

STATE OF MICHIGAN  
IN THE SUPREME COURT

APPEAL FROM THE MICHIGAN COURT OF APPEALS

WILLIAM BAILEY

Plaintiff

v.

ANTRIM COUNTY

Defendant

SECRETARY OF STATE JOCELYN  
BENSON

Intervenor-Defendant,

Supreme Court No. \_\_\_\_\_

COA Case No: 357838

LC Case No. 20-9238-CZ

**APPLICATION FOR LEAVE TO APPEAL**

Matthew S. DePerno (P52622)  
DEPERNO LAW OFFICE, PLLC  
Attorney for Plaintiff-Appellant  
951 W. Milham Avenue  
PO Box 1595  
Portage, MI 49081  
(269) 321-5064  
[matthew@depernolaw.com](mailto:matthew@depernolaw.com)

Allan C. Vander Laan (P33893)  
Douglas J. Curlew (P39275)  
CUMMINGS, MCCLOREY, DAVIS & ACHO, PLC  
Attorneys for Defendant Appellee  
2851 Charlevoix Dr., Ste. 327  
Grand Rapids, MI 49546  
(231) 922-1888  
[avanderlaan@cnda-law.com](mailto:avanderlaan@cnda-law.com)  
[dcurlew@cnda-law.com](mailto:dcurlew@cnda-law.com)

Heather S. Meingast (P55439)  
Erik A. Grill (P64713)  
Assistant Attorneys General  
Attorneys for Appellee Intervenor Benson  
PO Box 30736  
Lansing, MI 48909  
(517) 335-7659  
[meingasth@michigan.gov](mailto:meingasth@michigan.gov)  
[grille@michigan.gov](mailto:grille@michigan.gov)

**APPENDIX OF PLAINTIFF-APPELLANT**

**VOLUME 2**

**TABLE OF CONTENTS**

**Volume 1**

Ex 1: Court of Appeals Opinion, per curiam, dated April 21, 2022.....1

Ex 2: Errata Order, dated May 25, 2021 .....14

Ex 3: Order Denying Plaintiff's Motion for Rehearing or Reconsideration Under MCR 2.119(F)(3), dated June 25, 2021 .....17

Ex 4: Transcript, May 10, 2021 (Defendants' Joint Motion for Summary Disposition).....20

Ex 5: Transcript, May 18, 2021 (Ruling on Defendants' Motion for Summary Disposition).....135

Ex 6: Response to Motion for Summary Disposition.....157

    Ex 1. Testimony of Sheryl Guy .....195

    Ex 2. Benson Press Release, Nov 23, 2020 .....208

    Ex 3. Benson Press Release, Dec 9, 2020.....210

    Ex 4. Benson Press Release, Dec 14, 2020.....213

    Ex 5. Benson Press Release, Dec 18, 2020.....217

    Ex 6, Benson Press Release, Mar 2, 2021.....220

    Ex 7. Allied Security Operations Group, Preliminary Antrim Michigan Forensics Report .....224

    Ex 8. Dismissals.....248

    Ex 9. Errata – Order Setting Aside Dismissal.....251

    Ex 10. James Penrose, *Preliminary Assessment of Wireliess Communications Technology for Michigan Voting Systems*, Apr 9, 2021.....254

**Volume 2**

Ex 11. Affidavit of Benjamin R. Cotton, Apr 8, 2021 .....263

Ex 12. Cyber Ninjas, *Antrim County, MI Election Management System Application Security Analysis*, Apr 9, 2021 .....270

Ex 13. James Penrose, May 2, 2021 .....289

Ex 14. Jeffrey Lenberg, May 3, 2021 .....315

Ex 15. NOTICE: All County Audit, Dec 15, 2020.....333

Ex 16. Email.....	336
Ex 17: Hand Count Calculation Sheet .....	337
<b><u>Volume 3</u></b>	
Ex 18. Post-Election Audit Manual .....	339
Ex 19. <i>Ryan et al v Benson, Michigan Court of Claims, Opinion and Order Regarding Plaintiff's Emergency Motion for Immediate Declaratory Judgment, Case No. 20-000198-MZ</i> .....	353
Ex 7: Plaintiff's Supplemental Brief.....	363
Ex 1. Jeffrey Lenberg, <i>Preliminary Report of Subversion in the Antrim County Election Management System, Results Tallying and Reporting Application, May 9, 2021</i> .....	368
Ex 8: Plaintiff's Motion for Reconsideration.....	386
Ex 1. Errata Order .....	432
Ex 2. Jeffrey Lenberg, <i>Case Study Banks Township – Antrim County Election Management Server Found to be Subverted, Jun 9, 2021</i> .....	435
Ex 3. Sample ballot.....	474
Ex 4. Jeffrey Lenberg, <i>Centralized Subversion of Election Vote Totals and Paper Tapes, Jun 9, 2021</i> .....	477
Ex 5. Jeffrey Lenberg, <i>Central Lake Township Reversals Make Ballots Impossible to Count, Helena Township 21% Ballot Reversal Rate, 20% Higher Reversal Rate for Republican voters and Mancelona Late Night Ballot Processing, Jun 9, 2021</i> .....	494
<b><u>Volume 4</u></b>	
Ex 6. Judy Koslowski affidavit.....	504
Ex 7. Affidavit of Benjamin R. Cotton, Jun 8, 2021 .....	507
Ex 8. Jeffrey Lenberg, <i>Missing Evidence for Evaluation of Antrim County Election, Official Ballots are Easily Fabricated, and Official Ballot PDFs Flawed Making for Errors in Processing, Jun 9, 2021</i> .....	516
Ex 9: Order Staying All Matters, dated Sep 3, 2021 .....	525
Ex 10: Election Results Chart #1.....	528

Ex 11: Election Results Chart #2.....529

Ex 12: *Genetski v Benson*, Michigan Court of Claims, *Opinion and Order Granting Summary Disposition in Part to Plaintiffs and Granting Summary Disposition in Part to Defendants*, Case No. 20-000216-MM.....530

Ex 13: Transcript, April 12, 2021 (Motions).....547

Ex 14: Notice of Hearing, Defendants' Joint Motion for Summary Disposition.....675

Ex 15: Plaintiff's Motion to Adjourn.....677

Ex 1. Transcript, April 12, 2021 .....684

Ex 2. Notice of Hearing .....705

Ex 3. Email.....707

Ex 16: Notice of Hearing, Plaintiff's Motion to Adjourn .....710

Ex 17: Transcript, May 25, 2021 (Motions).....712

Ex 18: Motion to Amend Complaint .....750

Ex A. Amended Verified Complaint .....756

Ex 19: Supplement to Motion to Amend Complaint.....825

Ex A. Amended Verified Complaint (Exhibits in court file).....834

Ex 20: Second Supplement to Motion to Amend Complaint.....916

Ex 1. Jeff Lenberg, May 18, 2021 .....919

Ex 21: Notice of Hearing, Plaintiff's Motion to Amend Complaint.....923

Ex 22: Transcript, April 23, 2021 (Motions) .....925

Ex 23: Transcript, April 26, 2021 (Motions) .....943

Respectfully submitted

DePERNO LAW OFFICE, PLLC

Dated: June 2, 2022

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



# Exhibit 11

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 10<sup>th</sup> 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.



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.

  
Benjamin R. Cotton

# Exhibit 12



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](http://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

1	Revision History.....	1
3	Executive Summary.....	2
4	Scope.....	3
5	Background .....	3
5.1	Architecture .....	3
5.2	Definitions.....	5
6	Findings .....	5
6.1	Authentication & Authorization.....	5
6.2	Audit Logging & Tracking .....	6
6.3	Cryptography & Secret Storage .....	7
6.4	Credential Management .....	14
6.5	Certification.....	15
7	Affirmation.....	16
8	About Cyber Ninjas .....	16
	Appendix A: Bio – Douglas Logan.....	17

### 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 6<sup>th</sup>, 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 3<sup>rd</sup>, 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.

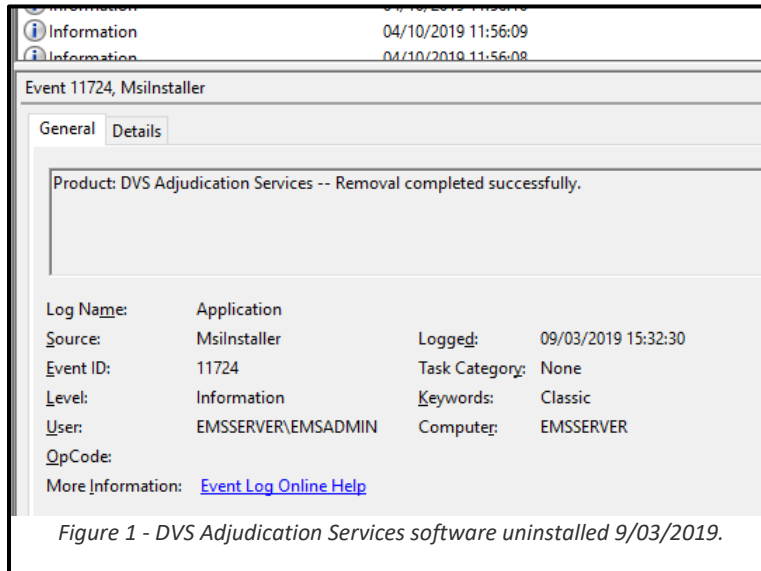


Figure 1 - DVS Adjudication Services software uninstalled 9/03/2019.

### 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	82 [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](https://www.eac.gov/sites/default/files/voting_system/files/Deficiency%20Report.pdf)

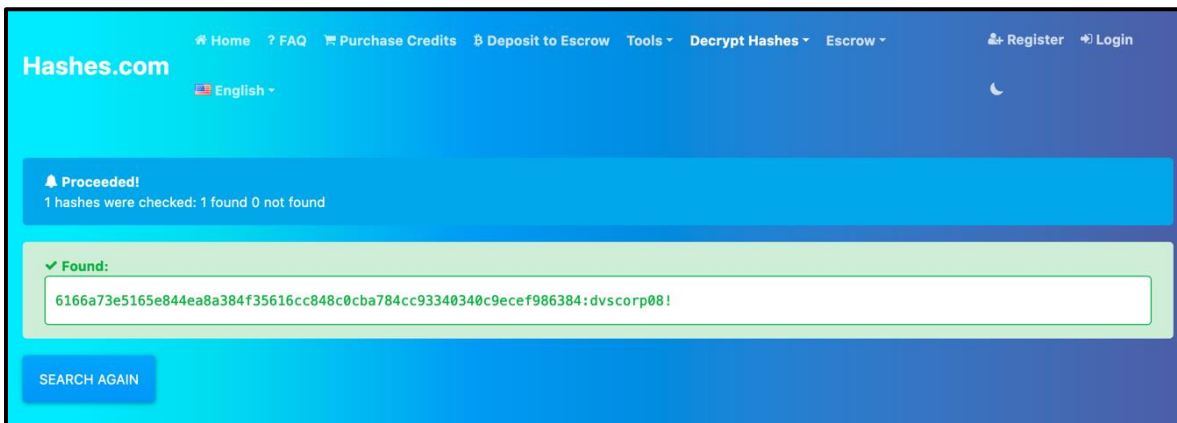
NOTE: These were detected by utilizing grep to search the binaries for the string "password".

File Name(s)	Value
/Election Data Translator/DVS.DemocracySuite.DatabaseService.dll	
/Election Event Designer/DVS.DemocracySuite.DatabaseService.dll	username="Techadvisor" password="YWanPIFI6ETqijhPNWFSyEjAy6eEzJM0A0DJ7O+YY4Q="
/Election Event Designer/DVS.DemocracySuite.DatabaseService.dll	
/Election Data Translator/DVS.DemocracySuite.DatabaseService.dll	
/Election Event Designer/DVS.DemocracySuite.DatabaseService.dll	username="MRO01" password="YWanPIFI6ETqijhPNWFSyEjAy6eEzJM0A0DJ7O+YY4Q="
/Election Event Designer/DVS.DemocracySuite.DatabaseService.dll	
/Election Data Translator/DVS.DemocracySuite.DatabaseService.dll	
/Election Event Designer/DVS.DemocracySuite.DatabaseService.dll	username="ROAdmin" password="YWanPIFI6ETqijhPNWFSyEjAy6eEzJM0A0DJ7O+YY4Q="
/Election Event Designer/DVS.DemocracySuite.DatabaseService.dll	
/Election Data Translator/DVS.DemocracySuite.DatabaseService.dll	
/Election Event Designer/DVS.DemocracySuite.DatabaseService.dll	username="Admin" password="YWanPIFI6ETqijhPNWFSyEjAy6eEzJM0A0DJ7O+YY4Q="
/Election Event Designer/DVS.DemocracySuite.DatabaseService.dll	

/Election Data Translator/DVS.DemocracySuite.DatabaseService.dll  /Election Event Designer/DVS.DemocracySuite.DatabaseService.dll  /Election Event Designer/DVS.DemocracySuite.DatabaseService.dll	username="SAdmin" password="YWanPIFI6ETqijhPNWFsyEjAy6eEzJM0A0DJ7O+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!”.



