Subject: Assessment of Halderman Expert Report Dated March 26, 2021
Analyst: James Thomas Penrose, IV and Jeffrey Lenberg
Date: 6/23/2021

Executive Summary

This assessment describes inaccuracies, omissions, and incorrect statements contained in the report authored by J Alex Halderman Dated March 26, 2021.

Halderman repeatedly asserts in his report that the underlying causes of what he calls discrepancies in the vote totals were attributed strictly to human error. He asserts that the election software should "do more to help election staff," while in fact the election software is subverted to do exactly the opposite. The Election Management System (EMS) in Antrim County is subverted, see the Lenberg report dated June 9, 2021 titled, "Case Study Banks Township - Antrim County Election Management Server Found to be Subverted." The subversion of the EMS prevents election workers from being notified of errors that would have permitted them to identify the problems with the compact flash cards provisioned for use during their election.

He specifically states that his analysis and conclusions account entirely for the discrepancy seen in Antrim County on election night. This is inaccurate. According to his explanation and logic, the shift of a vote by one index should have moved votes for Presidential Candidate Joe Biden / Vice-Presidential Candidate Kamala Harris to the Natural Law Party – Straight Party Vote. In reality, when this index shift occurred, the vote was recorded as an undervote, not as Natural Law Party, Straight Party vote that would have caused all of Biden/Harris's votes to move to the Natural Law Party Candidate, Rocky de la Fuente. On election night in Antrim County, all of the shifted Biden/Harris votes were turned into undervotes thus negating Halderman's explanation and logic. The Lenberg report dated June 9, 2021 titled, "Case Study Banks Township - Antrim County Election Management Server" explains in detail why this happened due to a subversion of the Antrim County EMS. Halderman is incorrect that his theory entirely explains what happened in Antrim County during their election, the evidence to the contrary shows that Dominion Democracy Suite software was subverted to allow the erroneous processing of the shifted votes to complete successfully.

The question of precisely who utilized the subverted Dominion Democracy Suite software, performed the remote anonymous administration activities, and ultimately fixed the issues is not possible to be ascertained from the forensics and discovery material available for analysis. The Lenberg report dated May 16, 2021, titled "Summary of Security Deficiencies in the Antrim County Voting Systems," details how the user account of Ben Smythe made changes to the EMS and the Antrim County election, but the true identity of Ben Smythe is not attainable through forensics alone and in fact appears to be a strawman user shared by all with access to the EMS, not a real human. Halderman completely disregards this fact in his assessment that local officials are the reason for the inaccurate vote totals, and erroneously concludes that there were no related security breaches that could have caused the issues experience in Antrim County.

Halderman asserts that the “irregularities” in the Antrim County election were not caused by a security issue or breach of any type. The expert report from Ben Cotton dated June 9, 2021 highlights two anonymous, administrator privileged, connections to the Antrim County EMS server. The fact that any anonymous connections were permitted to the EMS is a very serious security breach, as all remote connections must be attributable to a provisioned user account for security oversight and auditing purposes; best practice for cyber security is that there are no anonymous accounts permitted on critical systems. The operational deployment of the Antrim County EMS did not prohibit anonymous access and in fact allowed remote access and administration. This remote access security flaw is exacerbated by the commonality and sharing of administrative level passwords.

Cyber attackers frequently employ anti-forensic techniques in an attempt to delete or modify system logs and software configurations in order to cover their tracks and hide the true nature and timeline of their prior activities. The remote, anonymous, access to the Antrim County EMS on both Nov 5th and Nov 17th affords a cyber attacker the access needed to clean up the evidence of prior activities on the Antrim County EMS. Given this common tradecraft used by cyber attackers to hide their tracks, the experts analyzing the Antrim County must assume that logs and configurations may have been adulterated prior to the acquisition of forensics on December 6, 2021.

