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

1 Maricopa County – Analysis of Senate Review – Cyber Ninjas Response

Maricopa County continues to purposely mislead Arizonans and the American public about the nature of audit findings, and the impact they had on the 2020 General Election. Their response renames and redefines audit findings so the claim can be made that the findings are false, includes logical sounding arguments that simply don't add up, and is completely devoid of any supporting evidence. The following response to their review continues to refute their baseless claims with evidence and citations.

1.1 Voted using Prior Address (Pg. 6, 14 & 16)

The County stated that the US Postal Services National Change of Address (NCOA) should have been used as a trusted source. Melissa utilizes the NCOA for their move data. Melissa is a trusted source. This is clearly documented within the report within the respective findings and ignored by the County's response. This validates the audit results.

The lack of precision from the County's response also leaves a lot in question. Our report provides in the appendixes a full list of every voter ID affected, as well as details as to when and where that individual moved. The County's response doesn't even confirm an exact number of records that were validated, nor the explanation for why the records they validated were not an issue. The County expects that simply asserting that our claim is false makes it false, rather than providing any documentation to validate their claims.

Furthermore, the County's claim that voters can legally change their addresses after the voter registration period and still legally vote is an extremely misleading statement. Our report was primarily[1] based on the November 7th VM34 voter roll file, and therefore any address changes should have been reflected in that version of the file. In addition, this is only possibly applicable for individuals who move within Maricopa County (15,035) and would not apply to individuals who moved outside of the County (12,772) and would therefore be required to re-register to vote. It would also be expected that the County would be able to state exactly how many of the 15,035 changed their address, rather than making a blanket statement and implying that it fully explains the finding. The fact the County chose not to do this raises more questions.

It is also unclear why the analysis in the County's response for this finding talks about double-voters. This finding has nothing to do with double voters.

1.1.1 Mail-in Ballots Voted from Prior Address

On Twitter, the County suggested that the largest of our findings associated with a change in address was inaccurate because it didn't take into account college students, snowbirds, or military personnel. The County did not read the report very carefully if it believes that college students and snowbirds could significantly impact these numbers. The finding very clearly states that the address was checked after the documented move date and if anyone was still at the residence with the same last name the voter ID was removed from the list. This should account for almost all situations with college student and snowbirds.

[1] Please see page 20 of the Maricopa County Forensic Election Audit Volume III: Results Details report for additional details: https://c692f527-da75-4c86-b5d1-8b3d5d4d5b43.filesusr.com/ugd/2f3470_d36cb5eaca56435d84171b4fe7ee6919.pdf

The question of military personnel is potentially a legitimate partial answer. The voter rolls clearly delineate military personnel by specifying a military address, as well as frequently having eligibility for voting via the Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA). While the former is less likely to impact the numbers for the same reasons as the college students and snowbirds; UOCAVA eligible voters can vote via email, fax, or a portal in addition to via mail and it shows up as a mail-in vote. As a result, they would not necessarily have to have access to their prior residence address to receive their ballot in order to cast a mail-in-ballot. Running the 23,344 voter IDs who voted via mail-in ballots even though they had moved against a list of UOCAVA eligible voters finds 1,344 UOCAVA voters. This means the proper count for the first finding in our report should be an even 22,000.

1.2 More Early Ballots Returned by Voters Than Received

The numbers simply do not support the County's claim that the curing of ballots would result in a second scanning of the envelope, and therefore a second EV33 entry for a received ballot. This is a soundbite, not an explanation.

The 9,041 voter IDs that had more EV33 returned ballot entries than EV32 sent ballots, and the individual voted via mail was provided to Dr. Shiva to see if there was any correlation between these voter IDs and the prevalence of more than one scanned envelop. Only 2,138 of these voter IDs had more than one scanned ballot. If the County's explanation properly accounted for this issue, then there should be a one-for-one match with multiple scanned ballots for all 9,041 voter IDs. This simply cannot explain the issue when only 24% of the 9,041 had multiple envelop image scans.

1.3 Voters That Potentially Voted in Multiple Counties

It does not appear the County read the report carefully. The finding is extremely clear that the list of identified individuals should be validated further as name and birthdate overlaps can occur and be shared by different people. The County has access to full social security numbers and driver's license numbers. The audit does not. It is not uncommon nor improper for an audit to find things that require additional investigation, and we look forward to the Attorney General's review of this finding rather than the County's cursory dismissal of this issue as a "Faulty Claim".

Had the County taken this finding seriously their reply could have shown a good faith effort to validate the finding and indicate the quantity validated and the reasons why they were not valid. Without any numbers or evidence, it can only be assumed that the County completely dismissed this, as stated, as a "Faulty Claim".

