominion/ds510-cert.pdf.

[32] See "Original\0-4 Org Structure_Dominion and KNOWiNK - Redacted .pdf" at 3 *available at* https://sos.ga.gov/admin/uploads/Dominion.zip (last visited Aug. 19, 2020).

increases the “attack surface” of the election system: with two potentially vulnerable components to target instead of just one, attackers are more likely to succeed.

30. Georgia’s Dominion ICX BMDs are computers, they run outdated and vulnerable software, and they must be programmed using the State’s election management system before every election. Attackers could potentially infect Georgia’s BMDs with malware in several ways, including by spreading it from the election management system (EMS).

31. An attacker who infected the BMDs with malware could change a fraction of the printouts so that the barcodes encoded fraudulent votes but the human-readable text showed the voters’ true selections.

32. Voters would have no way to detect this attack. They cannot read the Dominion barcodes, which are encrypted, so it is impossible for them to verify whether the barcodes really match their selections. However, when the Dominion scanners tabulate BMD printouts, they ignore the printed text entirely and count only the votes encoded in the barcodes. This means that voters cannot verify the portion of their ballots that gets counted.

33. Such barcode attacks cannot be reliably detected using pre-election testing or parallel testing.[33] An attacker could decide which votes to modify based on a very large number of variables, including the time of day, the number of ballots cast, the voter's selections, and whether the voter used options such as a large font size or an audio ballot. It is impossible for any practical amount of testing to examine all sets of conditions under which attackers might choose to cheat.

34. In principle, a sufficiently rigorous audit that compared the human-readable portion of the printouts to the barcodes could detect such an attack. However, since attackers might choose to target any race in any election, every race and every election would need to be rigorously audited to rule out barcode-based fraud.

35. To my knowledge, Georgia has not announced plans to perform any kind of audit that would compare the barcodes and the printed text, nor what specific measures would be taken to render any potential audit sufficiently comprehensive and reliable.

36. Even if officials did detect that some ballots showed different choices in the barcode than in the text, there might be no way to determine the correct election

[33] *See* Philip B. Stark and Ran Xie, "Testing Cannot Tell Whether Ballot-Marking Devices Alter Election Outcomes" (2020), https://arxiv.org/pdf/1908.08144.pdf.

results. If the discrepancies resulted from an attack, this would cast doubt on *both* the barcodes and the ballot text. An attacker who was able to alter the barcode would be equally capable of altering the ballot text. Malware might be designed to sometimes alter only the barcode and sometimes only the text. This means that officials could not simply ignore the barcodes and count only the text if they suspected the BMDs had been compromised.

37. BMDs do not need to use barcodes. Several kinds of modern, EAC-certified BMDs deployed in other states do not use barcodes to encode votes. These include the Clear Ballot ClearAccess system[34] and the Hart Verity Touch Writer.[35] Instead of a barcode for vote tabulation, these systems print a ballot that looks like a hand-marked paper ballot but has scan targets filled in for the selected candidates.

38. In Dominion's response to the State's request for proposals, the company represented that an upcoming version of its BMD software would not need to print barcodes on ballots.[36] Instead, the BMDs would produce (and the scanners

[34] *See* Clear Ballot, "ClearAccess Accessible Voting," https://clearballot.com/products/clear-access.

[35] *See* Hart Intercivic, "Verity Touch Writer Ballot Marking Device," https://www.hartintercivic.com/wp-content/uploads/VerityTouchWriter.pdf.

[36] "Clarification Questions\MS 16-1 Supply Chain_Dominion and KNOWiNK Final.docx" *available at* https://sos.ga.gov/admin/uploads/Dominion.zip (last visited Aug. 19, 2020).

would count) an entirely human-readable ballot capable of verification by the voter. However, this option is described as an "upgrade" available only after "certification is complete at the EAC."

39. The Secretary of State's office and Dominion portray Georgia's BMDs as having this ability to print such a human-readable, "full-face" ballot. A video portraying such a capability is part of the "Important Voter Information" available to the public on the Secretary of State's elections security web page.[37] The video portrays a voter making her selections on a BMD displaying a mock ballot using Georgia state and local races and constitutional questions or referenda. At the end of the video, the voter selects "Print Ballot," and the attached printer produces a double-sided ballot with a darkened oval appearing next to the voter's selections.[38]

40. Dominion's in-precinct optical scanners already are capable of and certified to read such full-face paper ballots that do not encode votes using barcodes.

[37] https://www.dropbox.com/s/u0lc21u82ye2qpg/ICX%20BMD%20Cart.mp4, available through "Voting Cart" hyperlink at https://sos.ga.gov/securevoting (last visited Aug. 18, 2020).

[38] *Id.*

BMDs Limit the Effectiveness of Voter Verification

41. Even if Georgia were to implement rigorous post-election audits, BMDs make it possible for an attacker to compromise the auditability of the ballots and thereby undermine the primary goal of the paper trail. To do so, malware would cause the BMDs to sometimes print fraudulent selections in *both* the barcode and the human-readable text. This attack would be impossible to detect by auditing the printouts, because all records of the voter's intent would be wrong. Pre-election testing and parallel testing also cannot reliably detect such cheating.

42. Unlike the security of hand-marked paper ballots, the security of BMDs relies critically on voters themselves. The only practical way to discover a BMD attack that altered both the barcodes and the printed text would be if enough voters reviewed the printouts, noticed the errors, and alerted election officials. Yet several recent studies, including my own peer-reviewed research, have concluded that few

voters carefully review BMD printouts.[39,40,41] As a result, the BMD paper trail is not a reliable record of the votes expressed by the voters, and changes to enough printouts to change the winner of a close race would likely go undetected.

43. Even if some voters did notice that their selections were misprinted, these voters would have no way to prove that the BMDs were at fault. From an election official's perspective, the reporting voters might be mistaken or lying. Many voters would need to report that the BMDs misprinted their ballots before officials could be sure there was a systemic problem.

44. There are no protocols or policies in Georgia that I have found that address how many voter complaints, or other conditions, involving BMDs would be required within or across polling places to support a finding—or even a robust investigation—of a systemic problem. Moreover, it would be virtually impossible

[39] R. DeMillo, R. Kadel, and M. Marks, "What voters are asked to verify affects ballot verification: A quantitative analysis of voters' memories of their ballots" (2018). Available at https://ssrn.com/abstract=3292208.

[40] Matthew Bernhard, Allison McDonald, Henry Meng, Jensen Hwa, Nakul Bajaj, Kevin Chang, and J. Alex Halderman, "Can Voters Detect Malicious Manipulation of Ballot Marking Devices?" in *Proceedings of the 41st IEEE Symposium on Security and Privacy* (Jan. 2020), https://jhalderm.com/pub/papers/bmd-verifiability-sp20.pdf.

[41] Philip Kortum, Michael D. Byrne, and Julie Whitmore, "Voter Verification of BMD Ballots Is a Two-Part Question: Can They? Mostly, They Can. Do They? Mostly, They Don't" (Mar. 2020), https://arxiv.org/ftp/arxiv/papers/2003/2003.04997.pdf.

for officials to recognize the subtle signs of a BMD misprinting attack during a chaotic election in which there were widespread equipment malfunctions and other problems, as occurred in Georgia during the June 9, 2020 primary.[42]

45. Even if officials did suspect that the BMDs had been attacked, there would be no straightforward way to respond or recover. One possible response would be to delay certifying the election results and conduct a forensic analysis to understand why ballots were misprinted and how many BMDs and votes were affected. Such an analysis might take months and would not be guaranteed to uncover a sophisticated attack. Yet if an attack were confirmed, there is little chance that its effects could be undone. The only recourse might be to rerun the election, which could be statewide involving millions of voters across Georgia.

46. Election officials are unlikely to take disruptive actions, like a protracted and expensive forensic investigation, unless a large enough fraction of BMD voters report problems. Suppose officials would launch an investigation if more than 1% of BMD voters reported a problem. If outcome-changing fraud occurred in an election with a 1% margin of victory, voters would need to verify their ballots so

[42] Richard Fausset, Reid J. Epstein, and Rick Rojas, "'I Refuse Not to Be Heard': Georgia in Uproar Over Voting Meltdown," *The New York Times* (June 9, 2020), https://www.nytimes.com/2020/06/09/us/politics/atlanta-voting-georgia-primary.html.

carefully that they would report 67% of the modified BMD printouts. This is *ten times* greater than the rate of error reporting measured in my peer-reviewed research.