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

```

1 <?xml version="1.0" encoding="utf-8"?>
2 <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">
3   <extensions>
4     <!--<add assembly="CustomLayout"/>-->
5   </extensions>
6   <targets>
7     <target name="dbMssqlAsync" xsi:type="AsyncWrapper" overflowAction="Grow">
8       <target name="dbTargetMssql" type="Database">
9         <dbprovider>mssql</dbprovider>
10        <connectionString>Data Source=HELIOS\RV;Initial Catalog=EDMTrunk_Template;User Id=emsdbadmin;
  Password=dvscorp08!;MultipleActiveResultSets=True;Connect Timeout=10</ConnectionString>
11      <commandText>
12        INSERT INTO permission.[DeveloperLog] ([Date],[ThreadID],[LogLevel],[Logger],[Username]
  ,[Project],[StackValues],[Message],[ExceptionMessage]) VALUES (@date,@threadID,@logLevel,
  @logger,@username,@project,@stackvalues,@message,@exceptionMessage);
13      </commandText>
14      <parameter name="@date" layout="{date}" />
15      <parameter name="threadID" layout="{threadid}" />
16      <parameter name="@logLevel" layout="{level}" />
17      <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}"
  ConnectionStringStandAlone="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 hardcoded 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](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](https://www.eac.gov/sites/default/files/voting_system/files/Dominion_Voting_Systems_D-Suite_5.5-B_Test_Plan-Rev_02.pdf)

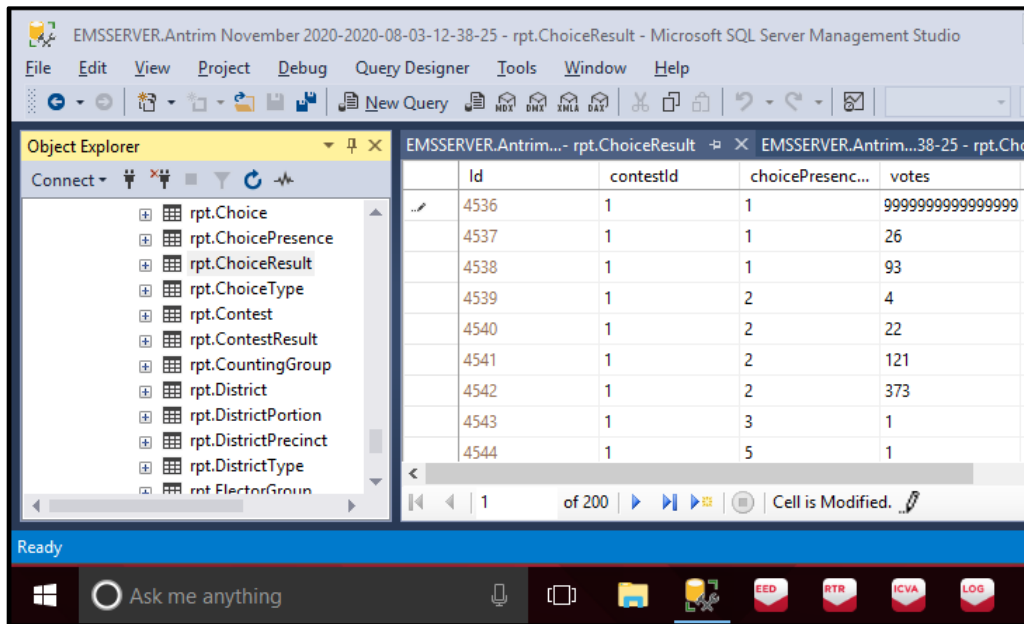


Figure 3 - SQL Management Tools allows the easy editing of a vote.



## 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 9<sup>th</sup> 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 responsibilities, he helped launch the Bloomington, Indiana office. Under Mr. Logan's technical leadership, Cigital was able to scale their Vulnerability Assessment 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-propagating 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 13

**Analyst: James Thomas Penrose, IV**

**Date: 2 May 2021**

### Executive Summary

ElectionSource technicians responsible for the creation and deployment of project files have supreme power in creating configurations that can be used to modify the votes in the EMS and the output of the tabulator paper tapes. Upon review of the Lenberg report dated May 2<sup>nd</sup>, 2021, ElectionSource technicians create project files for their clients and as a result can access, control, and modify any election they support.

ElectionSource configured and deployed Antrim County's project files that resulted in the modification of the votes during the general election. The Lenberg report indicates that vote modification in Antrim County was consistent with technical manipulation of the project file. This project file was generated and deployed by ElectionSource for the November 3<sup>rd</sup>, 2020 general election.

In order to research and investigate the Antrim County vote modification it is necessary to perform a full forensic examination and testing of all equipment utilized during the election. Michigan clerks take an oath to faithfully discharge the duties of a clerk including to hold fair and accurate elections. ElectionSource has issued a threat to Michigan clerks interested in conducting independent forensic examinations and testing of election equipment. See Exhibit A.

ElectionSource has the responsibility to review the log files on the Dominion Voting Systems, Election Management System (EMS), the log files are typically viewed by trained technicians with the appropriate experience to properly interpret the software prompts/warnings. During the preparation for the general election their were prompts/warnings ignored by ElectionSource.

ElectionSource failed to utilize version control. Version control is defined as the task of keeping a software system consisting of many versions and configurations well organized. Failure to utilize version control can lead to incorrect vote tally during an election. The lack of policy, procedures, and technical implementation on the part of ElectionSource led to a situation where an inaccurate tally could occur.

An ElectionSource whistleblower has also publicly spoke out about his concerns of fraud over technicians having access to a broad array of ballots from across the State of Michigan via ElectionSource thumb drives. The evidence of what occurred in Antrim County along with the statements of an ElectionSource whistleblower illustrate the multiple avenues for fraud.

### Details



## ElectionSource Threats Related to Forensics Analysis

ElectionSource sent a letter dated January 4<sup>th</sup>, 2021 stating that any independent forensic analysis of election equipment would require the Michigan Secretary of State's approval. This letter included a threat of legal action against any Michigan clerk that sought independent investigation related to their equipment in order to uphold their oath of office pertaining to elections.

### Weak and Hardcoded Passcodes

ElectionSource performed a number of functions on behalf of Antrim County in order to prepare for and conduct the November 3, 2020 general election. When examining the historic steps taken by the ElectionSource configuring the Antrim County EMS one of the actions taken was to set the default technician passcode for the entirety of Antrim County to a weak passcode. The weak passcode was "123456" set by ElectionSource as found in the configuration files used for the election. Moreover, the UserLog file on the EMS also indicated that the election password to open and close the polls was set to "1234678" for more than 19 months prior to the election at which time it was updated to a similarly weak and guessable passcode "11032020", the date of the general election. These passcodes work to give access to the tabulators to open/close, reopen, and rezero the tabulators.

A malicious actor seeking to commit fraud would need to know these passcodes to gain access to the tabulators and enable their operations. ElectionSource provisioned passcodes that were easily guessable and simple trial and error would reveal the correct passcodes with a tractable number of attempts, even done manually by hand by an attacker.

Table 1 below shows all the instances of the ElectionSource technicians making changes to the EMS and setting the default password for opening and closing the polls across the entirety of Antrim County precincts.

*Table 1 - UserInfo Log - Default Password Set Log Lines – Empty Columns Hidden*

Id	userRelatedInfo	executedCommand	__classid	operationTimestamp	logLevel
25BFF74B-6529-4D24-8875-016DE7DC8448	Admin	Instance with name 'Project Settings' of type 'Project Parameters' modified: defaultPasswordValue changed from '50831972' to '12345678'; tabulatorSameHMACKey=True; cardPartitionSize changed from 'Size 256' to 'Size 512';	LD01	2019-01-08 09:43:13.707	TraceMessage
FDD149A7-99A6-4F43-	Admin	Instance with name 'Project Settings' of type 'Project Parameters' modified:	LD01	2019-01-08 09:43:13.707	TraceMessage

8176-64A7DC45517A		defaultPasswordValue changed from '50831972' to '12345678'; tabulatorSameHMACKey=True; cardPartitionSize changed from 'Size 256' to 'Size 512'; createSplitsManually=True; serviceUrl = "; leadCardConsolidationLevel changed from 'Ballot Type' to 'Precinct Portion';			
654BC2E6-1F0C-4272-9260-CE67D466568B	Admin	Instance with name 'Project Settings' of type 'Project Parameters' modified: defaultPasswordValue changed from '50831972' to '12345678'; tabulatorSameHMACKey=True; cardPartitionSize changed from 'Size 256' to 'Size 512'; createSplitsManually=True; serviceUrl = ";	LD01	2019-01-08 09:43:13.707	TraceMessage
3B15E033-B474-4BEC-B614-E239660B18EF	Admin	Instance with name 'Project Settings' of type 'Project Parameters' modified: defaultPasswordValue changed from '12345678' to '11032020';	LD01	2020-08-03 12:41:51.990	TraceMessage

On January 8, 2019 the default passcode to open/close the polls was set by ElectionSource to be "12345678". This default passcode remained the same until August 3, 2020 when it was changed to "11032020" which was the passcode used during the Antrim County general election in November of 2020.

ElectionSource also hardcoded into the election project files for Antrim County the passcode of "123456" as the "technician passcode." The technician passcode allows for the polls to be re-opened and the tabulators to be re-zeroed. This weak passcode was set by ElectionSource.



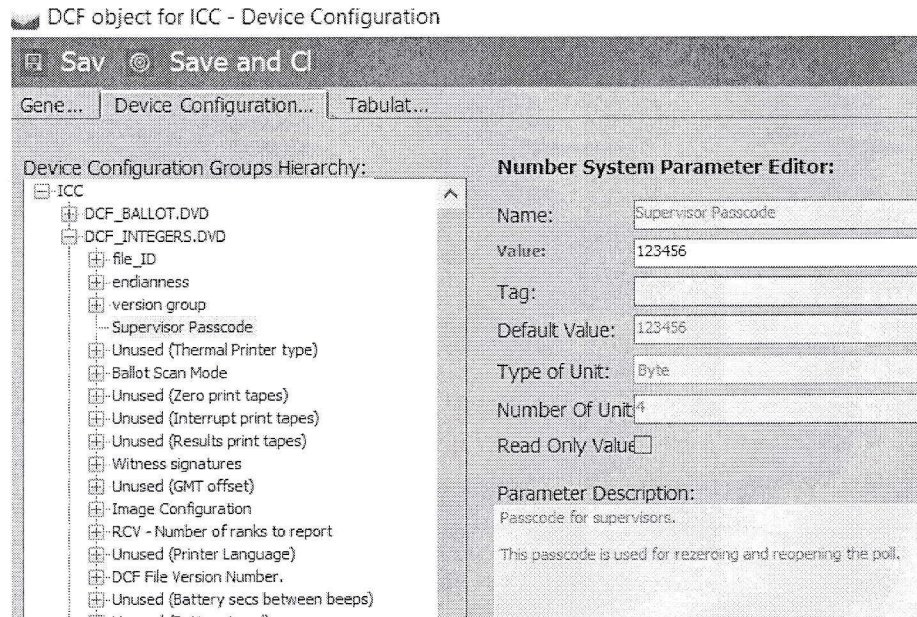


Figure 1 - Default Passcode

## Version Control, Configuration Management, and Development Practices

See Figures 3 and 4, ElectionSource set the “DCF File Version Number” associated with the Antrim County election to the same value, “50401,” regardless of the updates that were being deployed to the Antrim County Election Project Files and ballot definitions. There was no distinction made between the ICX, ICP, and ICC configurations that were deployed. This lack of version control resulted in ElectionSource’s failure to track that incompatible election configurations and ballot definitions were being deployed in Antrim County on election day.