NOTE: The County renamed this finding in their response to take out the word "Potentially" so it could be listed as a faulty claim, rather than recognized the validity of the finding.

1.4 Official Results Does Not Match Who Voted

This finding is accurate as written. The Official Results from the Canvass do not match the list of voters in the VM55 file. The County attempted to conceal this flaw by renaming this finding in their response to "Official Results Don't Include All Voters" for the sole purpose of falsely discrediting the claim. Their explanation states that protected voters are not included in the VM55 file and therefore there is a discrepancy. This does not explain the issued raised by the audit team; the fact the County couldn't reply with a precise number of protected voters who voted in the election that matches the outlined discrepancy shows that their response is not accurate and willingness to address flaws in their system is non-existent.

Furthermore, several weeks before the hearing the Senate attorney reached out to the County to request an explanation for this so that it could be ensured that the audit report was as accurate as possible. The County ignored the request for weeks and then replied to the request the night before the hearing with the details about the protected voters list. To ensure the accuracy of our audit despite the County's willful lack of cooperation, we both discussed this possible explanation in the hearing and included disclaimers in the report for findings that would be invalid if this information was true.

1.5 More Duplicate Ballots than Original

The County's response is extremely misleading and does not respond to any of the specific details outlined within the audit report. In the case cited by the County, Ward vs. Jackson, only 1,626 ballots were reviewed, while the audit reviewed all of the duplicated ballots[2]. The "spilled box of UOCAVA ballots" referenced in the County's response was not a box, but a stack of 20. That stack of 20 slide onto the ground in a manner that even maintained the order of the ballots; and was promptly picked up and put back in the box. This occurred within the contained space of the Senate's special ballot coral under the direct view of Ken Bennett and the Secretary of State observer, Ken. This doesn't account for anything close to the discrepancies detected by the audit.

Furthermore, the "detailed records" provided by the County for duplicate ballots were shown by the audit to be incorrect and full of mislabeling and other errors as documented in the report. Detailed records are only useful if they're correctly recorded.

1.6 EMS Database & Logs Purged, Files Deleted

The County's response to the purged and deleted data and files shows they do not know what is going on within their Election Management System (EMS), and that they didn't carefully read the subpoena. Not only are many of the items that were deleted specifically listed in the original subpoena, and therefore a request for an archive or backup wouldn't be needed; but the dates and timelines in their response to the audit report and on Twitter is not supported by the dates in the logs on the machines. Furthermore, what was done for the November 2020 general election does not match any past elections found on the EMS Server; countering any arguments that the purging and deletion of files is "standard procedure", and the over 2 terabytes of free storage on the device counters any arguments it had to be done for space. These arguments are handled in the following sections but show clear evidence that data that should have been protected by the subpoena was instead destroyed.

1.6.1 False County Claim: The Senate Needed to Subpoena Backups or Archives

The Senate did not need to subpoena backups or archives. All disputed items were clearly outlined within the Senate, this is nothing more than an attempt to misdirect and mislead. The original subpoena[3] item #4 clearly requests the "November 2020 general election in Maricopa County, Arizona", "Election Log Files" and "any other election files and logs", and it goes on to list "any other election files or logs" associated with the "Tabulators", "Result Pair Resolution", "Result Files", and "SQL Database Files". DVD result files and SQL database files are among the list of items deleted.

---

[2] https://recorder.maricopa.gov/justthefacts/courtcases/7%20Ward%20v.%20Jackson%20(AZ%20Supreme%20Court)/Ward%20v.%20Jackson%20APPEAL%20-%202020.12.08%20DECISION%20ORDER%20(Ward%20v.%20Jackson,%20Ariz.%20S.%20Ct.).pdf (pg. 4)

[3] https://www.scribd.com/document/531671852/SUBPOENA-January-12-2021-NEW-Senate-Sub-to-Maricopa-County

In addition, at the point where the SQL Database was purged of all data associated with the results of the November 2020 general election and later filled with audit data from ProV&V, it no longer would be a file reflective of the "November 2020 general election"; but would be a file that represented the ProV&V "audit". This would mean it would not meet the requirement from the subpoena for the SQL Database files associated with the election.

Furthermore, the original subpoena[4] item #7 clearly requests the "November 2020 general election in Maricopa County, Arizona", all "Windows Server & Desktop" "Windows event logs and Access logs". The Security event logs were not provided separately for any of the systems; even though this is the definition of what an "Access Log" is for a "Windows Server & Desktop". Since these logs were rolled over prior to us receiving the machine, they no longer covered the subpoenaed period of time.