Reserving BMDs for Voters Who Request Them Would Strengthen Security

47. When BMDs are used by all in-person voters, as in Georgia, there is a high risk that attackers could manipulate enough BMD votes to change the outcome of a close election without detection. Georgia is an outlier in adopting BMDs for all voters. As of December 2019, only 403 counties in the United States planned to do so, and almost 40% of them were in Georgia.[43] In contrast, the majority of election jurisdictions across the U.S. (representing nearly two-thirds of registered voters) provide BMDs exclusively for voters who request them (e.g., those with certain disabilities),[44] which is much safer.

48. Georgia can greatly strengthen the security of future elections through a straightforward procedural change. Rather than directing all in-person voters to use BMDs, the State could have in-person voters mark paper ballots by hand and reserve BMDs for voters who request to use them. This approach would require no additional equipment and would result in no loss in accessibility. Hand-marked

[43] Decl. of Warren Stewart, Dckt. 681-2.

[44] Verified Voting, *The Verifier*, https://verifiedvoting.org/verifier/#mode/navigate/map/ppEquip/mapType/normal/year/2020 (last visited Aug. 18, 2020).

paper ballots are already used in Georgia for absentee voting, and so they are prepared and printed for every ballot style in every election. The state's new Dominion scanners are already capable of counting hand-marked ballots. BMDs would continue to be available for voters who need them. Yet the risk that election outcomes could be hacked would be far less than under Georgia's planned system.

49. Securing against misprinting attacks is much easier if only a small fraction of voters uses BMDs (without barcodes) and the rest use hand-marked paper ballots. This is because an attacker would be forced to cheat on a much larger fraction of BMD ballots in order to achieve the same level of fraud. In Maryland, which uses hand-marked paper ballots but makes BMDs available to voters who request them, about 2% of voters use BMDs. If only 2% of voters used BMDs in the scenario above (¶ 46), 1% of BMD voters would report a problem even if voters noticed only 3.8% of errors. Empirical studies suggest that voters really do achieve this modest rate of verification accuracy, even though it is unlikely they can achieve the far greater accuracy required to detect fraud when all voters use BMDs.

50. Using BMDs for all voters has no practical security advantages compared to reserving BMDs for voters who request them. On the contrary, it makes BMDs a much more attractive target for attackers and leads to greatly increased risks

for all voters—including the disabled—that their right to vote will be subverted by an attack on the BMDs. And regardless, there is no need for barcodes at all.

Georgia's Audits Provide Insufficient Protection

51. Rigorous post-election audits are necessary in order to reliably prevent attacks that compromise election results by manipulating ballot scanners. A rigorous audit would also serve to correct errors caused by scanners misreading ballots, to the extent that these errors resulted in an incorrect election outcome. However, as I have explained, post-election audits are not sufficient to detect attacks against BMDs, since such attacks could change both the printed and electronic records of the votes.

52. For an audit to reliably detect outcome-changing attacks, several requirements must be met. Among them are: (i) the paper ballots being audited must correctly reflect voters' selections; (ii) the audit needs to be conducted manually, by having people inspect the ballots without reliance on potentially compromised electronic systems or records; (iii) the auditors need to inspect sufficiently many ballots to ensure that the probability that outcome-changing fraud could go undetected is low. In general, the closer the election result in a particular race, the more ballots need to be audited in order to confidently rule out fraud. Audits that constrain the probability that the reported outcome differs from the outcome that

would be obtained by a full manual recount to no more than a pre-defined level (the "risk limit") are called risk-limiting audits ("RLAs").[45]

53. I understand that Georgia statute requires a state-wide post-election audit to be conducted no later than the November 2020 election.[46] However, that audit is not required to be risk-limiting. If it is not, and there are close races in which an attacker changes the outcome by hacking the election equipment, there is a high probability that the audit will fail to uncover the attack.

54. A proposed rule change recently noticed by the State Elections Board would require all counties to participate in a risk-limiting audit, but only following November general elections in even-numbered years.[47] Other elections, including state-wide primaries and runoffs, are not included in the requirement. Moreover, under the proposed rule, the RLA would target only one contest, which would be selected by the Secretary of State. Adversaries could choose to attack any race in

[45] *See* Mark Lindeman and Philip B. Stark, "A Gentle Introduction to Risk-limiting Audits," in *IEEE Security and Privacy* (2012), https://www.stat.berkeley.edu/~stark/Preprints/gentle12.pdf.

[46] *See* O.C.G.A. § 21-2-498(b).

[47] Georgia State Elections Board, "Notice of Intent to Post a Rule of the State Election Board, Title 183-1, *Rules of State Election Board*, Chapter 183-1-15, *Returns of Primaries and Elections* and Notice of Public Hearing" (Aug. 11, 2020), https://sos.ga.gov/admin/files/SEB%20Rule%20183-1-15-.02(2)%20and%20.04%20-%20To%20Post%20For%20Public%20Comment.pdf.

any election, and an attack would likely not be detected if it occurred in a contest that was not the target of the RLA or during an election for which no RLA was conducted. Even for the one contest every two years that would be audited, the proposed rule does not describe the auditing procedure in enough detail to evaluate its sufficiency. The specific process that election superintendents would follow to carry out the audit is yet to be defined.

55. No matter what auditing procedures Georgia applies, the state's widespread use of BMDs makes it possible for an attacker to undermine the integrity of the paper trail. Malware could cause the BMDs to print fraudulent selections, both in the barcode and the human-readable text. Such an attack would be impossible to detect by auditing the ballots, even with an RLA, because all records of the voter's intent would be wrong.

<u>Hand-Marked Paper Ballots Are Much More Secure</u>

56. Hand-marked paper ballots (HMPBs) are the most widely used voting technology in the United States. More than 65% of voters live in jurisdictions that use HMPBs as their primary in-person voting technology,[48] and all 50 states, including Georgia, use them for absentee voting. When used with modern precinct-

[48] Verified Voting, *The Verifier*.

count optical scanners and rigorous RLAs, HMPBs can provide much stronger security than BMD-printed ballots, especially those based on barcodes.

57. Virtually every class of attack that affects HMPBs also affects BMDs, but BMDs—especially those that use barcodes—additionally suffer from the serious possibility that malicious software will alter the voter's choices without detection. In contrast, HMPBs can be well secured using existing election technology and procedural controls.

58. It is true that voters using hand-marked paper ballots sometimes make errors. However, modern ballot scanners, such as Georgia's Dominion ICPs, can be programmed to detect the most common types of errors by voters, such as overvotes and undervotes. Where ballots are scanned in-precinct, and the scanners are programmed correctly, voters then have the opportunity to correct their ballots once the scanners report the errors. Scanners also sometimes misread voters' marks, but such errors—to the extent that they affected an election outcome—would be detected and corrected during risk-limiting audits, which are necessary in any event in order to safeguard against outcome-changing attacks.

Georgia Elections Continue to be Threatened by Sophisticated Adversaries

59. Georgia's election system continues to face a high risk of being targeted by sophisticated adversaries, including Russia and other hostile foreign

governments. These adversaries could attempt to hack the election system to achieve a variety of goals, including undermining the legitimacy of the democratic process and causing fraudulent election outcomes.

60. The Mueller Report recently outlined the scale and sophistication of Russia's efforts to interfere in the 2016 election, leaving no doubt that Russia and other adversaries will strike again.[49] The Special Counsel concluded principally that "[t]he Russian government interfered in the 2016 presidential election in sweeping and systematic fashion."[50] The report further explained that foreign actors "sought access to state and local computer networks by exploiting known software vulnerabilities on websites of state and local governmental entities."[51] The report also found that these foreign agents were successful in attacking at least one state and that their activities involved "more than two dozen states."[52] As noted prior to the Special Counsel's final report, Georgia was among the states that Russia targeted.[53]

[49] Special Counsel Robert S. Mueller III, *Report on the Investigation into Russian Interference in the 2016 Presidential Election (Volume I of II)*, United States Department of Justice (Mar. 2019), https://www.justice.gov/storage/report.pdf.
[50] *Id.* at 1.
[51] *Id.* at 50.
[52] *Id.*
[53] *See* Indictment ¶ 75, *United States v. Netyksho*, No. 1:18-cr-00215-ABJ, (D.D.C. July 13, 2018), ECF No. 1.