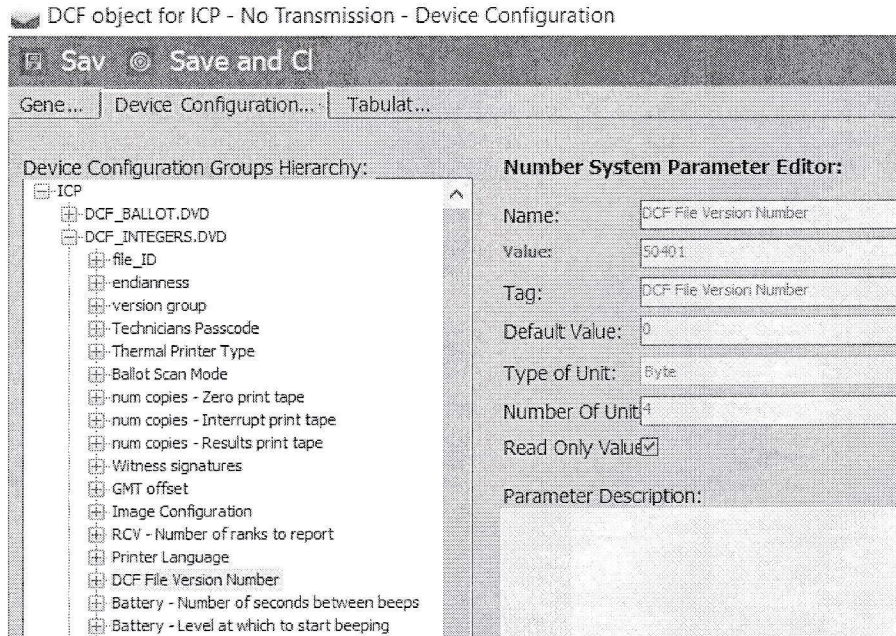


Figure 2 – September 29, 2020 - ICP Version Control Value 50401 (Same for all Tabulators Types)

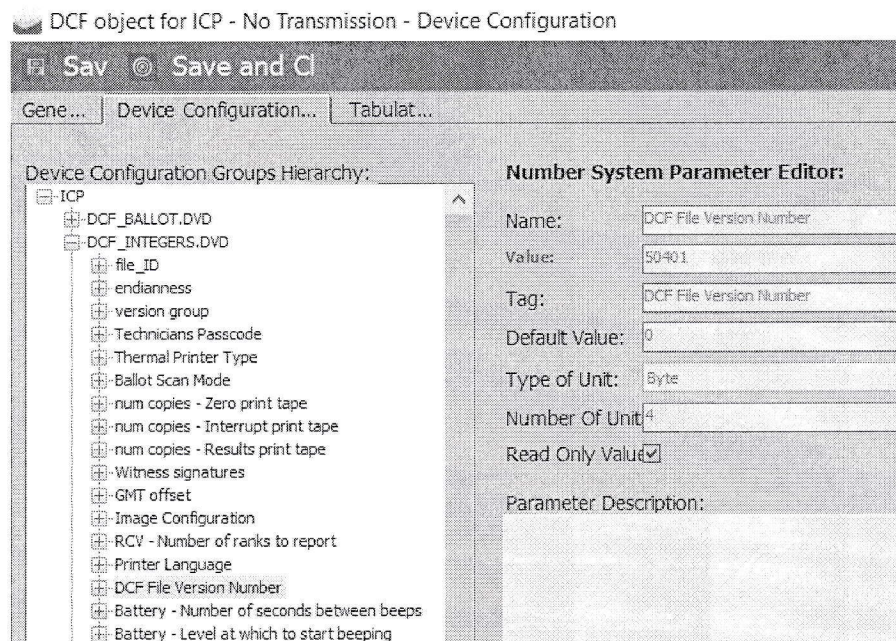


Figure 3 – October 23, 2020 - ICP Version Control Value 50401 (Same as ICP)

Figure 2 shows the original election/ballot configuration provisioned by ElectionSource on September 29<sup>th</sup>, 2020 for use in Antrim County for their ICPs. Figure 3 shows the final, corrected revision from October 23, 2020, of the election/ballot configuration for use in Antrim County ICPs. There is no evidence of a versioning process either technical or manual applied by ElectionSource to ensure that the proper version of the configuration would be deployed throughout the



entirety of Antrim County. ElectionSource's failure to employ version control led to vote manipulation during the November 3<sup>rd</sup>, 2020 election.

### **Error Handling and Remediation**

ElectionSource made substantive modifications to the election and ballot definitions that triggered the EMS to provide a number of "prompt" notifications that were acknowledged by the ElectionSource technician performing the updates. The technician failed or elected not to take action on the notification messages and request a wholesale redeployment of all compact flash cards for all precincts that would be required to proceed with a fully updated election package. Table 2 below shows the notification messages that were generated from the EMS when the technician updated the configuration. The specific message directed to the technician states, "All previously created and deployed election files will be unusable." The technician is then presented with an option to click OK or Cancel based on whether or not they wish to proceed. The last record of this prompt in the log was on October 5, 2020 when the technician selected, "OK" acknowledging that new election files, provisioned on compact flash cards, would need to be deployed as the previously deployed versions will be unusable. ElectionSource failed to address the aforementioned prompts resulting in a modified vote tally.

Id	userRelatedInfo	executedCommand	_classid	operationTimestamp	logLevel
<p>69196343-CC58-41C8-B770-6D25DEA61482</p>	<p>Admin</p>	<p>Prompt information: 'Election Files will be created based on the following parameters. Press Continue to continue the process.</p> <p>All previously created and deployed election files will be unusable.</p> <p>General project information:            Number of Districts: 61            Number of Precincts (including split Precincts): 62            Number of Choices: 364            Number of Contests: 141            Number of Offices: 48            Number of Political Parties: 8            Number of Counting Groups: 2</p> <p>Number of Tabulators: 42            Number of Polling Places: 22</p> <p>Ballot generation options:            Lead Card Consolidation Level: Precinct Portion            Consolidate Tail Cards: False            Force District Splits: False            Separate Voting Box Per Party Affiliation: False            Ballot Content Creator: Default Ballot Content Creator</p> <p>; User answered with: 'OK'</p>	<p>LD01</p>	<p>2020-09-23 13:20:55.740</p>	<p>UserAction</p>
<p>7E017D17-224D-41FF-940D-060AF3740015</p>	<p>Admin</p>	<p>Prompt information: 'Election Files will be created based on the following parameters. Press Continue to continue the process.</p> <p>All previously created and deployed election files will be unusable.</p> <p>General project information:            Number of Districts: 61            Number of Precincts (including split Precincts): 62            Number of Choices: 364            Number of Contests: 141            Number of Offices: 48            Number of Political Parties: 8            Number of Counting Groups: 2</p> <p>Number of Tabulators: 42            Number of Polling Places: 22</p>	<p>LD01</p>	<p>2020-10-05 14:10:09.850</p>	<p>UserAction</p>



	Ballot generation options: Lead Card Consolidation Level: Precinct Portion Consolidate Tail Cards: False Force District Splits: False Separate Voting Box Per Party Affiliation: False Ballot Content Creator: Default Ballot Content Creator  ; User answered with: 'OK'			
--	--	--	--	--

Table 2 – UserInfo Log File – Empty Columns Hidden  
 See complete table in Exhibit B

The final update to the election files prior to the general election was performed by ElectionSource on October 22<sup>nd</sup>, however, to truly complete the deployment of all the new election files to all precincts, completely new compact flash cards would need to be provisioned containing the new election files. From October 24<sup>th</sup> to November 2<sup>nd</sup> there were no entries in the UserInfo log file, indicating that there were no attempts made by either ElectionSource to complete this compact flash card update process during the crucial weeks ahead of the general election.

The Lenberg report indicates that manipulation of the project files can circumvent the canvassing process. ElectionSource technicians responsible for the creation and deployment of project files have supreme power in creating configurations that can be used to modify the votes in the EMS and the output of the tabulator paper tapes. ElectionSource technicians create project files for their clients and as a result can access, control, and modify any election they support.

ElectionSource configured and deployed Antrim County’s project files that resulted in the modification of the votes during the general election. The Lenberg report indicates that vote modification in Antrim County was consistent with technical manipulation of the project file.

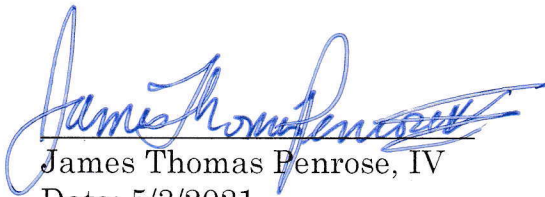
**ElectionSource Whistleblower Video**

A self-proclaimed ElectionSource employee made a video that was released shortly after the general election in 2020 stating that he believed the biggest risk to elections came from the use of thumb drives to transfer the ballot designs for all the

various localities around the State of Michigan supported by ElectionSource. The whistleblower said that it is very easy for an attacker to get a copy of any ballot from the thumb drive and make copies of the ballot of the correct paper stock and then proceed to stuff the ballot box with their own home made ballots based on the ballot designs that ElectionSource has their technicians keep on their thumb drives as part of their routine procedures for handling such sensitive election data.

The full video transcript is attached Exhibit C.

Under the penalties of perjury, I declare that I have read the foregoing report and that the fact stated in it are true.

A handwritten signature in blue ink, appearing to read "James Thomas Penrose, IV". The signature is stylized and cursive.

James Thomas Penrose, IV  
Date: 5/3/2021

**MICHIGAN NOTARY ACKNOWLEDGEMENT**

State of Michigan  
County of Michigan

The foregoing instrument was acknowledged before me on this 3<sup>rd</sup> day of May, 2021 by James T. Penrose, IV.

Notary Public Signature: *A.M. Howard*

Notary Printed Name: Ann M. Howard

Acting in the County of: Oakland

My Commission Expires: 2/24/2023

**ANN M. HOWARD**  
Notary Public, State of Michigan  
County of Oakland  
My Commission Expires 02-24-2023  
Acting In the County of *Oakland*

RECEIVED by MSC 6/2/2022 1:49:42 AM

Exhibit A – Election Source Equipment License Agreements



January 4, 2021

RE: Equipment License Agreements

Dear Clerks,

This letter is in response to an inquiry regarding a potential “forensic audit” of the Dominion system currently licensed to you. Any transfer of equipment or software to a third party would be in direct violation of the State of Michigan software license terms and conditions, which govern the use of the voting system and software in your jurisdiction. More specifically, the license terms state, “Licensor grants licensee a non-exclusive, **non-transferrable** license to use the Software” (emphasis added). Further, the license terms state that the licensee may NOT “Transfer or copy onto any other storage device or hardware or otherwise copy the Software in whole or in part except for purposes of system backup.”

Any transfer of any component of the voting system to a third party would be a violation of the agreement and Election Source, the State or Dominion may take immediate legal action for such breach of contract.

**Both Election Source and Dominion are open to a review of the voting system by an EAC accredited testing laboratory, as previously done during the EAC and State of Michigan certification processes. Any such review must be coordinated with the Michigan Secretary of State.**

ElectionSource – 4615 Danvers DR SE – Grand Rapids, MI 49512 – P 888-742-8037 – F 616-464-0926 – www.electionsource.com

---



**Exhibit B – UserInfo Log**

**Containing Prompt Messages Regarding Previous Election Files Being Unusable**

Id	userRelatedInfo	executedCommand	_classid	operationTimestamp	logLevel