1.6.2 False County Claim: Standard Archival Steps Were Taken on February 2nd.

The Results Tallying and Reporting (RTR) logs clearly show that all database data as well as files in the NAS directory were purged and deleted on February 1st. The action was started at 5:14:47 pm and finished at 5:20:00 pm. If any backups or archives were conducted on February 2nd, the data was already deleted.

userRelatedInfo	executedCommand	operationTimestamp
RTRAdmin	User initiates the OnPurgeResults activity	2021-02-01 17:14:47.363
RTRAdmin	PurgeResultsCommand (execution duration: 76478ms):All result files from database were deleted.	2021-02-01 17:16:27.810
RTRAdmin	PurgeResultsCommand (execution duration: 288779ms):The result files database, result files and images from NAS were deleted. Purging of results has finished successfully.	2021-02-01 17:20:00.097

If it was normal to purge data as can be seen in the finding in the audit report, it would be expected that this would be true for every other election on the EMS Server. However, as can be seen in the screenshots below the data is still present for other past elections. Since the drive had more than 2 terabytes of free space available there was no technical reason to delete the data before the two audits hired by Maricopa County. In fact, it begs to question what the auditors had to audit if there were no election results when ProV&V arrived on Feb 2nd.

[4] https://www.scribd.com/document/531671852/SUBPOENA-January-12-2021-NEW-Senate-Sub-to-Maricopa-County

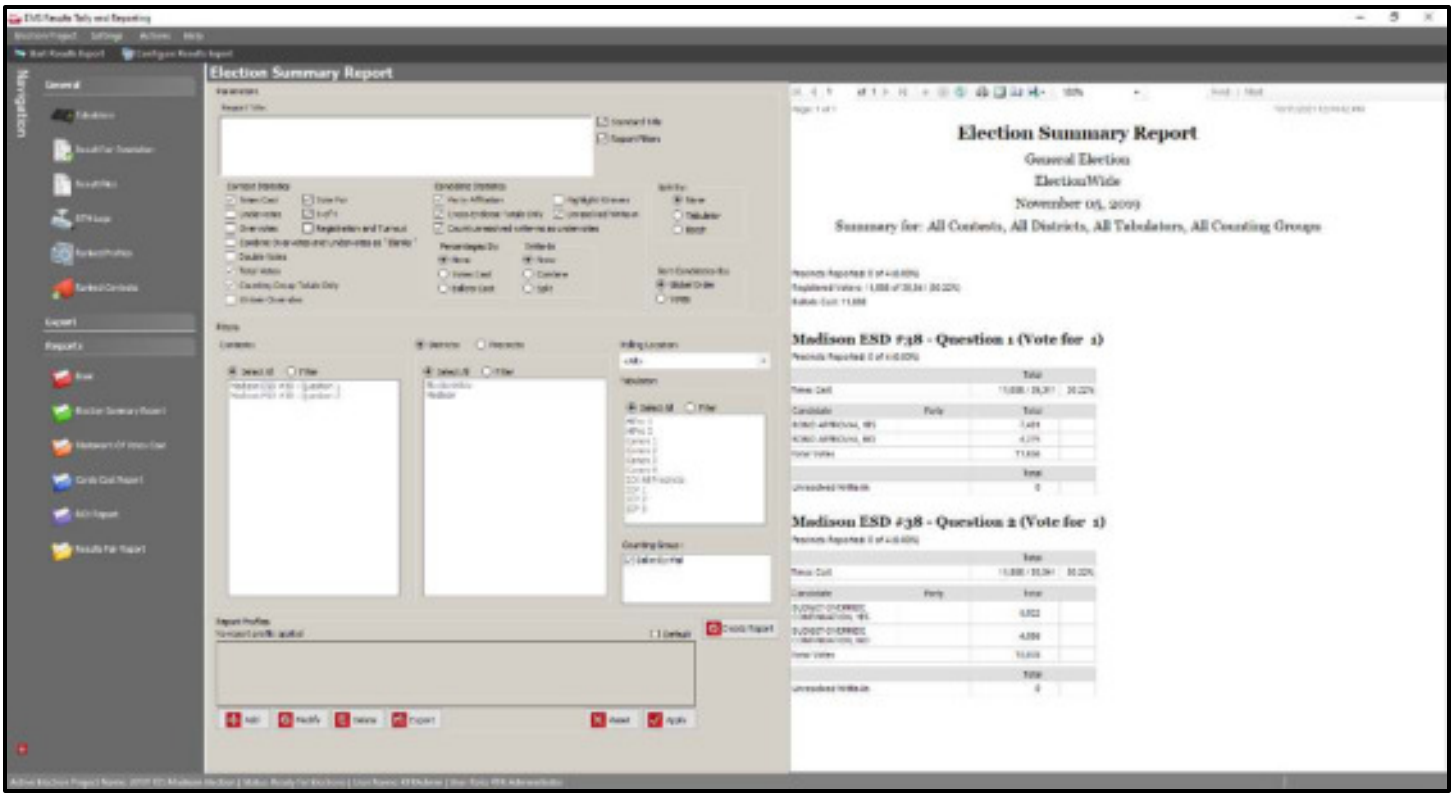


Figure 1 - Election Results for the 2019 Madison Election. These numbers match the Official Results on the Recorder's Site.