61. Russia has sophisticated cyber-offensive capabilities, and it has shown a willingness to use them to hack elections elsewhere even before 2016. For instance, according to published reports, during the 2014 presidential election in Ukraine, attackers linked to Russia sabotaged Ukraine's vote counting infrastructure, and Ukrainian officials succeeded only at the last minute in defusing vote-stealing malware that would have caused the wrong winner to be announced.[54]

62. Russia and other foreign governments continue to threaten Georgia's elections in 2020. As recently as this month, the U.S. Intelligence Community assessed that foreign threats to the 2020 election include "ongoing and potential activity" from Russia, China, and Iran, concluding that "[f]oreign efforts to influence or interfere with our elections are a direct threat to the fabric of our democracy."[55] These adversarial governments may "seek to compromise our election infrastructure

[54] Mark Clayton, "Ukraine election narrowly avoided 'wanton destruction' from hackers," *The Christian Science Monitor* (June 17, 2014), https://www.csmonitor.com/World/Passcode/2014/0617/Ukraine-election-narrowly-avoided-wanton-destruction-from-hackers.

[55] Office of the Director of National Intelligence, "Statement by NCSC Director William Evanina: Election Threat Update for the American Public" (Aug. 7, 2020), https://www.dni.gov/index.php/newsroom/press-releases/item/2139-statement-by-ncsc-director-william-evanina-election-threat-update-for-the-american-public.

for a range of possible purposes, such as interfering with the voting process, stealing sensitive data, or calling into question the validity of the election results."[56]

63. Georgia's BMD-based election system does not achieve the level of security necessary to withstand an attack by these sophisticated adversaries. Despite the addition of a paper trail, it suffers from severe security risks much like those of the DRE-based election system it replaced. Like paperless DREs, Georgia's BMDs are vulnerable to attacks that have the potential to change all records of a vote.

I declare under penalty of the perjury laws of the State of Georgia and the United States that the foregoing is true and correct and that this declaration was executed this 19th day of August, 2020 in Rushland, Pennsylvania.

J. ALEX HALDERMAN

[56] *Id.*

Exhibit 10

Antrim Michigan Forensics Report, Revised Preliminary Summary, v2

Allied Security Operations Group

Antrim Michigan Forensics Report

REVISED PRELIMINARY SUMMARY, v2

Report Date 12/13/2020

Client: **Bill Bailey**

Attorney: **Matthew DePerno**

A. WHO WE ARE

1. My name is Russell James Ramsland, Jr., and I am a resident of Dallas County, Texas. I hold an MBA from Harvard University, and a political science degree from Duke University. I have worked with the National Aeronautics and Space Administration (NASA) and the Massachusetts Institute of Technology (MIT), among other organizations, and have run businesses all over the world, many of which are highly technical in nature. I have served on technical government panels.

2. I am part of the management team of Allied Security Operations Group, LLC, (ASOG). ASOG is a group of globally engaged professionals who come from various disciplines to include Department of Defense, Secret Service, Department of Homeland Security, and the Central Intelligence Agency. It provides a range of security services, but has a particular emphasis on cybersecurity, open source investigation and penetration testing of networks. We employ a wide variety of cyber and cyber forensic analysts. We have patents pending in a variety of applications from novel network security applications to SCADA (Supervisory Control and Data Acquisition) protection and safe browsing solutions for the dark and deep web. For this report, I have relied on these experts and resources.

B. PURPOSE AND PRELIMINARY CONCLUSIONS

1. The purpose of this forensic audit is to test the integrity of Dominion Voting System in how it performed in Antrim County, Michigan for the 2020 election.

2. We conclude that the Dominion Voting System is intentionally and purposefully designed with inherent errors to create systemic fraud and influence election results. The system intentionally generates an enormously high number of ballot errors. The electronic ballots are then transferred for adjudication. The intentional errors lead to bulk adjudication of ballots with no oversight, no transparency, and no audit trail. This leads to voter or election fraud. Based on our study, we conclude that The Dominion Voting System should not be used in Michigan. We further conclude that the results of Antrim County should not have been certified.

3. The following is a breakdown of the votes tabulated for the 2020 election in Antrim County, showing different dates for the tabulation of the same votes.

Date	Registered Voters	Total Votes Cast	Biden	Trump	Third Party	Write-In	TOTAL VOTES for President
Nov 3	22,082	16,047	7,769	4,509	145	14	12,423
Nov 5	22,082	18,059	7,289	9,783	255	20	17,327
Nov 21	22,082	16,044	5,960	9,748	241	23	15,949

4. The Antrim County Clerk and Secretary of State Jocelyn Benson have stated that the election night error (detailed above by the vote "flip" from Trump to Biden, was the result of human error caused by the failure to update the Mancelona Township tabulator prior to election night for a down ballot race. We disagree and conclude that the vote flip occurred because of machine error built into the voting software designed to create error.

5. Secretary of State Jocelyn Benson's statement on November 6, 2020 that "[t]the correct results always were and continue to be reflected on the tabulator totals tape . . . ." was false.

6. The allowable election error rate established by the Federal Election Commission guidelines is of 1 in 250,000 ballots (.0008%). We observed an error rate of 68.05%. This demonstrated a significant and fatal error in security and election integrity.

7. The results of the Antrim County 2020 election are not certifiable. This is a result of machine and/or software error, not human error.

8. The tabulation log for the forensic examination of the server for Antrim County from December 6, 2020consists of 15,676 individual events, of which 10,667 or 68.05% of the events were recorded errors. These errors resulted in overall tabulation errors or ballots being sent to adjudication. This high error rates proves the Dominion Voting System is flawed and does not meet state or federal election laws.

9. These errors occurred after The Antrim County Clerk provided a re-provisioned CF card with uploaded software for the Central Lake Precinct on November 6, 2020. This means the statement by Secretary Benson was false. The Dominion Voting System produced systemic errors and high error rates both prior to the update and after the update; meaning the update (or lack of update) is not the cause of errors.

10. In Central Lake Township there were 1,222 ballots **reversed** out of 1,491 total ballots cast, resulting in an 81.96% rejection rate. All reversed ballots are sent to adjudication for a decision by election personnel.

11. It is critical to understand that the Dominion system classifies ballots into two categories, 1) normal ballots and 2) adjudicated ballots. Ballots sent to adjudication can be altered by administrators, and adjudication files can be moved between different Results Tally and Reporting (RTR) terminals with no audit trail of which administrator actually adjudicates (i.e. votes) the ballot batch. This demonstrated a significant and fatal error in security and election integrity because it provides no meaningful observation of the adjudication process or audit trail of which administrator actually adjudicated the ballots.

12. A staggering number of votes required adjudication. This was a 2020 issue not seen in previous election cycles still stored on the server. This is caused by intentional errors in the system. The intentional errors lead to bulk adjudication of ballots with no oversight, no transparency or audit trail. Our examination of the server logs indicates that this high error rate was incongruent with patterns from previous years. The statement attributing these issues to human error is not consistent with the forensic evaluation, which points more correctly to systemic machine and/or software errors. The systemic errors are intentionally designed to create errors in order to push a high volume of ballots to bulk adjudication.

13. The linked video demonstrates how to cheat at adjudication:

https://mobile.twitter.com/KanekoaTheGreat/status/1336888454538428418

14. Antrim County failed to properly update its system. A purposeful lack of providing basic computer security updates in the system software and hardware demonstrates incompetence, gross negligence, bad faith, and/or willful non-compliance in providing the fundamental system security required by federal and state law. There is no way this election management system could have passed tests or have been legally certified to conduct the 2020 elections in Michigan under the current laws. According to the National Conference of State Legislatures – Michigan requires full compliance with federal standards as determined by a federally accredited voting system laboratory.

15. Significantly, the computer system shows vote adjudication logs for prior years; but all adjudication log entries for the 2020 election cycle are missing. The adjudication process is the simplest way to manually manipulate votes. The lack of records prevents any form of audit accountability, and their conspicuous absence is extremely suspicious since the files exist for previous years using the same software. Removal of these files violates state law and prevents a meaningful audit, even if the Secretary wanted to conduct an audit. We must conclude that the 2020 election cycle records have been manually removed.