7E222529-6072-437A-BB80-E150D64D83C4	Admin	<p>Prompt information: 'Election Files will be created based on the following parameters. Press Continue to continue the process.'</p> <p>All previously created and deployed election files will be unusable.</p> <p>General project information:            Number of Districts: 61            Number of Precincts (including split Precincts): 62            Number of Choices: 364            Number of Contests: 141            Number of Offices: 48            Number of Political Parties: 8            Number of Counting Groups: 2</p> <p>Number of Tabulators: 42            Number of Polling Places: 22</p> <p>Ballot generation options:            Lead Card Consolidation Level: Precinct Portion            Consolidate Tail Cards: False            Force District Splits: False            Separate Voting Box Per Party Affiliation: False            Ballot Content Creator: Default Ballot Content Creator</p> <p>; User answered with: 'OK'</p>	LD01	2020-09-18 13:00:04.820	UserAction
EC28AE11-9D75-4F01-972C-833160F8984C	Admin	<p>Prompt information: 'Election Files will be created based on the following parameters. Press Continue to continue the process.'</p> <p>All previously created and deployed election files will be unusable.</p> <p>General project information:            Number of Districts: 61            Number of Precincts (including split Precincts): 62            Number of Choices: 364            Number of Contests: 141            Number of Offices: 48            Number of Political Parties: 8            Number of Counting Groups: 2</p> <p>Number of Tabulators: 42            Number of Polling Places: 22</p> <p>Ballot generation options:            Lead Card Consolidation Level: Precinct Portion            Consolidate Tail Cards: False            Force District Splits: False            Separate Voting Box Per Party Affiliation: False</p>	LD01	2020-09-18 13:12:31.543	UserAction

		<p>Ballot Content Creator: Default Ballot Content Creator</p> <p>; User answered with: 'OK'</p>			
<p>FF93A344-C5EA-4A1E-8ABB-A1C6350DA80C</p>	<p>Admin</p>	<p>Prompt information: 'Election Files will be created based on the following parameters. Press Continue to continue the process.</p> <p>All previously created and deployed election files will be unusable.</p> <p>General project information:            Number of Districts: 61            Number of Precincts (including split Precincts): 62            Number of Choices: 364            Number of Contests: 141            Number of Offices: 48            Number of Political Parties: 8            Number of Counting Groups: 2</p> <p>Number of Tabulators: 42            Number of Polling Places: 22</p> <p>Ballot generation options:            Lead Card Consolidation Level: Precinct Portion            Consolidate Tail Cards: False            Force District Splits: False            Separate Voting Box Per Party Affiliation: False            Ballot Content Creator: Default Ballot Content Creator</p> <p>; User answered with: 'OK'</p>	<p>LD01</p>	<p>2020-09-18 14:08:43.700</p>	<p>UserAction</p>



<p>918CF1BD-F2DF-4C48-A537-FAFCAE2F40CE</p>	<p>Admin</p>	<p>Prompt information: 'Election Files will be created based on the following parameters. Press Continue to continue the process.</p> <p>All previously created and deployed election files will be unusable.</p> <p>General project information:            Number of Districts: 61            Number of Precincts (including split Precincts): 62            Number of Choices: 364            Number of Contests: 141            Number of Offices: 48            Number of Political Parties: 8            Number of Counting Groups: 2</p> <p>Number of Tabulators: 42            Number of Polling Places: 22</p> <p>Ballot generation options:            Lead Card Consolidation Level: Precinct Portion            Consolidate Tail Cards: False            Force District Splits: False            Separate Voting Box Per Party Affiliation: False            Ballot Content Creator: Default Ballot Content Creator</p> <p>; User answered with: 'OK'</p>	<p>LD01</p>	<p>2020-09-23 10:30:08.620</p>	<p>UserAction</p>
<p>CD6C888C-B9F6-4B61-BAF4-11E95274538E</p>	<p>Admin</p>	<p>Prompt information: 'Election Files will be created based on the following parameters. Press Continue to continue the process.</p> <p>All previously created and deployed election files will be unusable.</p> <p>General project information:            Number of Districts: 61            Number of Precincts (including split Precincts): 62            Number of Choices: 364            Number of Contests: 141            Number of Offices: 48            Number of Political Parties: 8            Number of Counting Groups: 2</p> <p>Number of Tabulators: 42            Number of Polling Places: 22</p> <p>Ballot generation options:            Lead Card Consolidation Level: Precinct Portion            Consolidate Tail Cards: False            Force District Splits: False            Separate Voting Box Per Party Affiliation: False            Ballot Content Creator: Default Ballot Content Creator</p> <p>; User answered with: 'OK'</p>	<p>LD01</p>	<p>2020-09-21 08:48:54.560</p>	<p>UserAction</p>

<p>90CCE52F-E6B3-4EF3-A480-30B13E11C1FB</p>	<p>Admin</p>	<p>Prompt information: 'Election Files will be created based on the following parameters. Press Continue to continue the process.</p> <p>All previously created and deployed election files will be unusable.</p> <p>General project information:            Number of Districts: 61            Number of Precincts (including split Precincts): 62            Number of Choices: 364            Number of Contests: 141            Number of Offices: 48            Number of Political Parties: 8            Number of Counting Groups: 2</p> <p>Number of Tabulators: 42            Number of Polling Places: 22</p> <p>Ballot generation options:            Lead Card Consolidation Level: Precinct Portion            Consolidate Tail Cards: False            Force District Splits: False            Separate Voting Box Per Party Affiliation: False            Ballot Content Creator: Default Ballot Content Creator</p> <p>; User answered with: 'Cancel'</p>	<p>LD01</p>	<p>2020-09-21 09:11:57.397</p>	<p>UserAction</p>
<p>D7443ADD-BCC8-45E6-B0EF-278813BEF952</p>	<p>Admin</p>	<p>Prompt information: 'Election Files will be created based on the following parameters. Press Continue to continue the process.</p> <p>All previously created and deployed election files will be unusable.</p> <p>General project information:            Number of Districts: 61            Number of Precincts (including split Precincts): 62            Number of Choices: 364            Number of Contests: 141            Number of Offices: 48            Number of Political Parties: 8            Number of Counting Groups: 2</p> <p>Number of Tabulators: 42            Number of Polling Places: 22</p> <p>Ballot generation options:            Lead Card Consolidation Level: Precinct Portion            Consolidate Tail Cards: False            Force District Splits: False            Separate Voting Box Per Party Affiliation: False            Ballot Content Creator: Default Ballot Content Creator</p> <p>; User answered with: 'OK'</p>	<p>LD01</p>	<p>2020-09-21 09:12:12.750</p>	<p>UserAction</p>



<p>2B43456A-C566-49AA-B7ED-53DEEF43D2B4</p>	<p>Admin</p>	<p>Prompt information: 'Election Files will be created based on the following parameters. Press Continue to continue the process.'</p> <p>All previously created and deployed election files will be unusable.</p> <p>General project information:            Number of Districts: 61            Number of Precincts (including split Precincts): 62            Number of Choices: 364            Number of Contests: 141            Number of Offices: 48            Number of Political Parties: 8            Number of Counting Groups: 2</p> <p>Number of Tabulators: 42            Number of Polling Places: 22</p> <p>Ballot generation options:            Lead Card Consolidation Level: Precinct Portion            Consolidate Tail Cards: False            Force District Splits: False            Separate Voting Box Per Party Affiliation: False            Ballot Content Creator: Default Ballot Content Creator</p> <p>; User answered with: 'OK'</p>	<p>LD01</p>	<p>2020-09-21 09:27:30.520</p>	<p>UserAction</p>
<p>918CF1BD-F2DF-4C48-A537-FAFCAE2F40CE</p>	<p>Admin</p>	<p>Prompt information: 'Election Files will be created based on the following parameters. Press Continue to continue the process.'</p> <p>All previously created and deployed election files will be unusable.</p> <p>General project information:            Number of Districts: 61            Number of Precincts (including split Precincts): 62            Number of Choices: 364            Number of Contests: 141            Number of Offices: 48            Number of Political Parties: 8            Number of Counting Groups: 2</p> <p>Number of Tabulators: 42            Number of Polling Places: 22</p> <p>Ballot generation options:            Lead Card Consolidation Level: Precinct Portion            Consolidate Tail Cards: False            Force District Splits: False            Separate Voting Box Per Party Affiliation: False            Ballot Content Creator: Default Ballot Content Creator</p> <p>; User answered with: 'OK'</p>	<p>LD01</p>	<p>2020-09-23 10:30:08.620</p>	<p>UserAction</p>