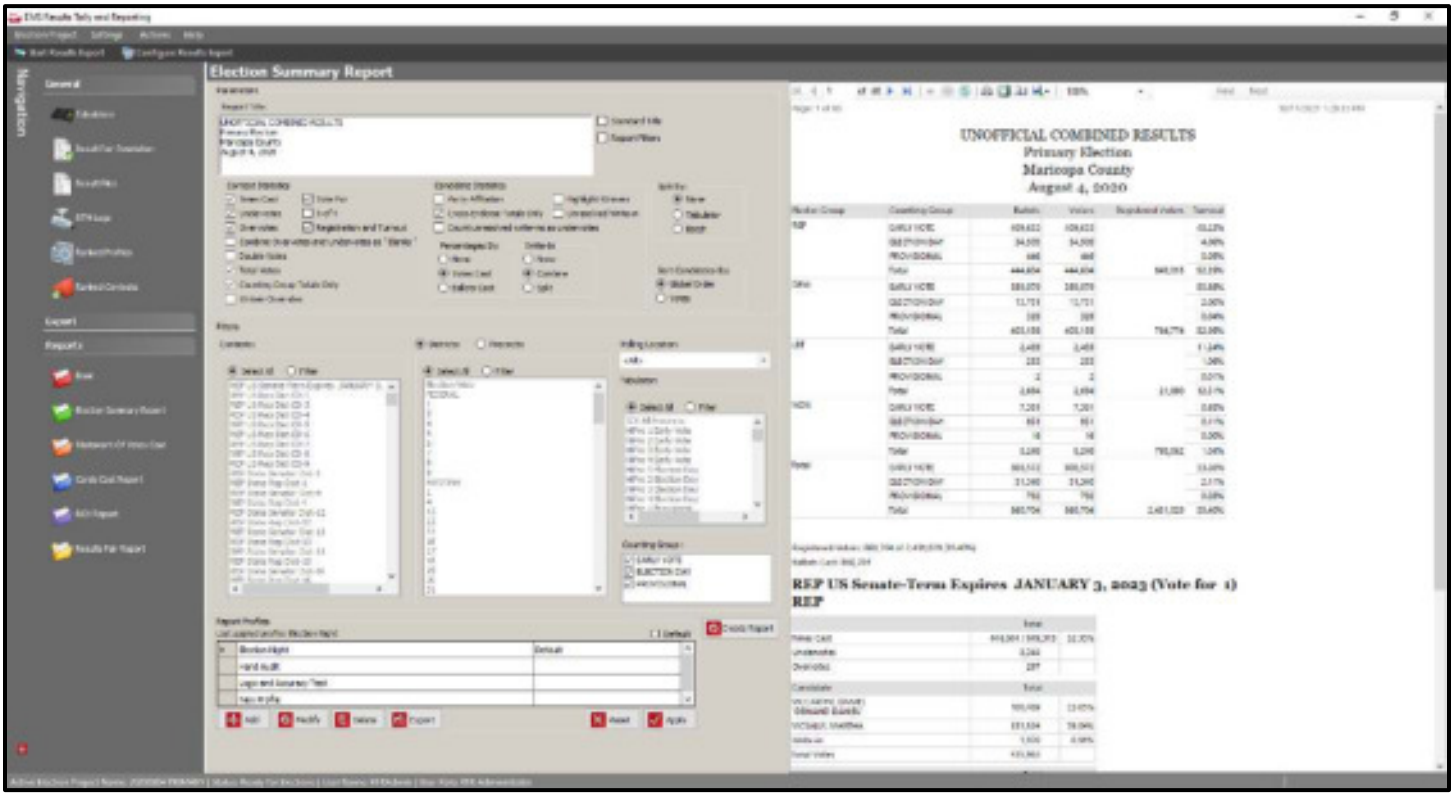
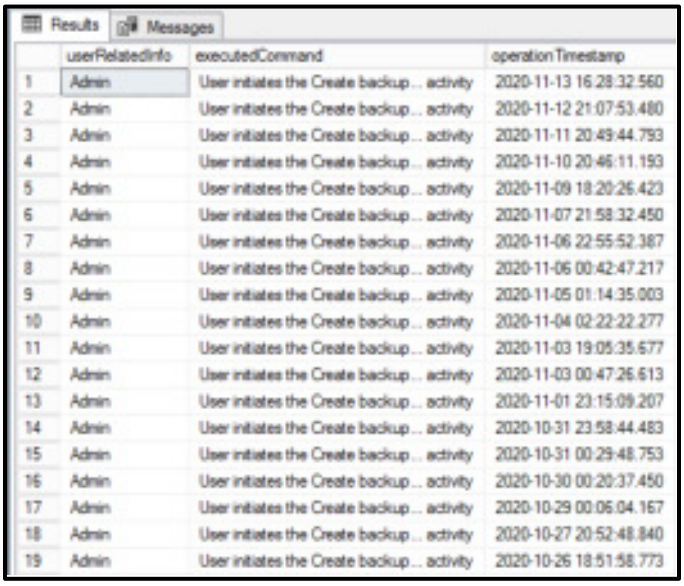