16. Likewise, all server security logs prior to 11:03 pm on November 4, 2020 are missing. This means that all security logs for the day after the election, on election day, and prior to election day are gone. Security logs are very important to an audit trail, forensics, and for detecting advanced persistent threats and outside attacks, especially on systems with outdated system files. These logs would contain domain controls, authentication failures, error codes, times users logged on and off, network connections to file servers between file accesses, internet connections, times, and data transfers. Other server logs before November 4, 2020 are present; therefore, there is no reasonable explanation for the security logs to be missing.

17. On November 21, 2020, an unauthorized user unsuccessfully attempted to zero out election results. This demonstrates additional tampering with data.

18. The Election Event Designer Log shows that Dominion ImageCast Precinct Cards were programmed with new ballot programming on 10/23/2020 and then again after the election on 11/05/2020. These system changes affect how ballots are read and tabulated, and our examination demonstrated a significant change in voter results using the two different programs. In accordance with the Help America Vote Act, this violates the 90-day Safe Harbor Period which prohibits changes to election systems, registries, hardware/software updates without undergoing re-certification. According to the National Conference of State Legislatures – Michigan requires full compliance with federal standards as determined by a federally accredited voting system laboratory.

19. The only reason to change software after the election would be to obfuscate evidence of fraud and/or to correct program errors that would de-certify the election. Our findings show that the Central Lake Township tabulator tape totals were significantly altered by utilizing two different program versions (10/23/2020 and 11/05/2020), both of which were software changes during an election which violates election law, and not just human error associated with the **Dominion Election Management System.** This is clear evidence of software generated movement of votes. The claims made on the **Office of the Secretary of State** website are false.

20. The Dominion ImageCast Precinct (ICP) machines have the ability to be connected to the internet (see Image 11). By connecting a network scanner to the ethernet port on the ICP machine and creating Packet Capture logs from the machines we examined show the ability to connect to the network, Application Programming Interface (API) (a data exchange between two different systems) calls and web (http) connections to the Election Management System server. Best practice is to disable the network interface card to avoid connection to the internet. This demonstrated a significant and fatal error in security and election integrity. Because certain files have been deleted, we have not yet found origin or destination; but our research continues.

21. Because the intentional high error rate generates large numbers of ballots to be adjudicated by election personnel, we must deduce that bulk adjudication occurred. However, because files and adjudication logs are missing, we have not yet determined where the bulk adjudication occurred or who was responsible for it. Our research continues.

22. Research is ongoing. However, based on the preliminary results, we conclude that the errors are so significant that they call into question the integrity and legitimacy of the results in the Antrim County 2020 election to the point that the results are not certifiable. Because the same machines and software are used in 48 other counties in Michigan, this casts doubt on the integrity of the entire election in the state of Michigan.

23. DNI Responsibilities: President Obama signed Executive Order on National Critical Infrastructure on 6 January 2017, stating in Section 1. Cybersecurity of Federal Networks, "The Executive Branch operates its information technology (IT) on behalf of the American people. The President will hold heads of executive departments and agencies (agency heads) accountable for managing cybersecurity risk to their enterprises. In addition, because risk management decisions made by agency heads can affect the risk to the executive branch as a whole, and to national security, it is also the policy of the United States to manage cybersecurity risk as an executive branch enterprise." President Obama's EO further stated, effective immediately, each agency head shall use The Framework for Improving Critical Infrastructure Cybersecurity (the Framework) developed by the National Institute of Standards and Technology." Support to Critical Infrastructure at Greatest Risk. The Secretary of Homeland Security, in coordination with the Secretary of Defense, the Attorney General, the Director of National Intelligence, the Director of the Federal Bureau of Investigation, the heads of appropriate sector-specific agencies, as defined in Presidential Policy Directive 21 of February 12, 2013 (Critical Infrastructure Security and Resilience) (sector-specific agencies), and all other appropriate agency heads, as identified by the Secretary of Homeland Security, shall: (i) identify authorities and capabilities that agencies could employ to support the cybersecurity efforts of critical infrastructure entities identified pursuant to section 9 of Executive Order 13636 of February 12, 2013 (Improving Critical Infrastructure Cybersecurity), to be at greatest risk of attacks that could reasonably result in catastrophic regional or national effects on public health or safety, economic security, or national security (section 9 entities);

This is a national security imperative. **In July 2018, President Trump strengthened President Obama's Executive Order to include requirements to ensure US election systems, processes, and its people were not manipulated by foreign meddling, either through electronic or systemic manipulation, social media, or physical changes made in hardware, software, or supporting systems.** The 2018 Executive Order. Accordingly, I hereby order:

Section 1. (a) Not later than 45 days after the conclusion of a United States election, the Director of National Intelligence, in consultation with the heads of any other appropriate executive departments and agencies (agencies), shall conduct an assessment of any information indicating that a foreign government, or any person acting as an agent of or on behalf of a foreign government, has acted with the intent or purpose of interfering in that election. The assessment shall identify, to the maximum extent ascertainable, the nature of any foreign interference and any methods employed to execute it, the persons involved, and the foreign government or governments that authorized, directed, sponsored, or supported it. The Director of National Intelligence shall deliver this assessment and appropriate supporting information to the President, the Secretary of State, the Secretary of the Treasury, the Secretary of Defense, the Attorney General, and the Secretary of Homeland Security.

We recommend that an independent group should be empaneled to determine the extent of the adjudication errors throughout the State of Michigan. This is a national security issue.

24. Michigan resident Gustavo Delfino, a former professor of mathematics in Venezuela and alumni of University of Michigan, offered a compelling affidavit [Exhibit 2] recognizing the inherent vulnerabilities in the SmartMatic electronic voting machines (software which was since incorporated into Dominion Voting Systems) during the 2004 national referendum in Venezuela (see attached declaration). After 4 years of research and 3 years of undergoing intensive peer review, Professor Delfino's paper was published in the highly respected "Statistical Science" journal, November 2011 issue (Volume 26, Number 4) with title "Analysis of the 2004 Venezuela Referendum: The Official Results Versus the Petition Signatures." The intensive study used multiple mathematical approaches to ascertain the voting results found in the 2004 Venezuelan referendum. Delfino and his research partners discovered not only the algorithm used to manipulate the results, but also the precise location in the election processing sequence where vulnerability in machine processing would provide such an opportunity. According to Prof Delfino, the magnitude of the difference between the official and the true result in Venezuela estimated at 1,370,000 votes. Our investigation into the error rates and results of the Antrim County voting tally reflect the same tactics, which have also been reported in other Michigan counties as well. This demonstrates a national security issue.

C. PROCESS

We visited Antrim County twice: November 27, 2020 and December 6, 2020.

On November 27, 2020, we visited Central Lake Township, Star Township, and Mancelona Township. We examined the Dominion Voting Systems tabulators and tabulator roles.

On December 6, 2020, we visited the Antrim County Clerk's office. We inspected and performed forensic duplication of the following:

1. **Antrim County Election Management Server** running **Dominion Democracy Suite** 5.5.3-002;

2. **Compact Flash** cards used by the local precincts in their **Dominion ImageCast Precinct;**

3. **USB memory sticks** used by the **Dominion VAT** (Voter Assist Terminals); and

4. **USB memory sticks** used for the Poll Book.

Dominion voting system is a Canadian owned company with global subsidiaries. It is owned by Staple Street Capital which is in turn owned by UBS Securities LLC, of which 3 out of their 7 board members are Chinese nationals. The Dominion software is licensed from Smartmatic which is a Venezuelan owned and controlled company. Dominion Server locations have been determined to be in Serbia, Canada, the US, Spain and Germany.

D. CENTRAL LAKE TOWNSHIP

1. On November 27, 2020, part of our forensics team visited the Central Lake Township in Michigan to inspect the **Dominion ImageCast Precint** for possible hardware issues on behalf of a local lawsuit filed by Michigan attorney Matthew DePerno on behalf of William Bailey. In our conversations with the clerk of **Central Lake Township** Ms. Judith L. Kosloski, she presented to us "two separate paper totals tape" from Tabulator ID 2.

   - One dated "Poll Opened Nov. 03/2020 06:38:48" (Roll 1);

   - Another dated "Poll Opened Nov. 06/2020 09:21:58" (Roll 2).

2. We were then told by Ms. Kosloski that on November 5, 2020, Ms. Kosloski was notified by Connie Wing of the County Clerk's Office and asked to bring the tabulator and ballots to the County Clerk's office for re-tabulation. They ran the ballots and printed "Roll 2". She noticed a difference in the votes and brought it up to the clerk, but canvasing still occurred, and her objections were not addressed.