<p>A6069645-C72A-42AE-B6D1-9E586E8AB38B</p>	<p>Admin</p>	<p>Prompt information: 'Election Files will be created based on the following parameters. Press Continue to continue the process.</p> <p>All previously created and deployed election files will be unusable.</p> <p>General project information:            Number of Districts: 61            Number of Precincts (including split Precincts): 62            Number of Choices: 364            Number of Contests: 141            Number of Offices: 48            Number of Political Parties: 8            Number of Counting Groups: 2</p> <p>Number of Tabulators: 42            Number of Polling Places: 22</p> <p>Ballot generation options:            Lead Card Consolidation Level: Precinct Portion            Consolidate Tail Cards: False            Force District Splits: False            Separate Voting Box Per Party Affiliation: False            Ballot Content Creator: Default Ballot Content Creator</p> <p>; User answered with: 'OK'</p>	<p>LD01</p>	<p>2020-09-23 13:16:00.213</p>	<p>UserAction</p>
<p>69196343-CC58-41C8-B770-6D25DEA61482</p>	<p>Admin</p>	<p>Prompt information: 'Election Files will be created based on the following parameters. Press Continue to continue the process.</p> <p>All previously created and deployed election files will be unusable.</p> <p>General project information:            Number of Districts: 61            Number of Precincts (including split Precincts): 62            Number of Choices: 364            Number of Contests: 141            Number of Offices: 48            Number of Political Parties: 8            Number of Counting Groups: 2</p> <p>Number of Tabulators: 42            Number of Polling Places: 22</p> <p>Ballot generation options:            Lead Card Consolidation Level: Precinct Portion            Consolidate Tail Cards: False            Force District Splits: False            Separate Voting Box Per Party Affiliation: False            Ballot Content Creator: Default Ballot Content Creator</p> <p>; User answered with: 'OK'</p>	<p>LD01</p>	<p>2020-09-23 13:20:55.740</p>	<p>UserAction</p>



<p>7E017D17-224D-41FF-940D-060AF3740015</p>	<p>Admin</p>	<p>Prompt information: 'Election Files will be created based on the following parameters. Press Continue to continue the process.</p> <p>All previously created and deployed election files will be unusable.</p> <p>General project information:          Number of Districts: 61          Number of Precincts (including split Precincts): 62          Number of Choices: 364          Number of Contests: 141          Number of Offices: 48          Number of Political Parties: 8          Number of Counting Groups: 2</p> <p>Number of Tabulators: 42          Number of Polling Places: 22</p> <p>Ballot generation options:          Lead Card Consolidation Level: Precinct Portion          Consolidate Tail Cards: False          Force District Splits: False          Separate Voting Box Per Party Affiliation: False          Ballot Content Creator: Default Ballot Content Creator</p> <p>; User answered with: 'OK'</p>	<p>LD01</p>	<p>2020-10-05 14:10:09.850</p>	<p>UserAction</p>
---	--------------	---	-------------	--------------------------------	-------------------

### Exhibit C – ElectionSource Whistleblower

Well, I'm probably gonna get fired over this, but it's something that's been weighing on my mind and something that I feel needs to be said, so I'm going to say it and. I'm just asking that people be respectful of my family. I just had a new baby and I'm just trying to be as open and honest as I possibly can be with where I see potential problems with how our state handled mail in voting. The machine issues that are being looked at by Rudy Giuliani, I think they're barking up the wrong tree there. There is they're going to go through that and they're going to find that the machine code is is pretty solid, in my opinion. Could things have been manipulated? Possibly. Possibly. But the reality of the situation is we've been through many elections in the past and in fact, even a democratic political action group came through in twenty sixteen. They were angry about Donald Trump winning that election. And they came to our our customers and they said, hey, we want we want to do a total recount of the entire state. So we want all of your ballot images. We want to compare them to the to the results that came out of the machines when it came to find out that the the ballot images and the machines were pretty much dead on. There's just there's just no financial incentive for a company like Dominion or a company like an election source to be involved with that that type of widespread fraud. I mean, you're risking your entire company to do that. So that's just that's just not happening, in my opinion. And if it is, it would be a huge surprise to me. It should be looked into for sure, because there's always bad actors. There could be bad actors at a company. But as far as I can tell, that that crowd is barking up the wrong tree. But there is. Unfortunately, because of the way that we did mass mail out voting, there is a potential for. A. A huge vulnerability in the election system and that vulnerability is this right here. All of the ballots that come out of the machines when they are made are digital PDF files. They are unsecured, they there is no chain of custody when it comes to them, and what I mean by that is when they are created on the on the county's software, the more software they are sent out to the printer, they are sent out to our company as as a as a company that needs to create tests for the machines. It's just a logical fact that we need that ballot in order to create those tests. So. You know, back before we did mass mail in voting, nobody thought twice about shipping those digital ballots to the appropriate sources. Nobody really felt like there needed to be a secure chain of command because, you know, what are you going to do with the digital ballot? You know, every precinct gets an allotment of ballots on Election Day and people come in and they vote in person. And there's a certain amount of registered absentee voters and it's minuscule. But the problem is the way we very sloppily handled mass mail out voting, we just kind of sent them around. And there wasn't a whole lot of accurate tracking as to where those ballots were going and who was receiving them and who is sending them back in. And there was some tracking. But just with the the sheer amount of ballots, there wasn't there wasn't there wasn't a good chain of custody for the physical ballots either, so. Because of that, I mean, this flash drive here, I wrote tests for the state of Michigan, so this flash drive here had all of the ballots for Wayne County on it. And I'm here in my bedroom right now. This is. All the ballots for Wayne County were on this, they're not on it anymore, you know, I've deleted them since, but. They were on that last drive before the election and weeks before the election, so, you know, if some. You know, if I can have them in my bedroom, right? You know, nobody nobody blinked



an eye about me having these digital files. So who else had them, right? If nobody cared that I had in my bedroom all the ballots for Wayne County. You know, I know for a fact that when those ballots gets into the printer, they get put on a Google Drive. You know, everybody thinks, you know, Google and Dropbox and Amazon are secure platforms, but in reality, any high level person at those companies has backdoor clearance to those drives. So. You know, all it takes is a scan of those drives and somebody at Google can have all the ballots for Wayne County. I mean, there's just there just is no chain of custody. And I'm not here saying that laws were broken. I'm not here saying that election source is nefarious. Not you're saying that dominion is even nefarious. But what I am saying is there is no chain of custody for digital ballots. So if some outside actor wanted to come in. With a nefarious goal of printing a hundred thousand ballots before election night, it's certainly possible. All they would have needed was this I had it in my bedroom. That's all they would have needed. And you can go. To any printer. You know, probably not a commercial one, because they'd probably be like, you know, why are you printing official ballots with us? You know, who are you? But if you had your own printer, you could I could print it on an inkjet printer at home. You know, I could have taken one of these ballots from this flash drive. And I could have printed 10000 of them. And on a laser printer. At my office. And if I had, you know, printed them there eight and a half by eleven, so it's very common, I could print them as long as I print them on cardstock. You know, there's a there's a there's a ballot stock thickness paper that you need. But I you know, that's about it, that's about the only you know, and I am pretty sure that a machine would read