Figure 2 - All Results Still Exist for the 2020 Primary. These numbers match the Official Results.

Furthermore, the standard way to "archive" Dominion software is to run a backup from Election Event Designer. This method of backup is found with every past election, and it's the only way to create a zip archive with all of the database details and all of the items within the NAS directory. This operation does NOT delete any data. The last time a package file was created was on November 13th as can be seen in the screenshot of the RTR logs. This is inconsistent with the County's statement an archive was created on Feb 2nd.



Results | Messages

	userRelatedInfo	executedCommand	operationTimestamp
1	Admin	User initiates the Create backup... activity	2020-11-13 16:28:32.560
2	Admin	User initiates the Create backup... activity	2020-11-12 21:07:53.480
3	Admin	User initiates the Create backup... activity	2020-11-11 20:49:44.793
4	Admin	User initiates the Create backup... activity	2020-11-10 20:46:11.193
5	Admin	User initiates the Create backup... activity	2020-11-09 18:20:26.423
6	Admin	User initiates the Create backup... activity	2020-11-07 21:58:32.450
7	Admin	User initiates the Create backup... activity	2020-11-06 22:55:52.387
8	Admin	User initiates the Create backup... activity	2020-11-06 00:42:47.217
9	Admin	User initiates the Create backup... activity	2020-11-05 01:14:35.003
10	Admin	User initiates the Create backup... activity	2020-11-04 02:22:22.277
11	Admin	User initiates the Create backup... activity	2020-11-03 19:05:35.677
12	Admin	User initiates the Create backup... activity	2020-11-03 00:47:26.613
13	Admin	User initiates the Create backup... activity	2020-11-01 23:15:09.207
14	Admin	User initiates the Create backup... activity	2020-10-31 23:58:44.483
15	Admin	User initiates the Create backup... activity	2020-10-31 00:29:48.753
16	Admin	User initiates the Create backup... activity	2020-10-30 00:20:37.450
17	Admin	User initiates the Create backup... activity	2020-10-29 00:06:04.167
18	Admin	User initiates the Create backup... activity	2020-10-27 20:52:48.840
19	Admin	User initiates the Create backup... activity	2020-10-26 18:51:58.773

Figure 3 - The last time an archive was created of the 2020 General Election was on 11/13 at 4:28pm.

1.6.3 False County Claim: The County Ran Two Forensic Audits By Certified Companies

The procedures documented within the ProV&V report for the first Maricopa County audit did not follow any industry recognized standard digital forensic processes, and the SLI report clearly documents that they could not forensically image the EMS Server due to the RAID configuration. This is consistent with the fact that neither company is certified for forensic examination of digital equipment, and this is not work either company regularly does. Both companies are certified by the Election Assistance Commission for certifying election equipment, not for completing forensic audits.

Furthermore, since all election results were cleared from the Election Management System (EMS) Server before any of these two audits were performed; the only thing these companies could do was run test cases against the election equipment to see if it behaved properly. No results were audited by either of these two companies.

1.6.4 Misleading County Claim: The County Ran A Hand Count

The hand count done by Maricopa County was such a small sample size that its margin of error was more than twice the amount of the margin of victory. It is extremely misleading to suggest this is equivalent or just as accurate as a full hand count. The hand count only counted 5,200 of the 2,089,563 ballots. This equates to roughly 1/4th of a percentage point of the total ballots. With this small sample size there would be a 1.357% margin of error to achieve a 95% confidence in the election results. This means that if the ballots were truly chosen randomly, then this hand count could be off by over 28,000 ballots. If the ballots were not chosen randomly then the counts could be off by even more.