3. Our team analyzed both rolls and compared the results. Roll 1 had **1,494** total votes and Roll 2 had **1,491** votes (Roll 2 had 3 less ballots because 3 ballots were damaged in the process.)

4. "Statement of Votes Cast from Antrim" shows that only **1,491** votes were counted, and the **3** ballots that were damaged were not entered into final results.

5. Ms. Kosloski stated that she and her assistant manually refilled out the three ballots, curing them, and ran them through the ballot counting system - but the final numbers do not reflect the inclusion of those **3** damaged ballots.

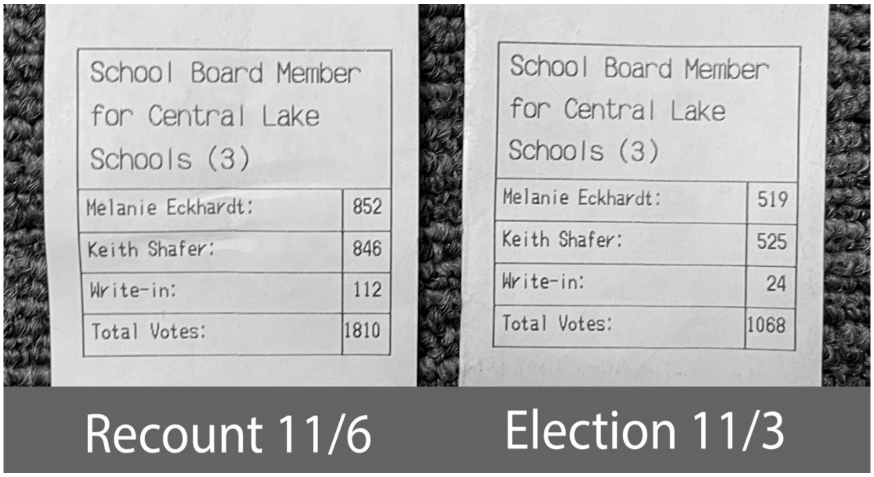
6. This is the most preliminary report of serious election fraud indicators. In comparing the numbers on both rolls, *we estimate **1,474** votes changed* across the two rolls, between the first and the second time the exact same ballots were run through the County Clerk's vote counting machine - *which is almost the same number of voters that voted in total.*

   - ***742** votes were added to* **School Board Member for Central Lake Schools (3)**
   - ***657** votes were removed from* **School Board Member for Ellsworth Schools (2)**
   - **7** votes were added to the total for **State Proposal 20-1 (1)** and out of those there were **611** votes moved between the Yes and No Categories.

7. There were incremental changes throughout the rolls with some significant adjustments between the 2 rolls that were reviewed. This demonstrates conclusively that votes can be and were changed during the second machine count after the software update. That should be impossible especially at such a high percentage to total votes cast.

8. For the **School Board Member for Central Lake Schools (3)** [Image 1] there were **742 votes** added to this vote total. Since multiple people were elected, this did not change the result of both candidates being elected, but one does see a change in who had most votes. If it were a single-person election this would have changed the outcome and demonstrates conclusively that votes can be and were changed during the second machine counting. That should be impossible.

[Image 1]:



School Board Member for Central Lake Schools (3)	
Melanie Eckhardt:	852
Keith Shafer:	846
Write-in:	112
Total Votes:	1810

Recount 11/6

School Board Member for Central Lake Schools (3)	
Melanie Eckhardt:	519
Keith Shafer:	525
Write-in:	24
Total Votes:	1068

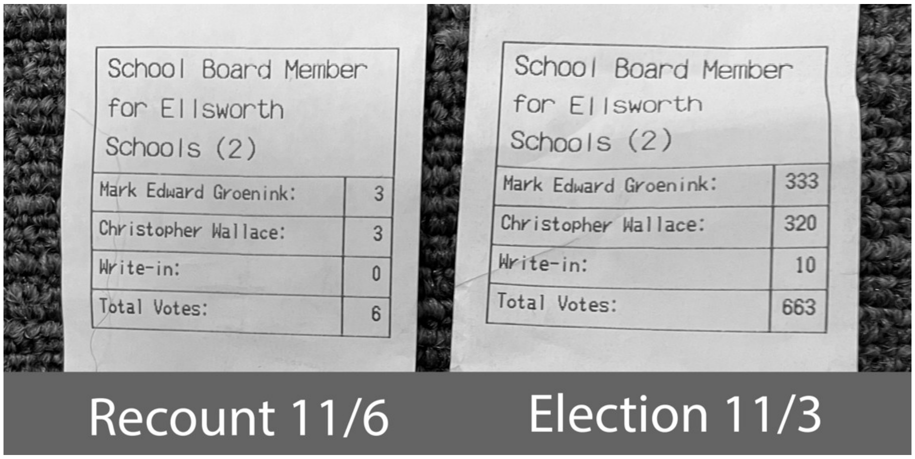
Election 11/3

9. For the **School Board Member for Ellsworth Schools (2)** [Image 2]

- Shows ***657*** *votes being removed* from this election.
- In this case, only **3** people who were eligible to vote actually voted. Since there were **2** votes allowed for each voter to cast.
- The recount correctly shows **6** votes.

But on election night, there was a major calculation issue:

[Image 2]:



School Board Member for Ellsworth Schools (2)	
Mark Edward Groenink:	3
Christopher Wallace:	3
Write-in:	0
Total Votes:	6

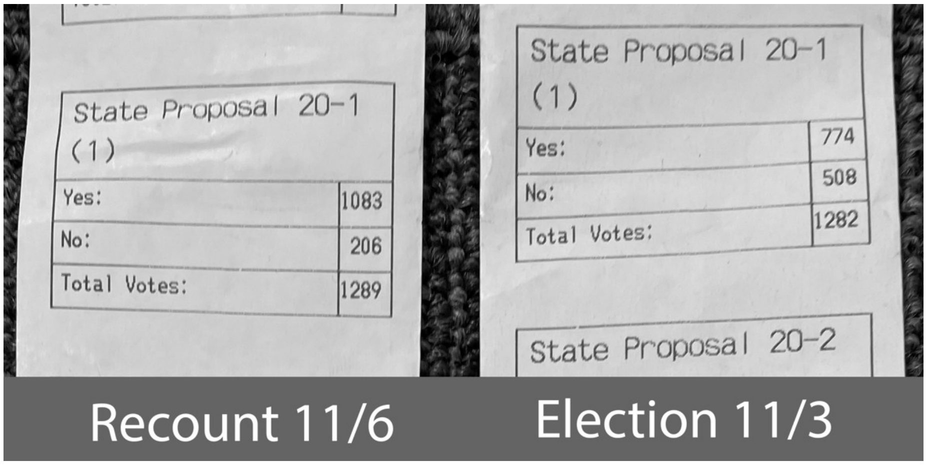
School Board Member for Ellsworth Schools (2)	
Mark Edward Groenink:	333
Christopher Wallace:	320
Write-in:	10
Total Votes:	663

Recount 11/6 Election 11/3

10. In **State Proposal 20-1 (1)**, [Image 3] there is a major change in votes in this category.

- There were **774 votes for YES** during the election, to **1,083 votes for YES** on the recount a change of **309 votes**.
- **7** votes were added to the total for **State Proposal 20-1 (1)** out of those there were **611** votes moved between the Yes and No Categories.