regular weighted paper, you know, don't quote me on that, but I'm pretty sure that they would. They probably read cardstock paper, too. But there's a specific ballot stock that next thickness. And I don't know if it's just regular card stock or not or if there is actually a specific ballot stock thickness. But yeah, it's the machine is agnostic as long as those timing marks which are on the PDF are correct. You know, about that's printed by the official printer versus a ballot is printed at home by a person that has. You know, the ballots ahead of time, because we need the ballots ahead of time, because we need to write tests, you know, it's just something that we need to do. You know, and I'm not in infectious actor. I didn't pass these ballots off to anybody, and I'm sure nobody at election source did and I'm sure nobody at Dominion did. But you know, who's to say somebody at the county knew about them or, you know, maybe not necessarily somebody at the county office, but somebody knew, you know, somebody knew that that these ballots were being stored somewhere and they took them or they or somebody at Google took them off of the Google Drive. I mean, there's plenty of avenues to get these ballots in digital form. And print them off. So I'm. That if there was election fraud. I'm not saying that there was. But if there was. That's probably where it would have been done. And because of our irresponsible. Mail in voting system where we just mass mailed it out, there's plenty of cover for a 100000 ballots coming in at midnight. You know who is going to say who's going to say, oh? You know. That's 100000 ballots, they all came in for Joe Biden. It doesn't matter because nobody there's no chain of custody. Nobody nobody knows what to expect, you know. You know, with any other election, if one hundred thousand ballots came in at midnight. You know, it would be obvious from. But nobody considers that fraud now because maybe there was one hundred thousand ballots that just were stored somewhere and nobody thought to open them up. Nobody knows, and all the



ballots are anonymous, so you'll never know. You'll never know. That's that's the story of this election, is you will never. Be guaranteed because of them, because of the mail system, you will never be guaranteed to know. For sure. The legitimate president. Or any of the downvotes, for that matter. This was a cluster fuck. This was a cluster and people are being disenfranchised. And what I'm here to tell you is that it's totally possible to bring a hundred thousand ballots, totally possible, I had this weeks before the election, plenty of time. You know, if you're a nefarious actor and you want to print a half thousand ballots and put them in boxes just in case. As long as you have this file that I had personally. You can do that. So. Is there avenues for election fraud? Yeah, absolutely. Or is it from the machines? I don't think so possible. Is there a nefarious actors at election source? No, I don't think so. Is there a serious actors at Dominion? I don't really know people at Dominion. I know people election source. They're very honest people. So please, for the love of God, leave us alone. I'm just trying to. I am just trying to tell you what's on my mind, that there is an avenue for possible fraud here. And I just had a new baby, so please, please be merciful to me, leave me alone. Please be merciful to the people at election source and leave them alone. They're good people and the people at Dominion, I'm sure most of them are just good people, you know. Is there a corruption at the top? I don't know anybody at the minute. I don't know the company at all, really. I don't know. We're a contractor for them. But, you know, we've run. Like I said, we run elections in the past for Dominion and they've come out completely scot free. OK. And the issue that happened in Antrim County, I mean, you got you have to leave that clerk alone. She's. You know, what happened there is completely, completely innocent and, you know, they had a late comer to the election, somebody that somebody that didn't get put on the ballot. Right. So they had Cotting for this ballot without that person on it. And they had a card with the coding for the person that. That was supposed to be on the ballot, so they were supposed to run the coding with the extra candidate, instead they ran the coding with the with the with the previous without the candidate in it. And that screwed everything up when they realized it on election night, they reran everything with the proper coding and everything was fine. It was no, it's not some sort of mass conspiracy from Dominion to switch votes. But is there an avenue for election fraud? Absolutely. This there's no chain of custody on ballots, it's a big deal. That's a big freaking deal. And if election officials don't take that seriously. Then they are screwing the public. Out of an accurate election. I wanted to say by.



**Exhibit D – CV James Thomas Penrose, IV**

**James Thomas Penrose, IV**  
 2550 S. Clark St.  
 Arlington, VA, 22202  
 cv@jimpenrose.org

**Education**

**George Washington University**, Washington, DC, USA  
 M.S. in Computer Science **2004**

**Drexel University**, Philadelphia, PA, USA  
 B.S. Magna Cum Laude in Computer Science **2001**  
 Minor in History and Political Science

**Experience**

Tenacity Cyber, LLC, Maryland, USA **April 2021-Present**  
**Owner**  
 Cybersecurity consulting and advisory services.

BlueVoyant, LLC, College Park, MD, USA **April 2021-Present**  
**Senior Advisor**  
 Providing expert advice on cyber security products, operations, and business to BlueVoyant senior leadership and customers.

BlueVoyant, LLC, College Park, MD, USA **2019-April 2021**  
**Chief Operating Officer**  
 Responsible for all operational aspects of BlueVoyant’s business focused on day-to-day cybersecurity delivery and execution. Primary driver responsible for innovating the Cyber Risk Management Services (CRx) offering. Thought leader to engage with prospects, customers, press and industry analysts articulating BlueVoyant’s value proposition, offerings, technology, and tradecraft. Cybersecurity expert with deep technical skills devoted to leading a tremendously talented workforce and inspiring overachievement through tenacious pursuit of success. Spearheaded the growth process by building product, engineering, sales, and marketing capabilities to take the CRx offering from concept to full operations with marquee reference customers over an 18-month period. Supported fundraising during the Covid-19 crisis to retain workforce and continued company operations with no degradation in service throughout the pandemic.

Redacted, Inc, Elkridge, MD, USA **2015-2019**  
**Executive Vice-President, Head of Product, Head of Services**  
 Served multiple leadership roles in various business units. Created a Managed Security Services (MSS) business from the business case, technology stack selection, Security

Operations Center (SOC) stand-up to initial customer acquisition and onboarding. Senior advisor to clients on all aspects of cyber risk; providing risk assessment, threat analysis, and strategic counsel to C-level executives across the financial, energy, and manufacturing sector. Offering innovative tactics to pursue and deter hostile cyber attackers targeting client businesses before a risk becomes a crisis. Created new 3<sup>rd</sup> party risk data product offerings and brought the new products to market leading to the creation of a new substantial stream of revenue.

Darktrace, Washington, DC, USA

**Executive Vice-President of Cyber Intelligence** **2014-2015**

Responsible for overall cyber threat intelligence activities of Darktrace in support of customers globally. Served as the primary assessor of cyber threats detected by Darktrace across all clients. Featured in public speaking engagements on behalf of Darktrace as a subject matter expert and thought leader on cyber operations. Performed media interviews with both television and print reporters on cyber issues.

National Security Agency (NSA), Fort George G. Meade, MD, USA

**Sub-Panel Member, National Security Agency Advisory Board** **2014-2017**

Participates in the National Security Agency's Emerging Technologies Panel creating insight and recommendations for the Director of NSA.

**Chief – Operational Discovery Center** **2013-2014**

Built and led a large organization with multiple project teams, both civilian and contractor, and managed a multi-million dollar budget to achieve top priority of enabling discovery in signals intelligence (SIGINT).

**Technical Director for Counterterrorism (CT) – SIGINT Directorate** **2010-2013**

Ensured technical competence in the execution of global CT operations. Drove the creation of new SIGINT capabilities in support of the CT mission. Led engagements with foreign partners in order to build CT capacity with our allies.

Central Intelligence Agency, Langley, VA, USA

**2009-2010**

**Senior NSA Representative – Technical Targeting Department, Counterterrorist Center**

Coordinated joint NSA/CIA operational activities in support of Counterterrorism