He also states that last minute ballot design changes were unlikely to have occurred in other jurisdictions in Michigan. This assertion is not substantiated with any evidence, there was no such data available for an expert to draw this conclusion. In fact the only empirical evidence that we have from Antrim county would lead one to deduce exactly the opposite. In Antrim County the quality control checks exhibited by ElectionSource to create the ballot definitions for Antrim County were inadequate and failed. If the same inadequate security and quality control processes employed in Antrim County were also employed statewide by ElectionSource, it is likely that the same bad actor would have attempted to subvert many other jurisdictions thus leading to inaccurate vote totals statewide.

Halderman asserts that “additional oversight of local election officials” is needed to avoid inaccurate elections such as this in the future. It is not accurate to assert that this is only a local official problem. The activities that led to the inaccurate vote totals in Antrim County involved ElectionSource, not only the local officials. Indeed, the ElectionSource technicians played a major role in the inaccurate vote totals that occurred in Antrim County, and in many cases, were the actual humans configuring critical election systems on behalf of the local election officials.

Halderman’s analysis of the inaccurate vote totals impact in Central Lake and Warner Townships entirely omitted the fact that there was an extremely high ballot reversal rate of 111% in Logic and Accuracy Testing in Warner Township on October 20, 2020. Central Lake Township had an 82% ballot reversal rate on November 6, 2020 when the ballots were reprocessed. He offers no explanation for why the high reversal rate in Warner Township during LAT was not identified and addressed; nor does he notice the fact that the reversals on November 6, 2020 in Central Lake Township are the same type of error message. The error message indicates that the outer makers on the ballots were too large and out of specification for processing. The omission of these facts and the lack of any remediation activities because of the high error rate during LAT illustrate a substantial omission of critical evidence from Halderman's assessment of the Antrim County inaccurate vote totals.

Details

Subverted Election Software Vice Deficient Software

From page 3 of Halderman's report:

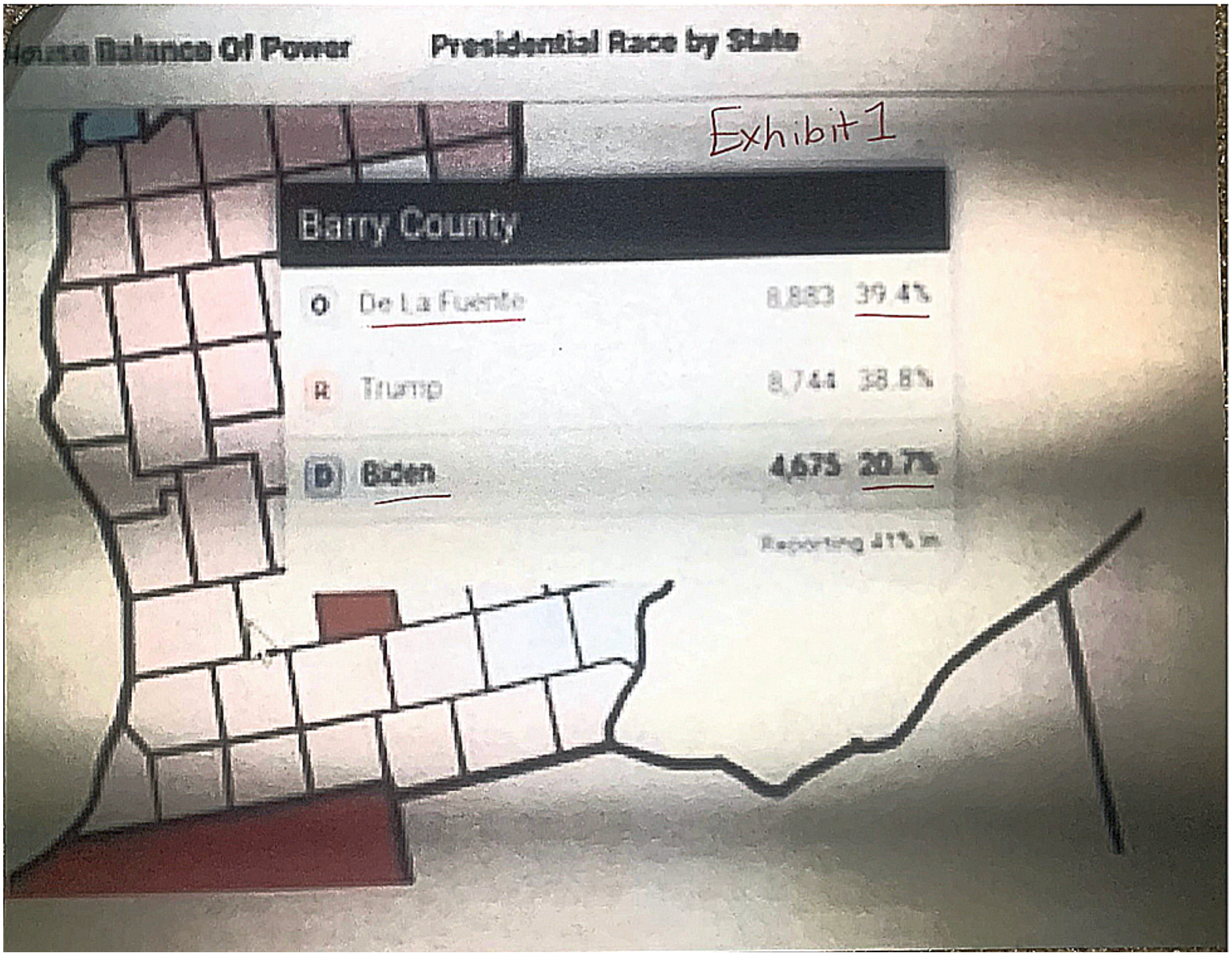
> – *The explanations provided by the county [2] and the Department of State [23] are correct that the inaccurate unofficial results were a consequence of human errors, but the problems were somewhat more complicated than initially understood. The human errors that initiated the incident were compounded by gaps in election procedures and their adherence. The election software also could have done more to help election staff avoid making mistakes that could lead to erroneous results.*