1.7 Corrupt and Missing Ballot Images

The County claims that the fact that the ballot images are corrupt or missing from the Election Management System (EMS) Server is inconsequential, and that ballot images should have been viewed from one of the other drives provided. This defies normal audit principles where the official system of record, the EMS Server, would be utilized for the analysis. This also doesn't explain why or how the images got corrupt, or why images are missing from that system. The drive provided wasn't even in the same folder structure as the NAS directory or have any other resemblance of an official backup. For this drive to be considered as the official source of images would require that there is some documented procedure for the collection of these images.

Furthermore, a review of the drive provided doesn't include all pre-adjudicated images. The post-adjudicated images on the drive show the expected 2,089,563 images, but the pre-adjudicated images only show 1,923,719 images. The difference of 165,844 appears to be the number of ballots processed by the Election Day ImageCast Precinct 2 tabulators based on the CVR, but it's unclear why or how these images would be collected in a manner where these images were missing. As a result, it creates further questions on the reliability of these images.

At this time, the drive of pre- and post-adjudicated images has not been validated to confirm that corrupt images do not exist, but this aspect will be reviewed and be confirmed.

1.8 Subpoenaed Equipment Not Provided

The County can't both state that the matter of missing subpoena items was resolved in the settlement, and then proceed to argue that certain items were not in the subpoena. Furthermore, failing to comply with a subpoena is a criminal offense and not something that can be included in a civil settlement. It will be up to the Attorney General to determine if the missing subpoena items are a sufficient grievance to merit further investigation or prosecution. This is not something that is within the Senate's responsibilities.

The actual report has a more extensive list of items that were missing from the subpoena, not all of which are addressed within the County's reply. However, to address the specific items listed in the County's reply:

- **Poll Worker Laptops / Sitebook Voter Roll Check-In Devices**
    - Item #11 on the original subpoena[5] states, "forensic image of computers/devices used to work with voter rolls". This was not provided.
- **Backup Dominion EMS Server**
    - The county states that the Backup Dominion EMS Server was not in use. Logs show regular backups conducted of the election database throughout the election. Normal practices would dictate that these would periodically be loaded onto a backup server to confirm the backups integrity. By definition, this is how a backup server is used and it was part of the election.
    - Item #3 on the original subpoena[6] states, "For the November 2020 general election in Maricopa County, Arizona", "Hardware and Forensic Images of Election Servers…". The backup EMS Server was not provided.
- **Ballot-on-Demand Printers & Accessible Voting Devices (ICX)**

[5] https://www.scribd.com/document/531671852/SUBPOENA-January-12-2021-NEW-Senate-Sub-to-Maricopa-County
[6] https://www.scribd.com/document/531671852/SUBPOENA-January-12-2021-NEW-Senate-Sub-to-Maricopa-County

- Item #1 of the original subpoena[7] states "The ballot tabulation and processing equipment from each polling place and tabulation center".
  - Based on the sentence "processing equipment" that is different than "ballot tabulation". It's unclear what else this could be referring to besides Ballot-on-Demand Printers and accessibility Ballot Marking Devices since those are the only other devices that process ballots at a polling location.
- Item #10 of the original subpoena[8] states "Election Systems and Software", "Ballot on Demand – BOD printing system":

1.9 Internet Connections & Cyber Security practices

The County continues to repeat the claims that there was no way any of the systems could access the internet, to abdicate all responsibility to other parties for the County's failure to properly maintain the security of election systems, and to purposely misdirect on all other legitimate findings of the audit. As usual, the County fails to cite a single piece of evidence to support their opinion.

1.9.1 Internet Connectivity

The County's response does not state that the systems were never connected to the internet; but always seems to address this issue in the present tense indicating that the election system is not currently connected to the internet; and then cite the two "forensic audits" conducted by the County that proved at the time of their "audits" there was no evidence of internet activity. CyFIR's analysis never stated that the systems were always connected to the internet, but simply stated that there are distinct periods of time where internet connectivity can be validated. As a result, while on the surface it looks like the County is countering the claims in the audit report; in fact, their response appears to be a misdirection.

CyFIR utilized a tool called HstEx v4 from Digital Detective to review the hard drives of all the affected systems for artifacts of internet activity. This tool both looks at the allocated space, which is the normal file structure you see on a system, and the unallocated space, which is what shows up on your system as "free space". When you delete a file on your file system the space that file occupied is shown in the computer as "free space"; but the file itself is still fully intact on the file system until the computer puts some other file in the space occupied prior by that file. In this way the tool looks at both normal files and deleted files.