National Security Agency, Fort George G. Meade, MD, USA

**2008**

**Global Network Exploitation and Vulnerability Analyst – Remote Operations Center, Tailored Access Operations**

Provided analytic support to drive computer network operations against high priority targets.

**Global Network Exploitation and Vulnerability Analyst,  
NSA Commercial Solutions Center**

**2007-2008**

Employed and integrated industry best practices and products into NSA analytic practices.

**Mission Manager – NSA/CSS Threat Operations Center**

**2005-2007**



Led intelligence production and military planning integration activities for a variety of missions focusing on computer network defense, exploitation, and attack.

**Watch Operations Officer – Computer Network Operations Fusion Center 2005**  
 Provided rotational 24-hour support as the focal point for intelligence queries from operational military elements conducting computer network operations.

**Technical Director – CNO Division, Office of Information Operations 2004-2005**  
 Led technical SIGINT exploitation activities of foreign CNO actors in support of military and intelligence community requirements.

**Global Network Exploitation and Vulnerability Analyst,  
 - Office of SIGINT Support to Information Operations 2001-2004**  
 Performed software development, integration, and testing of SIGINT capabilities to support CNO analysis. Created and integrated new capabilities into the SIGINT system for use by production analysts.

**Unix System Administrator – Directorate of Technology 1999-2000**  
 Performed a myriad of Unix system administration activities including full automation of Y2K upgrades for globally deployed, remotely administered systems.

**Intrusion Detection Analyst – Information Systems Security Organization 1997-1998**  
 Analyzed intrusion detection logs from various sources, evaluated threats, created incident reports, and made recommendations to remediate vulnerabilities.

### Awards

- Presidential Rank Award (Awarded Post Govt Service) 2016
- Director of National Intelligence Medal (Awarded Post Govt Service) 2015
- Elevated to Defense Intelligence Senior Level (DISL) from GS-14 2008
- National Intelligence Meritorious Unit Citation 2001, 2007, 2008
- Joint Meritorious Unit Award 2003, 2007
- Exceptional Performance Bonus 2009, 2010, 2011, 2012
- Spot promotion from GS-12 to GS-13 for Special Achievement 2005
- 13 Special Achievement Awards 1998-2008

### Professional Development

- NSA Director's Leadership Program 2013
- Joint Duty Assignment at Central Intelligence Agency 2009-2010
- NSA Senior Technical Development Program 2010
- Graduate Certificate in Computer Security and Information Assurance  
 George Washington University 2003

### Research Experience

- Undergraduate Research Assistant, Drexel University,  
Software Engineering Research Group

2000-2001

**Fraternal Organizations**

- Knights of Columbus

# Exhibit 14

**Analyst: Jeffrey Lenberg**

**Date: May 3, 2021**

### **Executive Summary**

Vote modification in Antrim County was consistent with technical manipulation of the election project file. This project file was generated and deployed by ElectionSource for the November 3, 2020 election.

ElectionSource configured and deployed Antrim County's project files that resulted in the modification of the votes during the election. The modification demonstrates manipulation of any and all races on the ballot. Administrator access (via administrator password) permits modification to these project files and creates inaccurate vote tally results observed during the election in Antrim County.

The SQL Management Studio Version 17.1 was found to be installed on the Antrim County Election Management System (EMS) (see Douglas Logan's Report dated 4/9/2021). This software is not certified by the Election Assistance Commission for use on electronic voting systems. This software tool was utilized in expert testing to replicate the Antrim County November 3, 2020 election vote tally manipulation. Testing using this software tool was consistent with technical manipulation of the project file resulting in inaccurate vote tallies.

The ElectionSource staff responsible for the creation and deployment of the project have direct access to make specific modifications to the project files. Testing indicates that vote modification can be pre-planned and deployed prior to an election. ElectionSource staff possesses all of the administrative access to make selective modification of the project files to manipulate the vote tally for any targeted county, precinct, or race.

Logs from the EMS indicate ElectionSource technicians responsible for deploying the project files to Antrim County also had access to numerous other counties project files to include:

Alcona	Alger	Alpena	Arenac	Berrien
Calhoun	Charlevoix	Cheboygan	Gogebic	Houghton
Iosco	Isabella	Keweenaw	Manistee	Marquette
Menominee	Midland	Otsego	Presque Isle	Schoolcraft
Wayne	Wexford			

It is unclear if modifications to the above counties listed impacted the Antrim County project file.



## Project Files

Testing of Antrim County project files indicates that modification of the project files can replicate the election inaccuracies observed in the November 3, 2020 election. In addition, further testing revealed that selective modification of the project files resulted in tailored manipulation of the votes tallied. The manipulation can be tailored to modify a specific county, precinct, or race. The steps used to manipulate the vote tally are listed below:

- Modify the specific precinct election files
  - Edit the VIF\_BALLOT\_INSTANCE.DVD
  - Note: Technical access to ElectionSource corporate resources would allow for these types of manipulations to the elections.
- Burn Compact Flash cards with the configurations for the tabulators
- Run the Election (Process the Ballots through the Tabulator)

The results of the modifications to the project file will show vote totals changed on the tabulator's printed tape as well as modified vote totals in the Results Tally Reporting (RTR) system.

In order to validate these findings; two test cases were run:

1. The swap of Trump and Jorgenson vote totals on both the paper tape and the RTR results
2. The swap of Biden and Trump (Presidential Race) and Ferguson and Bergman (Congressional) while leaving the Senate race unmodified on both the paper tape and the RTR results

Exhibit A contains photos of all the ballots that were run for test case number 2 as well as the paper tapes and RTR tallies showing the manipulations.

Both test cases were successful in that the modifications were made without any alerts or error messages being generated by the EMS or the tabulator. The test cases would not have been detected during the canvassing process because both the paper tapes and the RTR results matched.

## SQL Database Tools on the EMS

The SQL Management Studio Version 17.1 was found on the EMS (see Douglas Logan's report dated 4/9/2021) and this software is not certified by the Election Assistance Commission (EAC) for use on electronic voting systems. The SQL tool is a utility that enables the modification of project files and databases on the EMS.

Testing shows the replication of the Antrim County election vote manipulation as asserted by Halderman from November 3, 2020 modifying the vote totals on the EMS by utilizing the SQL tool resident on the EMS. The use of SQL tool requires no special access beyond being able to log into the EMS itself. Therefore, any actor with access to the EMS could create this manipulation of the election results.

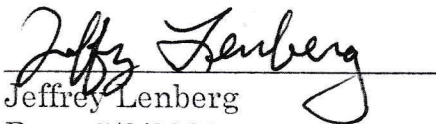
### **ElectionSource Staff Access to Other Counties**

ElectionSource staff that worked on the Antrim County project file also had access to a number of other counties across Michigan to include:

Alcona	Alger	Alpena	Arenac	Berrien
Calhoun	Charlevoix	Cheboygan	Gogebic	Houghton
Iosco	Isabella	Keweenaw	Manistee	Marquette
Menominee	Midland	Otsego	Presque Isle	Schoolcraft
Wayne	Wexford			

These counties appeared in the UserInfo log file on the EMS as being previously opened projects that were being utilized by the ElectionSource technician during the same timeframe that the ElectionSource technicians was working to configure and deploy project files for Antrim County.

It is certain that the ElectionSource technician had access project files for more than just Antrim County. It is unclear whether the configuration of the other counties had an impact on the Antrim county election.

  
 Jeffrey Lenberg  
 Date: 5/3/2021



**MICHIGAN NOTARY ACKNOWLEDGEMENT**

State of Michigan  
County of Michigan

The foregoing instrument was acknowledged before me on this 3<sup>rd</sup> day of May, 2021 by Jeffrey Lenberg.

Notary Public Signature: *A.M. Howard*

Notary Printed Name: Ann M. Howard

Acting in the County of: Oakland

My Commission Expires: 2/24/2023

**ANN M. HOWARD**  
Notary Public, State of Michigan  
County of Oakland  
My Commission Expires 02-24-2023  
Acting In the County of Oakland

Exhibit A – Test Case #2 – Presidential and Congressional Swap Only