[Image 3]:



State Proposal 20-1
(1)

Yes:	1083
No:	206
Total Votes:	1289

Recount 11/6

State Proposal 20-1
(1)

Yes:	774
No:	508
Total Votes:	1282

State Proposal 20-2

Election 11/3

11. **State Proposal 20-1 (1)** is a fairly technical and complicated proposed amendment to the Michigan Constitution to change the disposition and allowable uses of future revenue generated from oil and gas bonuses, rentals and royalties from state-owned land. Information about the proposal: https://crcmich.org/publications/statewide-ballot-proposal-20-1-michigan-natural-resources-trust-fund

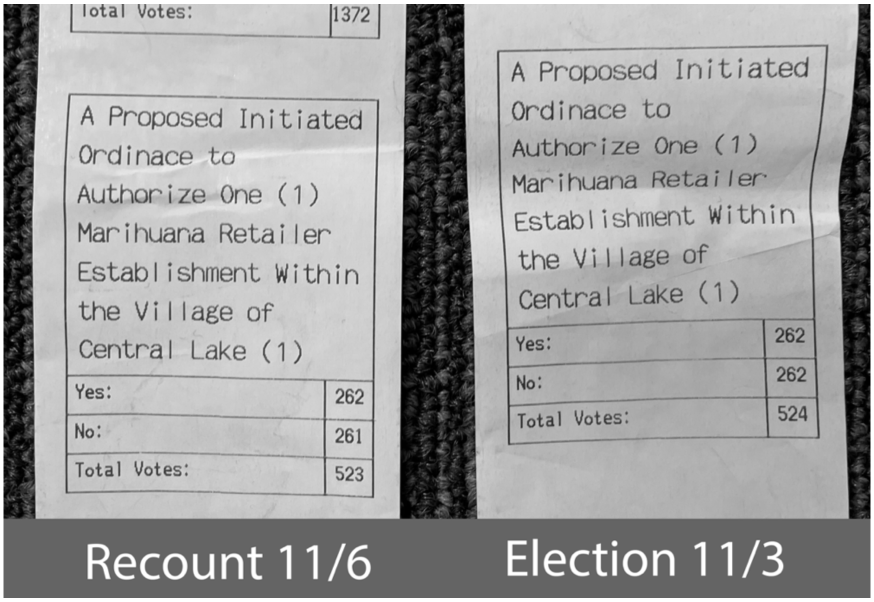
12. A Proposed Initiated **Ordinance to Authorize One (1) Marihuana (sic) Retailer Establishment Within the Village of Central Lake (1).** [Image 4]

    - On election night, it was a tie vote.

    - Then, on the rerun of ballots 3 ballots were destroyed, but only one vote changed on the totals to allow the proposal to pass.

When **3 ballots were not counted** and **programming change on the tabulator was installed** the proposal **passed with 1 vote being removed from the No** vote.

[Image 4]:



Total Votes:	1372

A Proposed Initiated
Ordinace to
Authorize One (1)
Marihuana Retailer
Establishment Within
the Village of
Central Lake (1)

Yes:	262
No:	261
Total Votes:	523

A Proposed Initiated
Ordinace to
Authorize One (1)
Marihuana Retailer
Establishment Within
the Village of
Central Lake (1)

Yes:	262
No:	262
Total Votes:	524

Recount 11/6 Election 11/3

13. On Sunday December 6, 2020, our forensics team visited the Antrim County Clerk. There were two USB memory sticks used, one contained the software package used to tabulate election results on November 3, 2020, and the other was programmed on November 6, 2020 with a different software package which yielded significantly different voting outcomes. The election data package is used by the **Dominion Democracy Suite** software & election management system software to upload programming information onto the Compact Flash Cards for the **Dominion ImageCast Precinct** to enable it to calculate ballot totals.

14. This software programming should be standard across all voting machines systems for the duration of the entire election if accurate tabulation is the expected outcome as required by US Election Law. This intentional difference in software programming is a design feature to alter election outcomes.

15. The election day outcomes were calculated using the original software programming on November 3, 2020. On November 5, 2020 the township clerk was asked to re-run the Central Lake Township ballots and was given no explanation for this unusual request. On November 6, 2020 the Antrim County Clerk, Sheryl Guy issued the second version of software to re-run the same Central Lake Township ballots and oversaw the process. This resulted in greater than a 60% change in voting results, inexplicably impacting every single election contest in a township with less than 1500 voters. These errors far exceed the ballot error rate standard of 1 in 250,000 ballots (.0008%) as required by federal election law.

- The original election programming files are last dated 09/25/2020 1:24pm

- The updated election data package files are last dated 10/22/2020 10:27 am.

16. As the tabulator tape totals prove, there were large numbers of votes switched from the November 3, 2020 tape to the November 6, 2020 tape. This was solely based on using different software versions of the operating program to calculate votes, not tabulate votes. This is evidenced by using same the Dominion System with two different software program versions contained on the two different USB Memory Devices.

17. The Help America Vote Act, Safe Harbor provides a 90-day period prior to elections where no changes can be made to election systems. To make changes would require recertification of the entire system for use in the election. The Dominion User Guide prescribes the proper procedure to test machines with test ballots to compare the results to validate machine functionality to determine if the **Dominion ImageCast Precinct** was programmed correctly. If this occurred a ballot misconfiguration would have been identified. Once the software was updated to the 10/22/2020 software the test ballots should have been re-run to validate the vote totals to confirm the machine was configured correctly.

18. The November 6, 2020 note from **The Office of the Secretary of State Jocelyn Benson** states: "The correct results always were and continue to be reflected on the tabulator totals tape and on the ballots themselves. Even if the error in the reported unofficial results had not been quickly noticed, it would have been identified during the county canvass. Boards of County Canvassers, which are composed of 2 Democrats and 2 Republicans, review the printed totals tape from each tabulator during the canvass to verify the reported vote totals are correct."

- Source: https://www.michigan.gov/sos/0,4670,7-127-1640_9150-544676--,00.html

19. The **Secretary of State Jocelyn Benson's** statement is false. Our findings show that the tabulator tape totals were significantly altered by utilization of two different program versions, and not just the **Dominion Election Management System.** This is the opposite of the claim that the **Office of the Secretary of State** made on its website. The fact that these significant errors were not caught in ballot testing and not caught by the local county clerk shows that there are major inherent built-in vulnerabilities and process flaws in the **Dominion Election Management System**, and that other townships/precincts and the entire election have been affected.

20. On Sunday December 6, 2020, our forensics team visited the Antrim County Clerk office to perform forensic duplication of the **Antrim County Election Management Server** running **Dominion Democracy Suite** 5.5.3-002.

21. Forensic copies of the **Compact Flash** cards used by the local precincts in their **Dominion ImageCast Precinct** were inspected, **USB memory sticks** used by the **Dominion VAT** (Voter Assist Terminals) and the **USB memory sticks** used for the Poll Book were forensically duplicated.

22. We have been told that the ballot design and configuration for the **Dominion ImageCast Precinct** and VAT were provided by **ElectionSource.com** which is which is owned by MC&E, Inc of Grand Rapids, MI.

E. MANCELONA TOWNSHIP

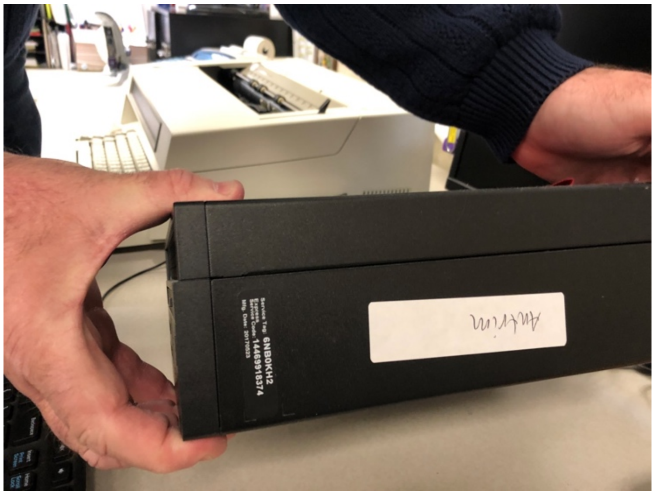
1. In Mancelona township, problems with software versions were also known to have been present. Mancelona elections officials understood that ballot processing issued were not accurate and used the second version of software to process votes on 4 November, again an election de-certifying event, as no changes to the election system are authorized by law in the 90 days preceding elections without re-certification.

2. Once the 10/22/2020 software update was performed on the Dominion ImageCast Precinct the test ballot process should have been performed to validate the programming. There is no indication that this procedure was performed.

F. ANTRIM COUNTY CLERK'S OFFICE

1. Pursuant to a court ordered inspection, we participated in an onsite collection effort at the Antrim County Clerk's office on December 6, 2020. [Image 5]:

Among other items forensically collected, the Antrim County Election Management Server (EMS) with Democracy Suite was forensically collected. [Images 6 and 7].



The EMS (Election Management Server) was a:

Dell Precision Tower 3420.

Service Tag: 6NB0KH2

The EMS contained 2 hard drives in a RAID-1 configuration. That is the 2 drives redundantly stored the same information and the server could continue to operate if either of the 2 hard drives failed. The EMS was booted via the Linux Boot USB memory sticks and both hard drives were forensically imaged.