HstEX v4 identified and extracted all internet history into a .hstx file that was analyzed using the Digital Detective NetAnalysis v2 tool. In addition to the URL that was navigated to, this data includes a visits column. Per the tool documentation[9] and basic forensic analysis, the visits field is ONLY populated when a URL is actually visited and does not populate when a web page cannot be resolved. This visits column can be seen in all of the following screenshots of the tool output, and clearly refutes the claim that the machines never had a pathway to the internet.

[7] https://www.scribd.com/document/531671852/SUBPOENA-January-12-2021-NEW-Senate-Sub-to-Maricopa-County
[8] https://www.scribd.com/document/531671852/SUBPOENA-January-12-2021-NEW-Senate-Sub-to-Maricopa-County
[9] https://www.digital-detective.net/Documents/NetAnalysis%20v2%20User%20Guide.pdf

1.9.1.1 EMS Server Connections

On 2 February 2021 the EMS Server connected to the az700632.vo.msecnd.net web site three times.

Date Visited [UTC]	Date Visited [Local]	Visits	URL
2021-02-02 00:17:30.906	2021-02-01 17:17:30.906	1	https://az700632.vo.msecnd.net/pub/ExtMgr/CompatList/CompatibilityList.xml.errormarker
2021-02-02 00:17:33.935	2021-02-01 17:17:33.935	2	https://az700632.vo.msecnd.net/pub/ExtMgr/CompatList/CompatibilityList.xml.errormarker

Figure 4 - EMS Internet Connections

1.9.1.1 EMS Client 1 Connections

The EMS Client 1 connected to three different sites a total of 9 separate times after the installation of the Dominion software. Figure 5 – EMS Client 1 Connections details these connections.

Date Visited [UTC]	Date Visited [Local]	Visits	URL	User
02/07/2020 20:02:19	02/07/2020 13:02:19	2	http://www.bing.com/search?q=192.168.100.11&src=IE-SearchBox&FORM=IE11SR&pc=EUPP_	
02/22/2021 23:08:13	02/22/2021 16:08:13	5	https://go.microsoft.com/fwlink/?LinkId=838604	emsadmin01
02/07/2020 20:00:53	02/07/2020 13:00:53	2	https://go.microsoft.com/fwlink/p/?LinkId=255141	emsadmin01

Figure 5 - EMS Client 1 Connections

1.9.1.2 EMS Client 3 Connections

The EMS Client 3 connected to the go.microsoft.com web site 6 times after the installation of the Dominion software. Figure 6 – EMS Client 3 Connections details these connections.

Date Visited [UTC]	Date Visited [Local]	Visits	URL	User
08/06/2019 16:26:03	08/06/2019 09:26:03	2	http://192.168.100.11/portal_top.html	emsadmin01
08/06/2019 16:26:01	08/06/2019 09:26:01	2	http://192.168.100.11/	emsadmin01
08/06/2019 16:26:03	08/06/2019 09:26:03	2	http://192.168.100.11/portal_top.html	emsadmin01
08/06/2019 16:26:03	08/06/2019 09:26:03	2	http://192.168.100.11/portal_top.html	emsadmin01
08/06/2019 16:26:01	08/06/2019 09:26:01	2	http://192.168.100.11/	emsadmin01
08/06/2019 16:26:13	08/06/2019 09:26:13	3	http://192.168.100.11/	emsadmin01
08/06/2019 16:26:27	08/06/2019 09:26:27	3	http://192.168.100.11/checkLogin.cgi	emsadmin01
08/06/2019 16:26:27	08/06/2019 09:26:27	3	http://192.168.100.11/portal_top.html	emsadmin01
02/04/2021 00:36:19	02/03/2021 17:36:19	6	https://go.microsoft.com/fwlink/?LinkId=838604	emsadmin03

Figure 6 - EMS Client 3 Connections

1.9.1.3 REWEB1601 and REGIS1202 Connections

The Maricopa County Board of Supervisors represented to the public and to the auditors that none of the election systems were connected to the internet. The Maricopa Board of Supervisors did not provide any qualifying statements to the auditors at the time of equipment delivery, nor did they provide a network diagram explaining that the REWEB1601 and the REGIS1202 servers were connected to the internet. The auditors subsequently took the Maricopa Board of Supervisors at their stated word and reported the internet connections to each of these servers to the Arizona Senate. The auditors appreciate the Maricopa County Board of Supervisors admission that these two servers were indeed connected to the internet. The Maricopa County Board of Supervisors stated that two federally certified Voting System Testing Laboratories independently reported that the systems were not connected to the internet. It is not uncommon for firms to miss internet artifacts that may exist in the unallocated and allocated space of a system.