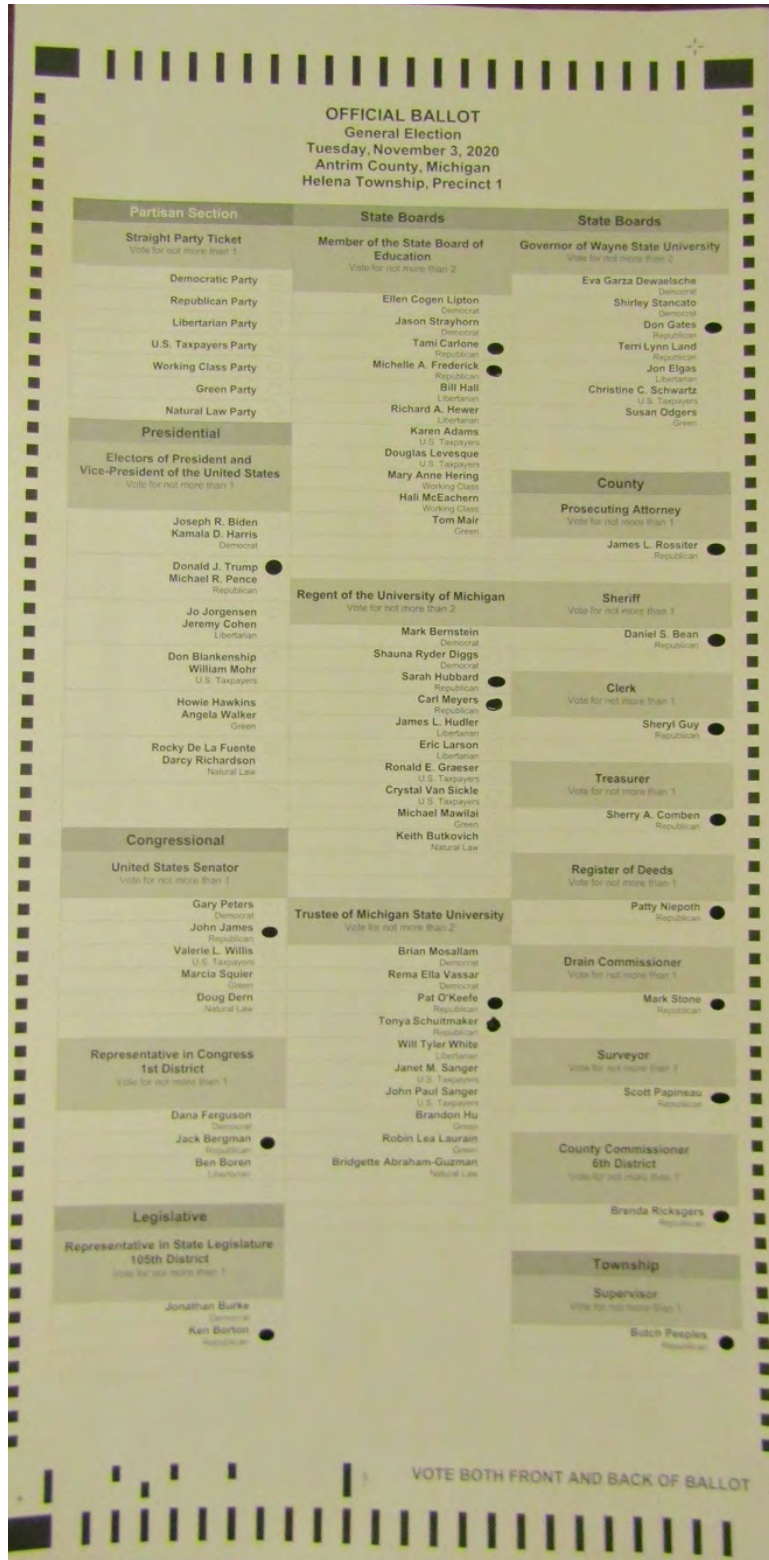


Figure 1 - Trump/James/Bergman

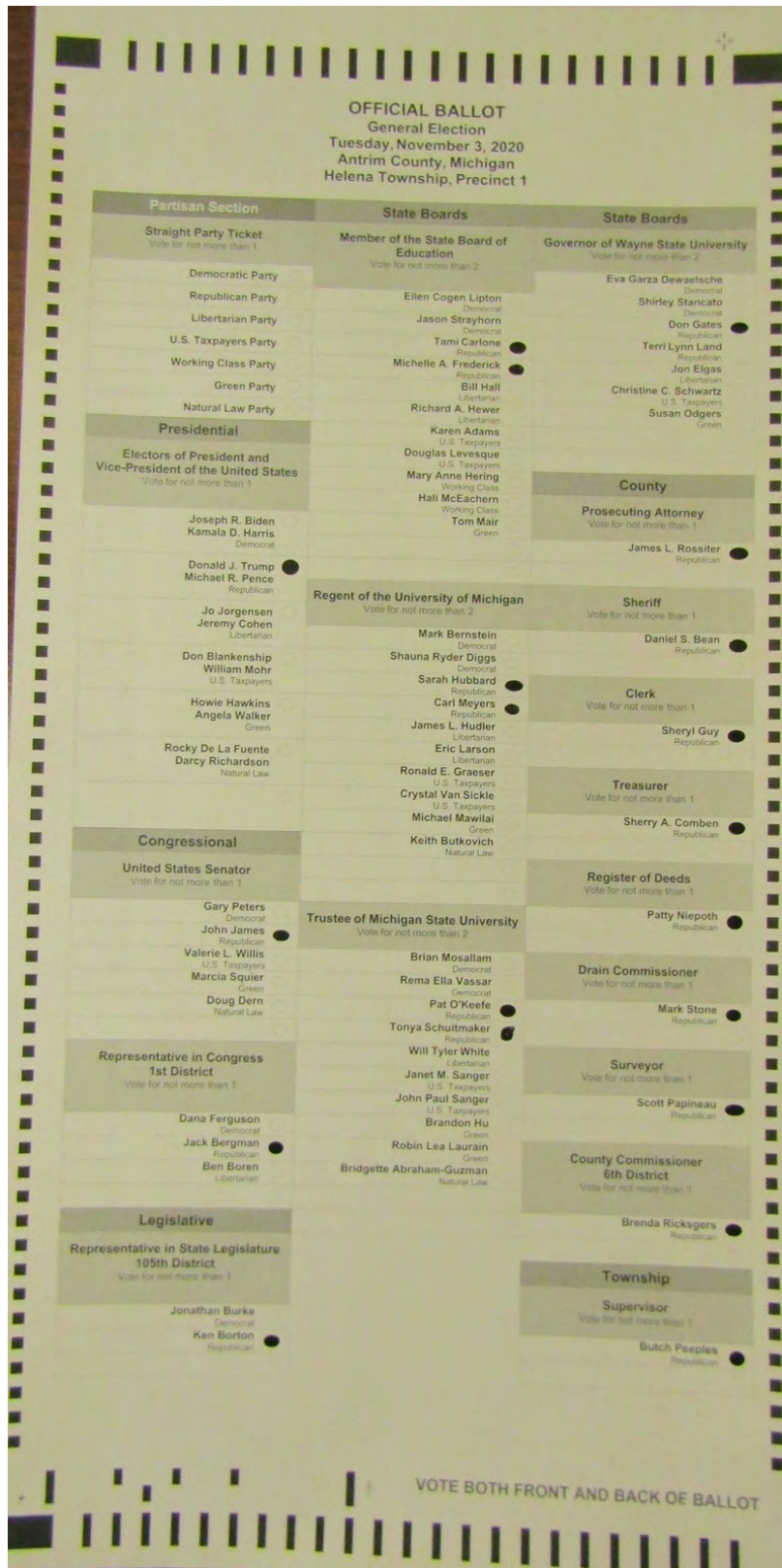


Figure 2 - Trump/James/Bergman



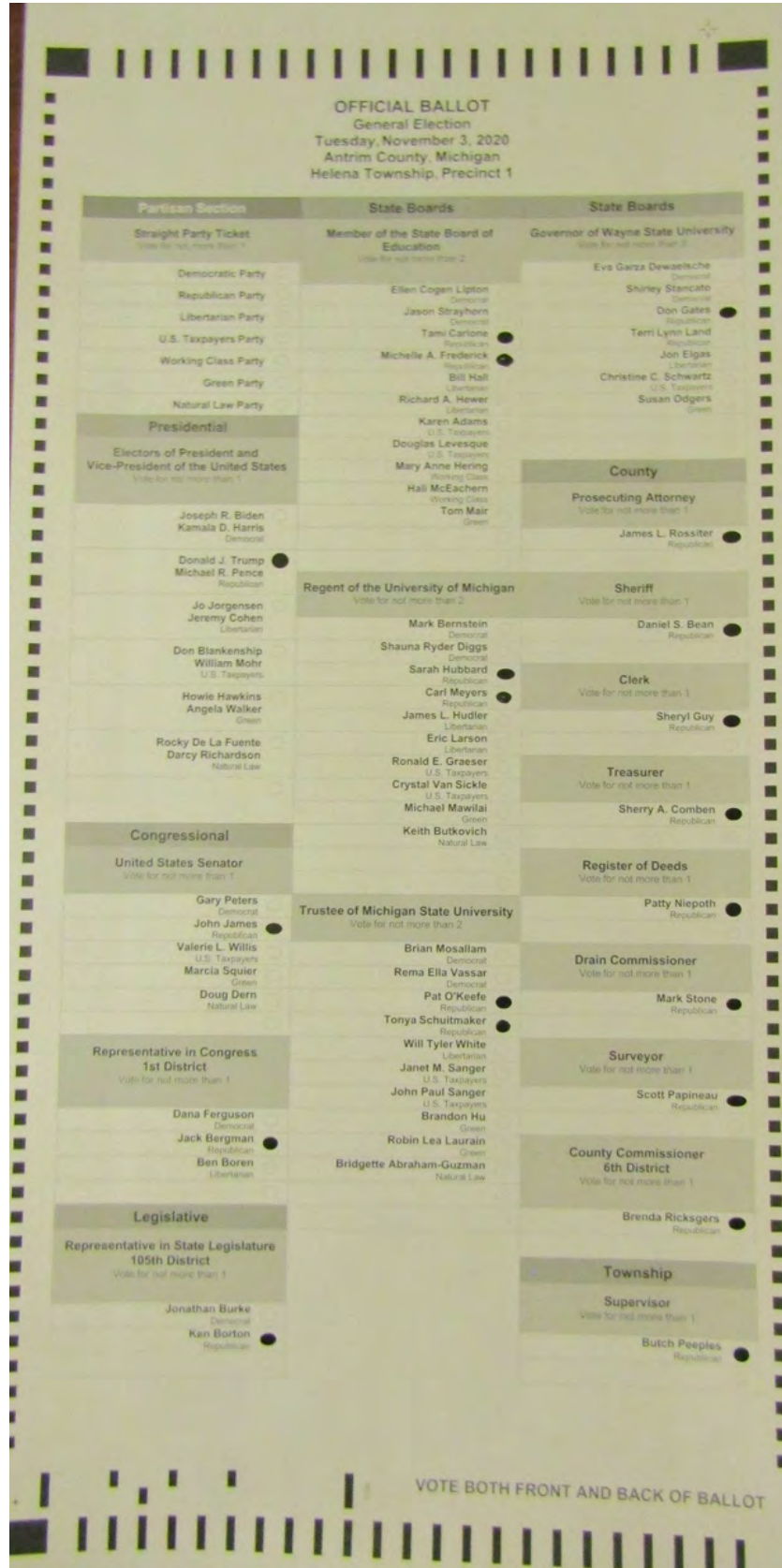


Figure 3 - Trump/James/Bergman

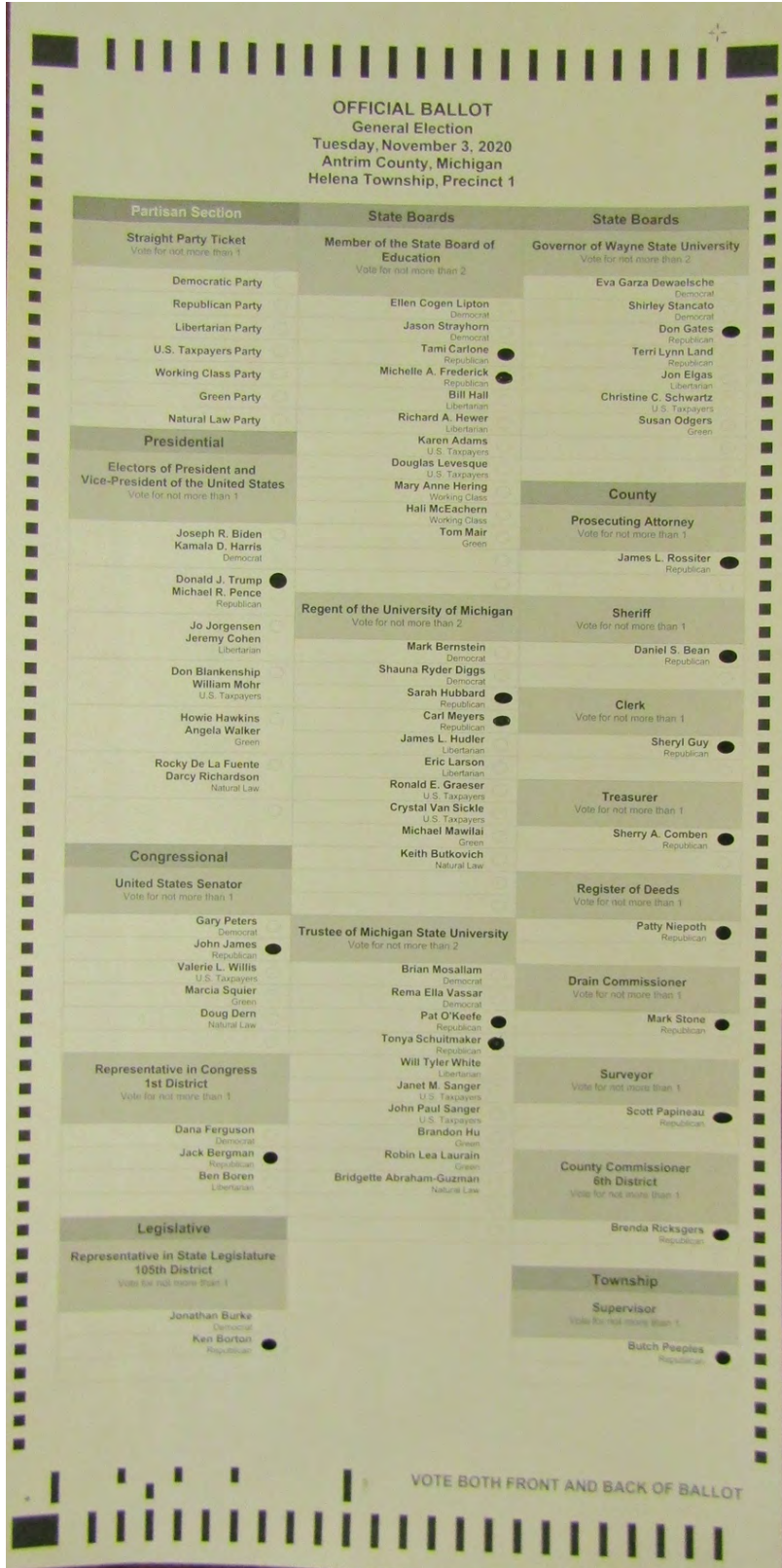


Figure 4 - Trump/James/Bergman



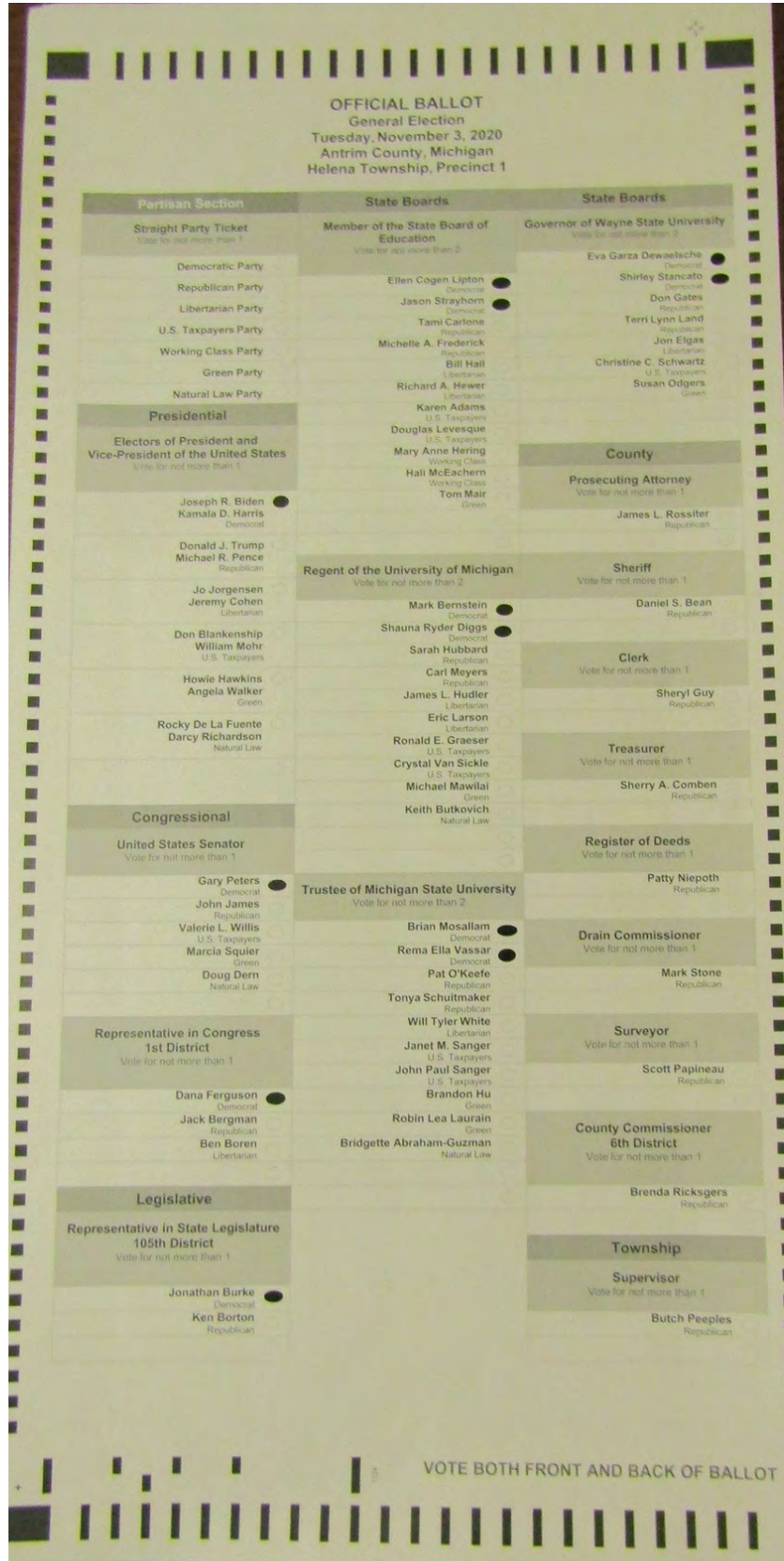


Figure 5 - Biden/Peters/Ferguson



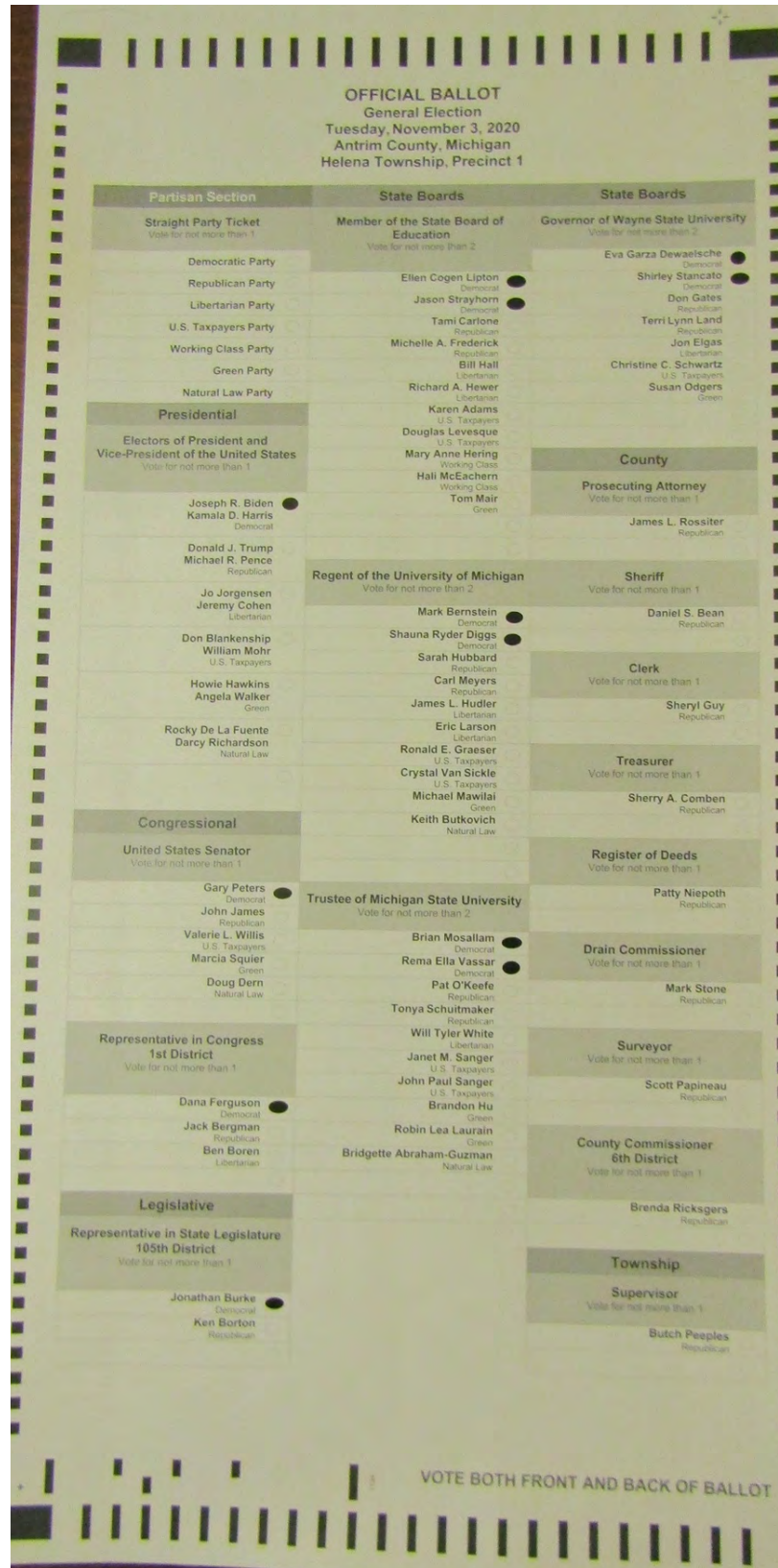


Figure 6 - Biden/Peters/Ferguson

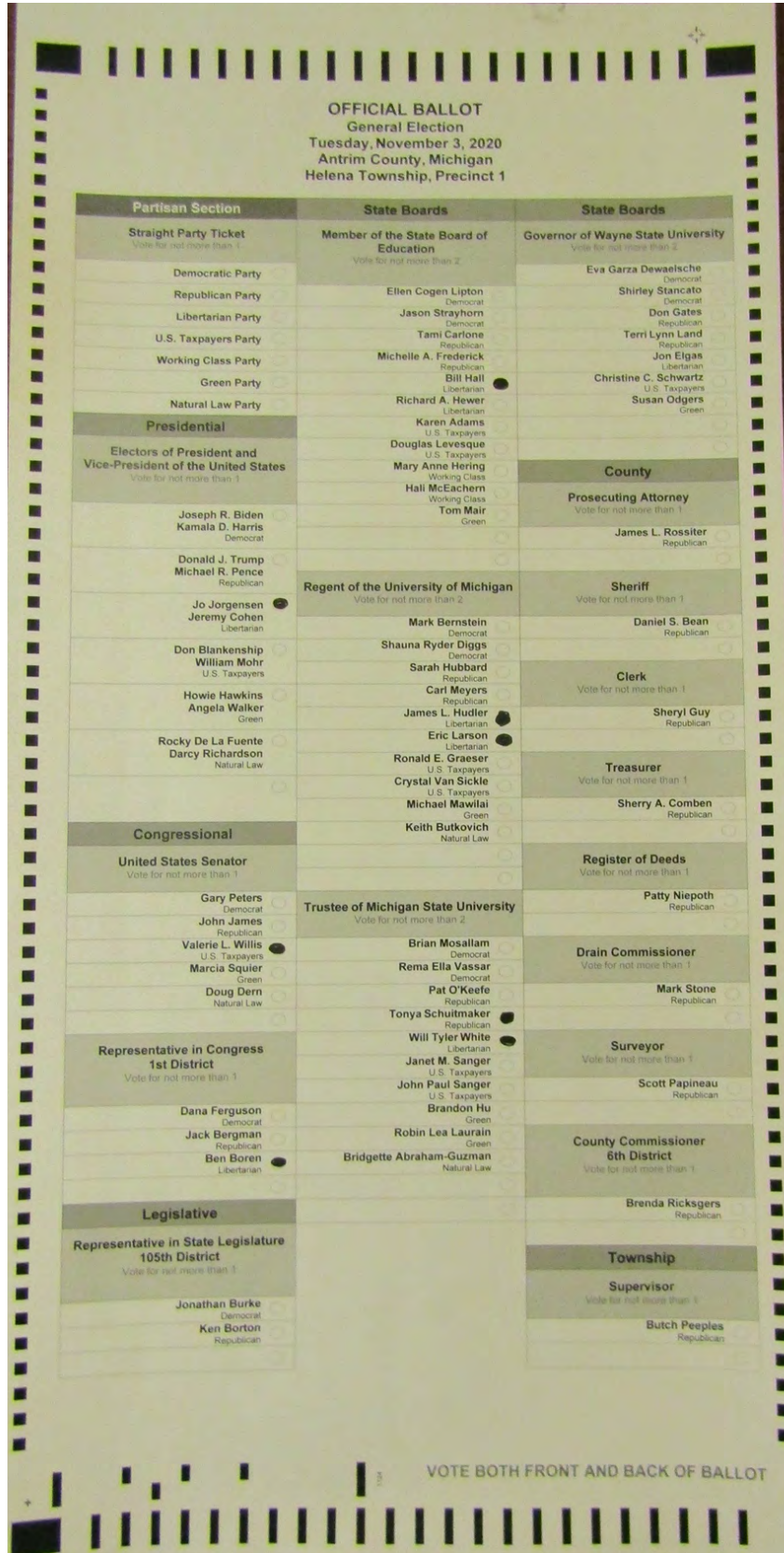


Figure 7 - Jorgenson/Willis/Boren

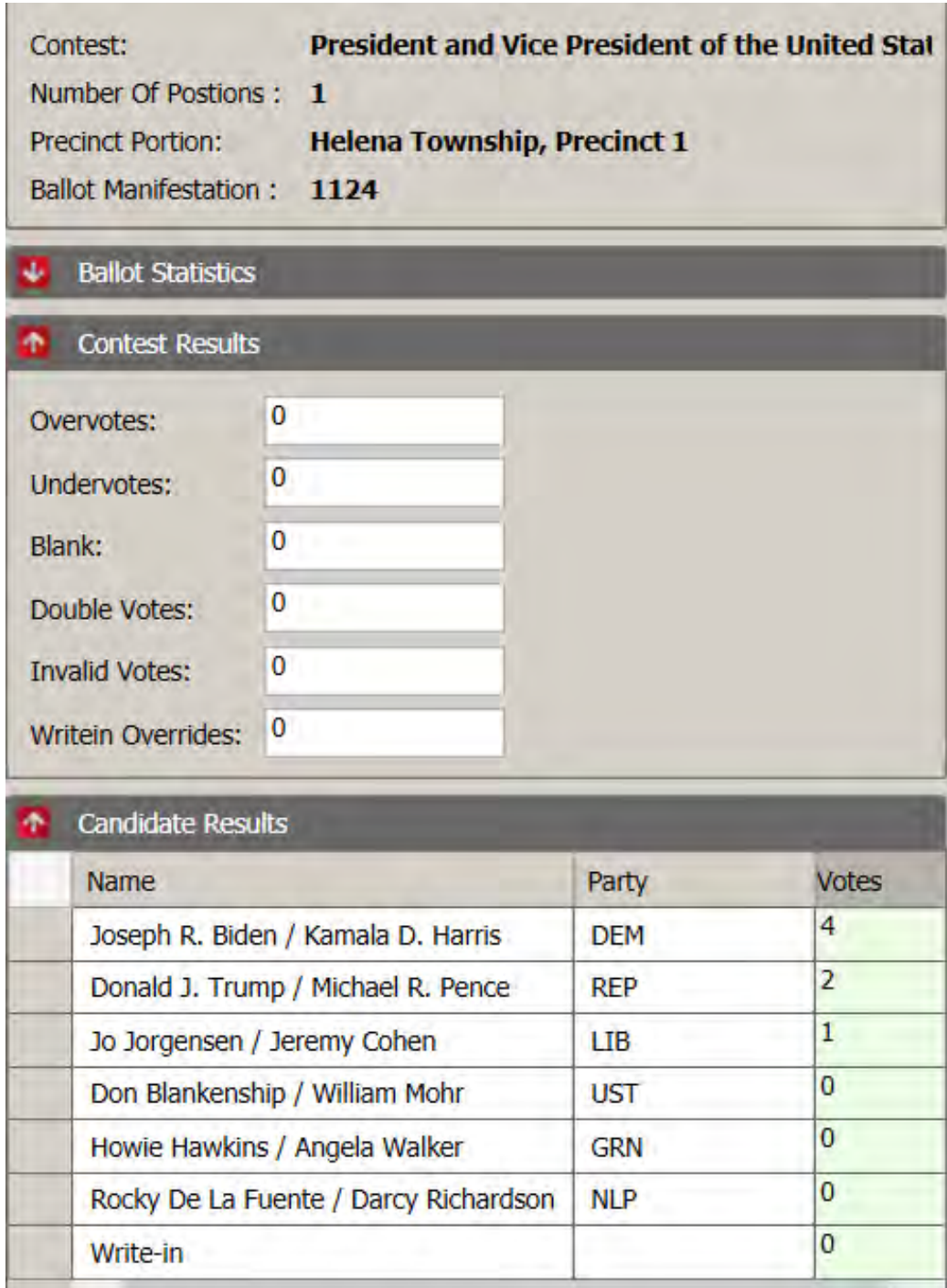


Figure 8 - Trump/Biden Flipped on RTR



Contest: **United States Senator for State**  
 Number Of Postions : **1**  
 Precinct Portion: **Helena Township, Precinct 1**  
 Ballot Manifestation : **1124**

**Ballot Statistics**

**Contest Results**

Overvotes:   
 Undervotes:   
 Blank:   
 Double Votes:   
 Invalid Votes:   
 Writein Overrides:

**Candidate Results**


Name	Party	Votes
Gary Peters	DEM	2
John James	REP	4
Valerie L. Willis	UST	1
Marcia Squier	GRN	0
Doug Dern	NLP	0
Write-in		0

Figure 9 - Senate - Correct - No Flip




Contest: **Representative in Congress 1st District**  
 Number Of Postions : **1**  
 Precinct Portion: **Helena Township, Precinct 1**  
 Ballot Manifestation : **1124**

---


 **Ballot Statistics**

---

 **Contest Results**

Overvotes:   
 Undervotes:   
 Blank:   
 Double Votes:   
 Invalid Votes:   
 Writein Overrides:

---

 **Candidate Results**

Name	Party	Votes
Dana Ferguson	DEM	4
Jack Bergman	REP	2
Ben Boren	LIB	1
Write-in		0

Figure 10 - Congressional District - Ferguson/Bergman Flipped

President and Vice President of the United States (1)	
Joseph R. Biden / Kamala D. Harris (Democrat):	4
Donald J. Trump / Michael R. Pence (Republican):	2
Jo Jordansen / Jeremy Cohen (Libertarian):	1
Don Blankenship / William Mohr (U.S. Taxpayers):	0
Howie Hawkins / Angela Walker (Green):	0
Rocky De La Fuente / Darcy Richardson (Natural Law):	0
Write-in:	0
Total Votes:	7

United States Senator for State (1)	
Gary Peters (Democrat):	2
John James (Republican):	4
Valerie L. Willis (U.S. Taxpayers):	1
Marcia Squier (Green):	0
Doug Dern (Natural Law):	0
Write-in:	0
Total Votes:	7

Representative in Congress 1st District (1)	
Dana Ferguson (Democrat):	4
Jack Bergman (Republican):	2
Ben Boren (Libertarian):	1
Write-in:	0

Figure 11 - Paper Tape Results Showing Presidential/Congressional Flipped - Senate Correct

Exhibit B – Jeffrey Lenberg CV

Retired Distinguished Member of the Technical Staff Sandia National Laboratories Chief Technology Officer World Light Power LLC, World Light Africa Limited

Jeff Lenberg graduated from the University of New Mexico with a Bachelors degree (1978) and Masters degree (1980) in Electrical Engineering. While in college he gained two years experience at the NASA Dryden Flight Research Center at Edwards AFB, CA working on the development of flight simulators.

In 1980 Jeff joined Sandia National Laboratories. He retired in December, 2011 after thirty-one plus years at the labs. He spent several years as a first level supervisor and finished his career as a Distinguished Member of the Technical Staff.

The first twelve years at Sandia, Jeff developed satellite systems involving flight hardware, test software, test systems, project management, and supervisor roles.

For two and a half years, he led the development of secure national and international networks for export control while on assignment at DOE headquarters in Washington DC. While in DC and on his own time, he was involved in the investigation of potential election fraud associated with the 1994 Maryland gubernatorial election. He assisted the FBI with data analysis in their investigation which was initiated in March 1995.

After returning from Washington and for the rest of his career, Jeff performed national vulnerability assessments and led the development of national security related projects. These projects required systems analysis, hardware (including low power microsystems) and software design, team development, project management, and program development. These projects varied from a one person, \$100K project to a one hundred person, \$20M project.

While working on national security projects, Jeff held high level security clearances. He worked on projects with several governmental

agencies. He led “black hat” teams whose objective was to expose vulnerabilities by developing ways to break in (if possible) to what were considered to be secure systems and demonstrate that it could be done (physical security, secure hardware, and secure software systems).

In 2012 after Jeff retired from Sandia Labs, he started a renewable energy development company and in 2014 started a company based in Nairobi, Kenya to help create African jobs and bring energy to those who are without it.



# Exhibit 15



**SHERYL A. GUY**  
Antrim County Clerk  
P.O. Box 520  
Bellaire, Michigan 49615  
Phone (231) 533-6353  
Fax (231) 533-6935  
guys@antrimcounty.org

December 15, 2020

To: Township Clerks and Recount Team members

From: Sheryl Guy, County Clerk  
Connie Wing, Election Specialist

The Secretary of State/Bureau of Elections will be performing an

**ALL COUNTY AUDIT**

CONDUCTED BY THE STATE

**COVID PROTOCOL WILL BE FOLLOWED AND MASKS WILL BE PROVIDED**

Original Audit scheduled for 2 days State changed to 1 day

**Date: December 17, 2020 9:00 a.m. Kearney Township Hall**

**VOLUNTEERS:**

- Please note arrival time 8:45 a.m.
- Lunch will be provided at 12:00 noon

**TOWNSHIP CLERKS:**

All canisters must be brought to the Kearney Township Hall that morning or make arrangements for authorized transporter to get them to Kearney Township and the Local Clerks are responsible please deliver between 8:00 a.m. – 8:30 a.m.

Recount Team Members:

Carolyn Barnett	Judy Kosloski	Donna Heeres	Deb Hiltz
Cherie Hogan	Taylor Blackmore	Vickie Bishop	Marvin Rubingh
Jan Olach	Greg MacMaster	Martha Hawkins	Irene Shooks
Fred Goldenberg	Martha Davidson	Shelley Boisvert	Don Seman
Jonathan Kelly Sumner	Dale Eschenburg	Dorothy Eschenburg	Bonnie Robbins
Laura Reid Edwards			

Thank you.

# Exhibit 16

---

## Antrim County Audit by Bureau of Elections

1 message

---

**Meingast, Heather (AG)** <MeingastH@michigan.gov>

Tue, Dec 15, 2020 at 10:35 AM

To: Matthew DePerno <matthew@depernolaw.com>, "Haider A. Kazim" <hkazim@cmda-law.com>

Cc: "Grill, Erik (AG)" <GrillE@michigan.gov>, "Albro, Lisa (AG)" <AlbroL@michigan.gov>

Dear Counsel,

For your information, the audit will commence at 9:00 a.m. on Thursday, December 17 at the Kearney Township Hall, 4820 Aero Park Drive, Bellaire, Michigan. All attendees must wear a face covering that covers their nose and mouth and social distance. You are welcome to attend the meeting as members of the public.

Thank you,

Heather

Heather S. Meingast, Division Chief

Civil Litigation, Employment & Elections Division

Michigan Department of Attorney General

meingasth@michigan.gov

(517) 335-7659 (office)



# Exhibit 17

/2022 1:49:42 AM

### HAND COUNT CALCULATION SHEET

**OFFICE:** President of the United States

**COUNTY:** Antrim

Jurisdiction	Biden			Trump			Jorgenson			Hawkins			Blankenship			De La Fuente		
	Democratic Party			Republican Party			Libertarian Party			Green Party			U.S. Taxpayers Party			Natural Law Party		
	Original	Hand Count	Net	Original	Hand Count	Net	Original	Hand Count	Net	Original	Hand Count	Net	Original	Hand Count	Net	Original	Hand Count	Net
<b>TOTAL VOTES</b>	<b>7769</b>	<b>5959</b>	<b>-1810</b>	<b>4509</b>	<b>9759</b>	<b>5250</b>	<b>93</b>	<b>190</b>	<b>97</b>	<b>29</b>	<b>28</b>	<b>-1</b>	<b>22</b>	<b>17</b>	<b>-5</b>	<b>12</b>	<b>9</b>	<b>-3</b>

<b>TOTAL CHANGE</b>	<b>-1810</b>	<b>5250</b>	<b>97</b>	<b>-1</b>	<b>-5</b>	<b>-3</b>
---------------------	--------------	-------------	-----------	-----------	-----------	-----------

Banks Township, Precinct 1	349	349	0	756	758	2	11	11	0	2	2	0	1	1	0	1	1	0
Central Lake Township, Precinct 1	549	549	0	908	906	-2	16	16	0	6	6	0	1	1	0	0	0	0
Chestonia Township, Precinct 1	197	93	-104	3	197	194	0	3	3	0	0	0	0	0	0	1	0	-1
Custer Township, Precinct 1	523	240	-283	11	521	510	4	11	7	0	1	1	1	2	1	0	0	0
Echo Township, Precinct 1	392	198	-194	8	392	384	1	8	7	0	2	2	2	1	-1	0	0	0
Elk Rapids Township, Precinct 1	1198	984	-214	625	1029	404	8	17	9	5	9	4	5	4	-1	0	0	0
Forest Home Township, Precinct 1	755	610	-145	19	753	734	1	19	18	1	0	-1	0	1	1	2	1	-1
Helena Township, Precinct 1	432	306	-126	4	430	426	0	4	4	1	1	0	1	0	-1	0	1	1
Jordan Township, Precinct 1	372	182	-190	13	369	356	1	14	13	0	1	1	1	1	0	2	0	-2
Kearney Township, Precinct 1	744	470	-274	16	743	727	0	16	16	0	3	3	3	0	-3	4	0	-4
Mancelona Township, Precinct 1	276	277	1	835	835	0	20	20	0	0	0	0	0	0	0	1	1	0
Mancelona Township, Precinct 2	247	247	0	646	646	0	13	13	0	1	1	0	2	3	1	0	0	0
Milton Township, Precinct 1	686	767	81	484	1023	539	14	18	4	3	0	-3	1	2	1	1	4	3
Star Township, Precinct 1	462	166	-296	10	468	458	0	10	10	0	0	0	0	0	0	0	0	0
Torch Lake Township, Precinct 1	527	461	-66	8	526	518	1	7	6	1	2	1	1	1	0	0	1	1
Warner Township, Precinct 1	60	60	0	163	163	0	3	3	0	9	0	-9	3	0	-3	0	0	0