Halderman states, "the election software also could have done more to help election staff avoid making mistakes that could lead to erroneous results," and later in the report he further says, "the election management system did not alert the operator about this problem while loading the results."

The Lenberg report dated June 9, 2021 titled, "Case Study Banks Township - Antrim County Election Management Server Found to be Subverted," explains the specific subversion of the error handling routine in the Dominion Democracy Suite Election Management Server (EMS). The fact that the EMS software treats movement of any internalMachineIDs across contests as an undervote versus recording the vote based on the internalMachineID index indicates that specific error handling code was modified to allow for vote shifts within individual contests, but designed to mute movements between contests. The movement of an index outside of the contest it originated in, creates an undervote, it is as if the vote never happened at all according to the EMS's error handling routines.

The EMS subversion is designed to avoid "bleed-over" situation where the shifted index creates an obvious artifact of the fraud. A prime example of such an artifact can be found in the Lenberg report dated May 15, 2021, titled "Evidence of Vote Shifting in Barry County Michigan." This report includes a graphic taken from an affidavit of a Barry County resident that shows the election night reporting system reflecting the Natural Law Party Candidate, Rocky de la Fuente with 8,883 votes with 41% of the precincts reporting, see Figure 1.

The artifact in Figure 1 matches precisely the expected behavior of the EMS when processing a vote shift **without the subversion in the EMS error handling routine.** This is the reason that Rocky de la Fuente had so many votes at that point during election night in Barry County. The EMS software is installed locally on each EMS machine in every individual jurisdiction. Variations between the software configuration of the EMS in Antrim and Barry counties explains why in Antrim county, “logical bumpers” exist to protect from bleed-over, however, in Barry there were no logical bumpers at that time of election night. Of course, ad hoc updates to the Barry County EMS configuration may have been performed to deploy the subversion to the EMS on election night or the next morning. Forensic images of the EMS in Barry County along with the ElectionSource technician’s field laptop, and removeable media would be needed to make a complete evaluation of the inaccurate vote totals in Barry County.