1.9.2 Software and Patch Management

The County's neglect of the software, patch management, and virus scan updates violates all solid principles of Cyber Security and demonstrates a negligence in protecting the integrity of voting system. Their attempts to blame the Election Assistance Commission (EAC) is disingenuous at best and simply demonstrates they're failure to take responsibility and control of their election systems, and instead attempting to delegate all responsibility to the voting machine vendor.

The EAC clearly has a process for "de minimis changes"[10] to account for Operating System level patches and changes to trusted builds, and advocates those critical patches be applied[11]. This advice is further enforced by the Cybersecurity & Infrastructure Security Agency[12] (CISA), and the Center for Internet Security[13] (CIS). Nowhere in any documentation is there any indication that virus scans update would somehow negate the certification, yet those were also not applied.

The fact that the County failed to recognize the risk of having out-of-date software and never requested the voting machine vendor to go through the simple process to get patches approved, as is required by the "Warranty" section of the County's contract[14], nor did they choose to move to a later version of the voting system software that has later approved patches; does not somehow make their system secure. The County failed to implement basic Cybersecurity hygiene. This should be acknowledged, and policies put in place to make sure this never happens again.

1.9.3 Credential Management

The County's response related to credential management is beyond misleading and goes into the realm out outright lies. They state, "To access each tabulator, an operator needs a series of two passwords and a security token (key). Passwords used to access the election program and to tabulate ballots are changed prior to each election." This statement only applies to the ImageCast Precinct 2 (ICP2) tabulators which were ONLY used on election day and doesn't apply to ballots tabulated on the HiPro or the ImageCast Precinct devices. To give perspective, the ICP2 only accounted for 7.9% of the vote, while the other tabulators accounted for 92.1% of the vote. The devices that tabulated 92.1% of the vote, as well as the systems utilized to generate the output for the official certified results; were where the problems outlined within the audit report were found.

To be more specific, the credential management finding is specific to the username and passwords required to access the EMS server, the EMS workstations, the Adjudication workstations, the HiPro scanners and the ImageCast (ICC) Workstations. Accessing these systems did not require anything but a typical computer username and password combination. The usernames/accounts of these systems were not assigned to specific individuals, but rather were shared between various people. The passwords for these accounts were created during the installation of the Dominion software on 8/6/2019 and were never changed up to the point where these systems were delivered for the audit. Furthermore, in complete disregard to all standard security practices, the same password was used for ALL user accounts on ALL of the EMS, EMS Client, ICC, HiPro, and Adjudication systems. To be clear, if someone knew the password to a single user account on one of these systems that individual would know the password to the admin account on any of these systems.

[10] https://www.eac.gov/sites/default/files/voting_equipment/NOC19.01_SoftwareDeMinimisChanges_11-15-2019.pdf
[11] https://www.eac.gov/windows-critical-update-faq
[12] https://us-cert.cisa.gov/ncas/tips/ST19-002
[13] https://www.cisecurity.org/spotlight/ei-isac-cybersecurity-spotlight-patching/
[14] https://www.scribd.com/document/533751776/Maricopa-County-Elections-Tabulation-System-Contract (Page 34)

1.9.4 Log Management

The Maricopa County Board of Supervisors stated the following in response to the Audit report concerning the County's failure to preserve the operating logs on the EMS server "The system automatically logs all actions taken on the equipment. These logs are configured according to factory settings and have a storage limit of 20 megabytes." This statement ignores the crux of the finding.

1.9.4.1 Failure to Properly Retain Logged Data

Maricopa county had full administrative authorities over the configuration and maintenance of the logging functions and the log retention duration operations. To claim that the reason the log data was not retained because the log size default setting was only 20MB is disingenuous at best when the county had the full control to properly modify this setting to ensure that the logged data was properly retained. The retention period for these log artifacts should have been for twenty-two (22) months but wasn't.

1.9.4.2 Intentional Execution of Scripts to Deliberately Ensure that Log Entries Were not Retained

The response by Maricopa County does not address the fact that a user leveraging the emsadmin account deliberately and purposely executed a script that checked the accounts for duplicate passwords 38,478 times. This deliberate execution of the script occurred over three days, specifically on 2/11/2021 there were 462 log entries overwritten, on 3/3/2021 there were 37,686 log entries overwritten, and on 4/12/2021 there were 330 log entries overwritten. Given that the Maricopa County knew that the setting on the log retention was limited to 20MB, the act of executing these scripts had the effect of deliberated ensuring that the Windows security logs covering the dates of the general election would not be available for review.