At the onset of the collection process we observed that the initial program thumb drive was not secured in the vault with the CF cards and other thumbdrives. We watched as the County employees, including Clerk Sheryl Guy searched throughout the office for the missing thumb drive. Eventually they found the missing thumb drive in an unsecured and unlocked desk drawer along with multiple other random thumb drives. This demonstrated a significant and fatal error in security and election integrity.

G. FORENSIC COLLECTION

We used a built for purpose Linux Boot USB memory stick to boot the EMS in a forensically sound mode. We then used Ewfacquire to make a forensic image of the 2 independent internal hard drives.

Ewfacquire created an E01 file format forensic image with built-in integrity verification via MD5 hash.

We used Ewfverify to verify the forensic image acquired was a true and accurate copy of the original disk. That was done for both forensic images.

H. ANALYSIS TOOLS

X-Ways Forensics: We used X-Ways Forensics, a commercial Computer Forensic tool, to verify the image was useable and full disk encryption was not in use. In particular we confirmed that Bit locker was not in use on the EMS.

Other tools used: PassMark – OSForensics, Truxton - Forensics, Cellebrite – Physical Analyzer, Blackbag-Blacklight Forensic Software, Microsoft SQL Server Management Studio, Virtual Box, and miscellaneous other tools and scripts.

I. SERVER OVERVIEW AND SUMMARY

1. Our initial audit on the computer running the Democracy Suite Software showed that standard computer security best practices were not applied. These minimum-security standards are outlined the 2002 HAVA, and FEC Voting System Standards – it did not even meet the minimum standards required of a government desktop computer.

2. The election data software package USB drives (November 2020 election, and November 2020 election updated) are secured with bitlocker encryption software, but they were not stored securely on-site. At the time of our forensic examination, the election data package files were already moved to an unsecure desktop computer and were residing on an unencrypted hard drive. This demonstrated a significant and fatal error in security and election integrity. Key Findings on Desktop and Server Configuration: - There were multiple Microsoft security updates as well as Microsoft SQL Server updates which should have been deployed, however there is no evidence that these security patches were ever installed. As described below, many of the software packages were out of date and vulnerable to various methods of attack.

   a) Computer initial configuration on 10/03/2018 13:08:11:911

   b) Computer final configuration of server software on 4/10/2019

   c) Hard Drive not Encrypted at Rest

   d) Microsoft SQL Server Database not protected with password.

   e) Democracy Suite Admin Passwords are reused and share passwords.

   f) Antivirus is 4.5 years outdated

   g) Windows updates are 3.86 years out of date.

   h) When computer was last configured on 04/10/2019 the windows updates were 2.11 years out of date.

   i) User of computer uses a Super User Account.

3. The hard drive was not encrypted at rest – which means that if hard drives are removed or initially booted off an external USB drive the files are susceptible to manipulation directly. An attacker is able to mount the hard drive because it is unencrypted, allowing for the manipulation and replacement of any file on the system.

4. The Microsoft SQL Server database files were not properly secured to allow modifications of the database files.

5. The Democracy Suite Software user account logins and passwords are stored in the unsecured database tables and the multiple Election System Administrator accounts share the same password, which means that there are no audit trails for vote changes, deletions, blank ballot voting, or batch vote alterations or adjudication.

6. Antivirus definition is 1666 days old on 12/11/2020. Antrim County updates its system with USB drives. USB drives are the most common vectors for injecting malware into computer systems. The failure to properly update the antivirus definition drastically increases the harm cause by malware from other machines being transmitted to the voting system.

7. Windows Server Update Services (WSUS) Offline Update is used to enable updates the computer – which is a package of files normally downloaded from the internet but compiled into a program to put on a USB drive to manually update server systems.

8. Failure to properly update the voting system demonstrates a significant and fatal error in security and election integrity.

9. There are 15 additional updates that should have been installed on the server to adhere to Microsoft Standards to fix known vulnerabilities. For the 4/10/2019 install, the most updated version of the update files would have been 03/13/2019 which is 11.6.1 which is 15 updates newer than 10.9.1

   This means the updates installed were 2 years, 1 month, 13 days behind the most current update at the time. This includes security updates and fixes. This demonstrated a significant and fatal error in security and election integrity.

   - Wed 04/10/2019 10:34:33.14 - Info: Starting WSUS Offline Update (v. 10.9.1)

   - Wed 04/10/2019 10:34:33.14 - Info: Used path "D:\WSUSOFFLINE1091_2012R2_W10\cmd\" on EMSSERVER (user: EMSADMIN)

   - Wed 04/10/2019 10:34:35.55 - Info: Medium build date: 03/10/2019

- Found on c:\Windows\wsusofflineupdate.txt

- *WSUS Offline Update (v.10.9.1) was created on 01/29/2017

*WSUS information found here https://download.wsusoffline.net/

10. Super User Administrator account is the primary account used to operate the **Dominion Election Management System** which is a major security risk. The user logged in has the ability to make major changes to the system and install software which means that there is no oversight to ensure appropriate management controls – i.e. anyone who has access to the shared administrator user names and passwords can make significant changes to the entire voting system. The shared usernames and passwords mean that these changes can be made in an anonymous fashion with no tracking or attribution.

J. ERROR RATES

1. We reviewed the Tabulation logs in their entirety for 11/6/2020. The election logs for Antrim County consist of 15,676 total lines or events.

   - Of the 15,676 there were a total of 10,667 critical errors/warnings or a 68.05% error rate.

   - Most of the errors were related to configuration errors that could result in overall tabulation errors or adjudication. These 11/6/2020 tabulation totals were used as the official results.

2. For examples, there were 1,222 ballots **reversed** out of 1,491 total ballots cast, thus resulting in an 81.96% rejection rate. Some of which were reversed due to "Ballot's size exceeds maximum expected ballot size".

   - According to the NCSL, Michigan requires testing by a federally accredited laboratory for voting systems. In section 4.1.1 of the Voluntary Voting Systems Guidelines (VVSG) Accuracy Requirements a. **All systems shall achieve a report total error rate of no more than one in 125,000**.

   - https://www.eac.gov/sites/default/files/eac_assets/1/28/VVSG.1.1.VOL.1.FINAL1.pdf

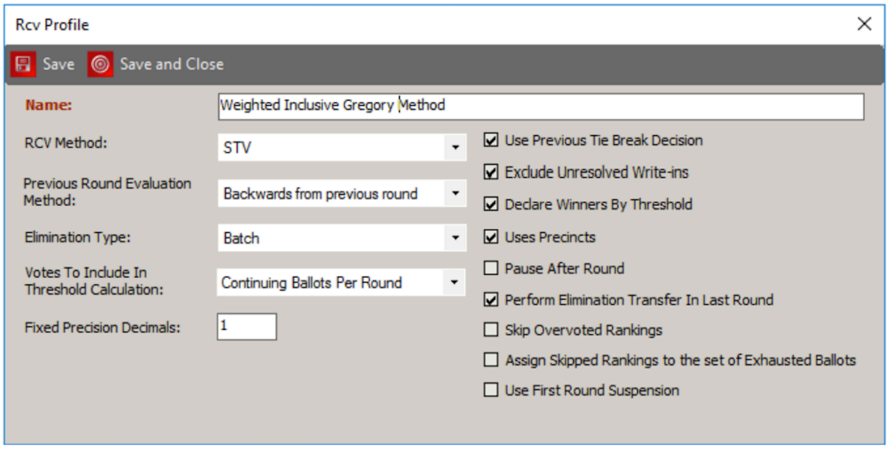
   - In section 4.1.3.2 Memory Stability of the VVSG it states that **Memory devices used to retain election management data shall have demonstrated error free data retention for a period of 22 months**.

   - In section 4.1.6.1 Paper-based System Processing Requirements sub-section a. of the VVSG it states "The ability of the system to produce and receive electronic signals from the scanning of the ballot, perform logical and numerical operations upon these data, and reproduce the contents of memory when required **shall** be sufficiently free of **error** to enable satisfaction of the system-level accuracy requirement indicated in Subsection 4.1.1."

- These are not human errors; this is definitively related to the software and software configurations resulting in error rates far beyond the thresholds listed in the guidelines.