Barry County

O	De La Fuente	8,883	39.4%
R	Trump	8,744	38.8%
D	Biden	4,675	20.7%

Reporting 41% in

Figure 1 - Artifact of Vote Shifting in Barry County, Michigan During November 3, 2020 Election

Security Breach of Antrim County EMS

Halderman makes his conclusion on page 48 of his report stating:

> *Several of the election procedures that broke down due to human error are important security protections. Furthermore, the EMS lacks important security updates, has weak authentication and access control mechanisms, and is vulnerable to compromise if an attacker has physical access to the computer. These are serious vulnerabilities that should be mitigated on a priority basis, but there is no evidence that any of these problems was ever exploited in Antrim County. My analysis has precisely accounted for all known anomalies in Antrim's November 2020 election results, and none was the product of a security breach.*

Halderman's unequivocal assessment that the inaccurate vote totals found in Antrim County were not the product of a security breach is unfounded. The affidavit from Benjamin R. Cotton dated June 8, 2021 highlights two remote, anonymous logins to the Antrim County EMS server:

> *The first occurred on 11/5/2020 at 5:55:56 PM and the second occurred on 11/17/2020 at 5:16:49 PM EST. Both of these logons appeared to have escalated privileges at the time of logon. Given that this computer was supposed to be on a private network, this is very alarming.*

Anonymous, remote, access to the Antrim County EMS in the days after the November 2020 election casts doubt Halderman's assertion that the inaccurate vote totals in Antrim County was not linked to a security breach. As discussed earlier, the lack of Windows security log data prior to November 4, 2020 prevents a full analysis of the extent to which a breach may have occurred and the full extent of unauthorized access to the voting systems. Typical behavior of a cyber attacker is to clean up log files after they are done perpetrating their acts, this is done in order to cover their tracks and avoid forensic analysis of their activities. Knowing that these anonymous, remote logins occurred before December 6, 2020 when the forensics were acquired for the Antrim County election equipment including the EMS, it must at least be contemplated that the EMS's files, configuration, and logs were adulterated prior to the forensics acquisition process on December 6, 2020.

It is also critical to recall that there are no windows security logs present on the EMS before November 4, 2020 due to the retention policy for those log files. The absence of this forensic data makes it inappropriate to conclude that there no security breaches of the EMS prior to November 4, 2020. On the contrary, given evidence of anonymous, remote access to the EMS on both November 5th and again on November 17th, it is likely that the same actor had access prior to November 4th, using precisely the same techniques to breach the EMS.

This remote access security flaw is exacerbated by the commonality and sharing of administrative level passwords. Halderman fails to note that the same password was utilized for the Windows accounts named AdjSys, EMSADMIN, EMSADMIN01, EMSUSER, ICCUSER01, ICCUSER02 and the EMSEPUSER. Halderman also failed to note that the security problem of shared of passwords did not solely exist at the Windows User level on this system, it was also present in the actual database user's access as well. The users admin and RTRAdmin shared a common password. Additionally, the accounts ROAdmin, SAdmin and MRO01 all shared a common password. Halderman entirely omitted the fact of these security breaches, and the relevant question of who accessed the EMS remotely using an anonymous login. Therefore, Halderman was incorrect in his specific conclusion that there were no security breaches. A security breach can be caused by a system administrator or technician as easily as a cyber attacker. A user authorized to access the EMSUSER account and who accessed the EMSADMIN account (because they were the same password) would constitute a security breach. Based on the log retention policies that were in place on the EMS server, the windows event log history was extremely limited. To further compound the complexity of the security situation, there is a fundamental lack of user attribution. No record of which actual human was provided the individual EMS account access nor when the account was utilized who the actual person was that utilized the account. These blatant violations of sound security practices make Halderman's statement that there was no security breach of the system inaccurate. If you cannot ensure that only authorized personnel accessed the system, there is no way to assert that unauthorized accesses or breaches did not occur. If Halderman cannot account for remote anonymous user accesses and activity, then he cannot assert that unauthorized accesses or breaches did not occur.