3. A high "error rate" in the election software (in this case 68.05%) reflects an algorithm used that will weight one candidate greater than another (for instance, weight a specific candidate at a 2/3 to approximately 1/3 ratio). In the logs we identified that the RCV or Ranked Choice Voting Algorithm was enabled (see image below from the Dominion manual). This allows the user to apply a weighted numerical value to candidates and change the overall result. The declaration of winners can be done on a basis of points, not votes. [Image 8]:

> choice voting results are evaluated on a district per district basis and each district has a set number of points (100). Elimination and declaration of winners is done on basis of points, not votes.



Rcv Profile

Name: Weighted Inclusive Gregory Method

RCV Method: STV

Previous Round Evaluation Method: Backwards from previous round

Elimination Type: Batch

Votes To Include In Threshold Calculation: Continuing Ballots Per Round

Fixed Precision Decimals: 1

☑ Use Previous Tie Break Decision
☑ Exclude Unresolved Write-ins
☑ Declare Winners By Threshold
☑ Uses Precincts
☐ Pause After Round
☑ Perform Elimination Transfer In Last Round
☐ Skip Overvoted Rankings
☐ Assign Skipped Rankings to the set of Exhausted Ballots
☐ Use First Round Suspension

Figure 11-3: RCV Profile screen

4. The Dominion software configuration logs in the Divert Options, shows that all write-in ballots were flagged to be diverted automatically for adjudication. This means that all write-in ballots were sent for "adjudication" by a poll worker or election official to process the ballot based on voter "intent". Adjudication files allow a computer operator to decide to whom to award those votes (or to trash them).

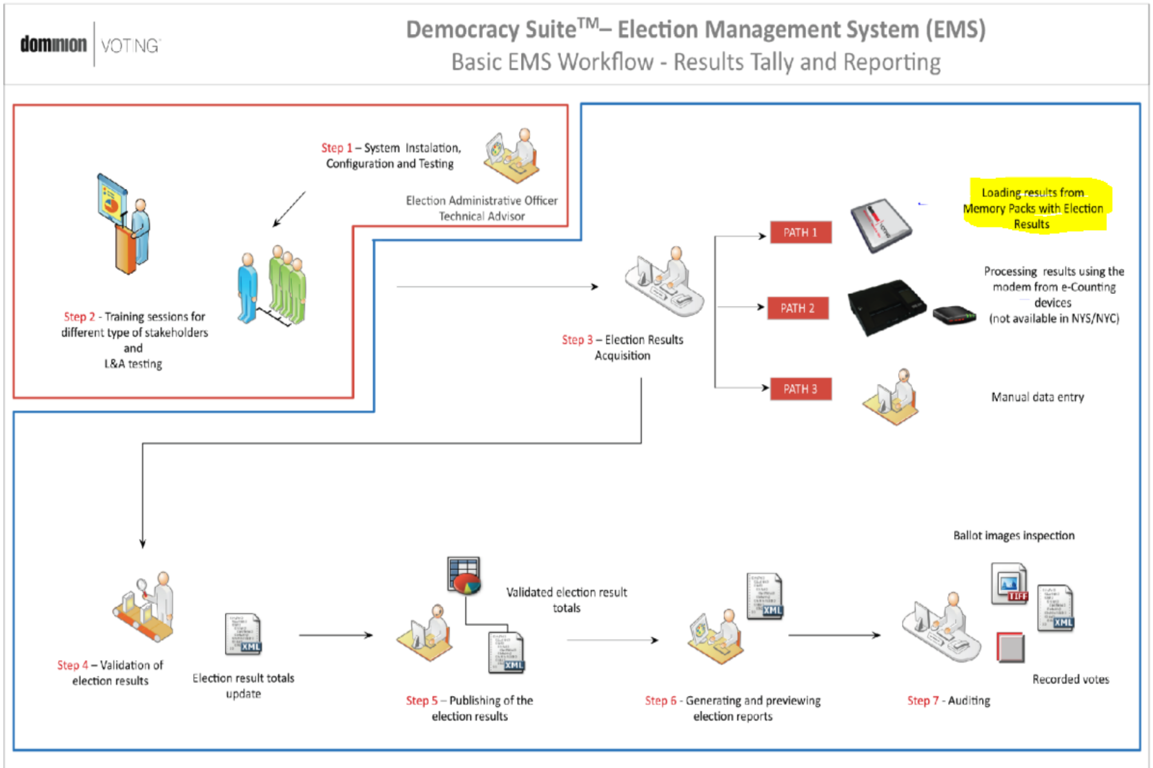
5. In the logs all but two of the Override Options were enabled on these machines, thus allowing any operator to change those votes. [Image 9]:

[redacted]

6. In the logs all but two of the Override Options were enabled on these machines, thus allowing any operator to change those votes. This gives the system operators carte blanche to adjudicate ballots, in this case 81.96% of the total cast ballots with no audit trail or oversight. [Image 10]:

[redacted]

7. On 12/8/2020 Microsoft issued 58 security patches across 10+ products, some of which were used for the election software machine, server and programs. Of the 58 security fixes 22, were patches to remote code execution (RCE) vulnerabilities. [Image 11]:


dominion VOTING
Democracy Suite™– Election Management System (EMS)
Basic EMS Workflow - Results Tally and Reporting
Step 1 – System Instalation, Configuration and Testing
Election Administrative Officer
Technical Advisor
Step 2 - Training sessions for different type of stakeholders and L&A testing
Step 3 – Election Results Acquisition
PATH 1
PATH 2
PATH 3
Loading results from Memory Packs with Election Results
Processing results using the modem from e-Counting devices (not available in NYS/NYC)
Manual data entry
Step 4 – Validation of election results
Election result totals update
XML
Validated election result totals
Step 5 – Publishing of the election results
Step 6 - Generating and previewing election reports
Ballot images inspection
TIFF
Recorded votes
Step 7 - Auditing

8. We reviewed the Election Management System logs (EmsLogger) in their entirety from 9/19/2020 through 11/21/2020 for the Project: Antrim November 2020. There were configuration errors throughout the set-up, election and tabulation of results. The last error for Central Lake Township, Precinct 1 occurred on 11/21/2020 at 14:35:11 System.Xml.XmlException System.Xml.XmlException: The ' ' character, hexadecimal value 0x20, cannot be included in a name. Bottom line is that this is a calibration that rejects the vote (see picture below). [Image 12]:

[redacted]

Notably 42 minutes earlier on Nov 21 2020 at 13:53:09 a user attempted to zero out election results. Id:3168 EmsLogger - There is no permission to {0} - Project: User: Thread: 189. This is direct proof of an attempt to tamper with evidence.

[redacted]

9. The Election Event Designer Log shows that Dominion ImageCast Precinct Cards were programmed with updated new programming on 10/23/2020 and again after the election on 11/05/2020. As previously mentioned, this violates the HAVA safe harbor period.

Source: C:\Program Files\Dominion Voting Systems\Election Event Designer\Log\Info.txt

- Dominion Imagecast Precinct Cards Programmed with 9/25/2020 programming on 09/29/2020, 09/30/2020, and 10/12/2020.

- Dominion Imagecast Precinct Cards Programmed with New Ballot Programming dated 10/22/2020 on 10/23/2020 and after the election on 11/05/2020

Excerpt from 2020-11-05 showing “ProgramMemoryCard” commands.

[redacted]

[redacted]

10. Analysis is ongoing and updated findings will be submitted as soon as possible. A summary of the information collected is provided below.

```
10|12/07/20 18:52:30| Indexing completed at Mon Dec 7 18:52:30 2020
12|12/07/20 18:52:30| INDEX SUMMARY
12|12/07/20 18:52:30| Files indexed: 159312
```

```
12|12/07/20 18:52:30| Files skipped: 64799
12|12/07/20 18:52:30| Files filtered: 0
12|12/07/20 18:52:30| Emails indexed: 0
12|12/07/20 18:52:30| Unique words found: 5325413
12|12/07/20 18:52:30| Variant words found: 3597634
12|12/07/20 18:52:30| Total words found: 239446085
12|12/07/20 18:52:30| Avg. unique words per page: 33.43
12|12/07/20 18:52:30| Avg. words per page: 1503
12|12/07/20 18:52:30| Peak physical memory used: 2949 MB
12|12/07/20 18:52:30| Peak virtual memory used: 8784 MB
12|12/07/20 18:52:30| Errors: 10149
12|12/07/20 18:52:30| Total bytes scanned/downloaded: 1919289906
```

Dated: December 13, 2020

Russell Ramsland