The Customer Experience Improvement Program (CEIP) has been found to be disabled in the Microsoft Windows registry and yet was enabled by the Dominion Democracy Suite software on the EMS. The CEIP program is typically enabled as a Microsoft tool to report back telemetry to Microsoft to improve their application performance. However, in this case, there is no evidence to suggest that CEIP was enabled through routine use of Microsoft software. It appears that it was enabled by an unknown third-party to gather the same telemetry for a different purpose. Moreover, the logs and telemetry generated by the CEIP process are set to automatically delete every 5 minutes and they are not retained for use in security or performance audits. The most likely explanation for this CEIP process is to assist a user that is modifying system behavior which might cause severe errors to occur; the CEIP process allows a user to discover severe errors and respond to them without leaving a lasting log for security analysis. Halderman made no mention of this tool in his report.

Inappropriate Assumption Regarding Last Minute Ballot Changes

Halderman, on Page 4, states the following regarding last minute ballot changes across the State of Michigan:

> *The incident in Antrim County arose due to the county's mishandling of last-minute ballot design changes, a circumstance that is unlikely to have occurred widely in Michigan during the 2020 election.*

This statement from Halderman pre-supposes that last-minute ballot changes were the true origin of the inaccurate vote totals in Antrim County. Given the absence of evidence from the Michigan Secretary of State on this issue occurring in other counties, the abnormalities seen in Barry County during election night (Figure 1), and the fact that unauthorized actors had access to the EMS prior to the forensic acquisition of the EMS on December 6, 2020, it is impossible to conclude with certainty that last minute ballot changes was the true origin of the inaccurate vote totals in Antrim County. Vulnerability testing has revealed that remote interactive changes using a virtual machine image of the Antrim County EMS have been able to replicate the anomalies found in the Antrim county election results, see Lenberg's May 9, 2021 report titled, "Preliminary Report of Subversion in the Antrim County Election Management System, Results Tallying and Reporting Application."

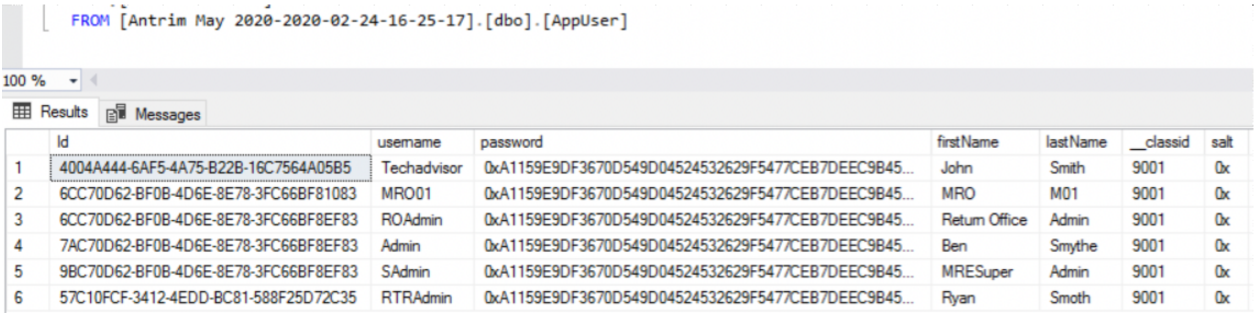
The timeline of events affords an actor ample time to concoct an explainable scenario and modify the files and logs on the EMS to reflect that data. The high-level timeline of events is as follows:

- November 4, 2020 – Antrim County Officials Determine Election Has Irregularities
- November 5, 2020 – Anonymous remote login to the Antrim County EMS
- November 6, 2020 – Antrim County Reprocesses Central Lake Township Ballots
- November 17, 2020 – Anonymous remote login to the Antrim County EMS
- December 6, 2020 – Forensics acquisition of Antrim County election equipment
- December 17, 2020 – State Bureau of Elections conducted Antrim County recount of the presidential race only

The actor with anonymous remote access to the Antrim County EMS had up to 31 days total to concoct an explainable scenario as to what happened on election night in Antrim County. In the most conservative assessment of the actor's activities, the actor had 13 days (until the November 17, 2020) to determine and implement the changes needed to have the files, configurations, and logs on the EMS to comport with the last-minute ballot change narrative given by the State of Michigan.

Omission - Lack of Attribution of Administration Activity on EMS

Halderman entirely omits from his report any analysis or discussion of the usage of shared administrator accounts on the EMS. The Lenberg report dated May 16, 2021, titled "Summary of Security Deficiencies in the Antrim County Voting Systems," lists the EMS accounts that have administrator access to the critical EMS software package.



```
FROM [Antrim May 2020-2020-02-24-16-25-17].[dbo].[AppUser]
```

	Id	username	password	firstName	lastName	__classid	salt
1	4004A444-6AF5-4A75-B22B-16C7564A05B5	Techadvisor	0xA1159E9DF3670D549D04524532629F5477CEB7DEEC9B45...	John	Smith	9001	0x
2	6CC70D62-BF0B-4D6E-8E78-3FC66BF81083	MRO01	0xA1159E9DF3670D549D04524532629F5477CEB7DEEC9B45...	MRO	M01	9001	0x
3	6CC70D62-BF0B-4D6E-8E78-3FC66BF8EF83	ROAdmin	0xA1159E9DF3670D549D04524532629F5477CEB7DEEC9B45...	Return Office	Admin	9001	0x
4	7AC70D62-BF0B-4D6E-8E78-3FC66BF8EF83	Admin	0xA1159E9DF3670D549D04524532629F5477CEB7DEEC9B45...	Ben	Smythe	9001	0x
5	9BC70D62-BF0B-4D6E-8E78-3FC66BF8EF83	SAdmin	0xA1159E9DF3670D549D04524532629F5477CEB7DEEC9B45...	MRESuper	Admin	9001	0x
6	57C10FCF-3412-4EDD-BC81-588F25D72C35	RTRAdmin	0xA1159E9DF3670D549D04524532629F5477CEB7DEEC9B45...	Ryan	Smoth	9001	0x

Figure 2 - EMS Database Administrator Account List

The use of the account "Ben Smythe" as the administrator to make changes on the EMS obfuscates the name of the true user responsible for the administrative activity. This lack of detailed attribution to user and administrator activity again makes it impossible to reach the conclusion that there were no security breaches during the Antrim County election.

Moreover, there is a pattern of anonymous login accounts and shared accounts being used for escalated privilege and administrative functions. These vulnerable configurations are non-compliant with cyber security best practices put forward by the National Institute of Standards and Technology[1] and the Department of Homeland Security[2]. In critical systems, such as voting systems, identity and access management is paramount to ensure attribution of administrative and user activity to the specific individual taking the action. Halderman disregards the severe lack of security controls related to identity and access management in the Antrim County Dominion voting systems, ignoring a critical aspect of cyber security best practices.

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

Jeffrey Lenberg

Jeffrey Lenberg

James T Penrose

James Thomas Penrose, IV

[1] https://nvd nist.gov/download/800-53/800-53-controls.xml

[2] https://us-cert.cisa.gov/ncas/alerts/aa20-245a

MICHIGAN NOTARY ACKNOWLEDGEMENT

State of Michigan
County of Oakland

The foregoing instrument was acknowledged before me on this 23rd day of June, 2021 by James Thomas Penrose, IV and Jeffrey Lenberg.

Notary Public Signature: Ann M. Howard

Notary Printed Name: Ann M. Howard
Acting in the County of: Oakland
My Commission Expires: 2/24/2023