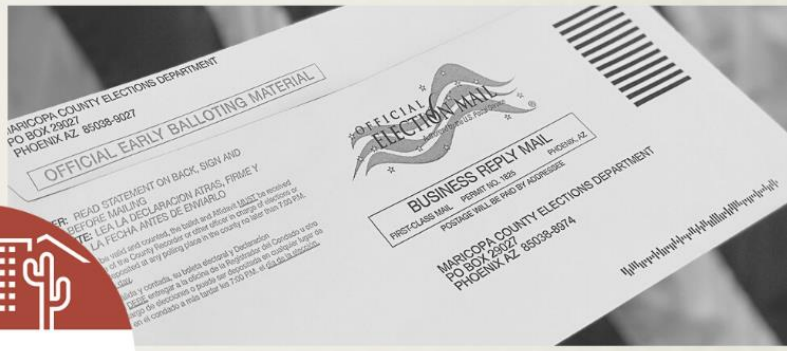
MARICOPA COUNTY ELECTIONS DEPARTMENT

JANUARY 2022

CORRECTING THE RECORD

Maricopa County's In-Depth Analysis of the Senate Inquiry



I VOTED
Maricopa County Recorder & Elections Department

PREPARED BY

MARICOPA COUNTY ELECTIONS DEPARTMENT
& OFFICE OF THE RECORDER

Executive Summary

Maricopa County is the second largest voting jurisdiction in the United States. With more than 2.6 million registered voters, Maricopa County represents more than 60 percent of Arizona's registered voters. The Elections Department reports to both the County Board of Supervisors and the County Recorder and administers city, town, school district, special district, county, state, and federal elections in Maricopa County.

Transparency, accuracy, and accountability are paramount to Maricopa County and its Elections Department. Maricopa County's election staff are trained and Certified Election Officers with knowledge of state and federal election laws and the Arizona Election Procedures Manual. Our role as election administrators is guided by statute and our team follows those laws and procedures so that every eligible vote is counted.

> **The November 2020 General Election was administered with integrity and the results were accurate and reliable. This has been proven through statutorily required accuracy tests, court cases, hand counts performed by the political parties, and post-election audits. The Elections Department followed all federal and state election laws.**

On November 23, 2020, Maricopa County delivered the November General Election certified canvass results to the Arizona Secretary of State. The Elections Department stands by these certified results.

Many allegations about the November 2020 General Election made their way to court and Maricopa County clearly presented the facts to judges at both the state and federal level. Fourteen different times complaints alleged election fraud, manipulation, or tampering in Maricopa County's 2020 General Election. No claim succeeded. For a complete listing of all court cases, see *Exhibit – COURT CASES*.

The County welcomes objective and unbiased scrutiny and reviews of its elections processes. Following the August 2018 Primary Election, the Maricopa County Board of Supervisors enlisted both the County's internal audit department and an external auditing company to conduct a review of the County's election processes. Those professional, non-partisan reviews yielded many positive changes to the County's elections.

After the November 2020 General Election, the County hired two federally certified Voting System Test Laboratories to conduct an audit of the tabulation equipment used to count ballots for all five of the elections administered in 2020. Both certified laboratories found no anomalies in the tabulation equipment and confirmed that:

- All tested software, systems, and equipment were using certified software
- No malicious malware or hardware was installed
- No evidence of internet connectivity was found
- The 2020 General Election program and tabulation equipment was accurate (test completed by only one Voting System Test Laboratory)

Despite all evidence to the contrary, false allegations continue to persist and damage voter confidence. Many falsehoods have been perpetuated through the Senate's review of Maricopa County's ballots, equipment and data, which were subpoenaed by Arizona Senate President Karen Fann and Senate Judiciary Committee Chairman Warren Petersen.

Maricopa County worked in good faith to comply with the subpoenas, while the Senate hired partisan contractors with no election experience.

Throughout the review, the Senate's contractors released inaccurate and misleading information, in some instances during presentations delivered to Senators Fann and Petersen. The Senate's review culminated in a series of inaccurate reports and presentations delivered by its contractors on September 24, 2021, which called into question the integrity of Maricopa County employees and the validity of legitimate votes cast by eligible voters.

This continuous release of inaccurate information required the County to develop a website to combat misinformation: JustTheFacts.Vote.

This report, prepared by election professionals, was commissioned by the Board of Supervisors and the County Recorder, who directed the Elections Department to conduct a thorough review of the claims and voter appendices contained in Cyber Ninjas Volume III report (Pgs. 1-61), CyFIR's presentation and findings included in Cyber Ninjas Volume III (Pgs. 61-97), EchoMail's envelope images presentation and report (Pgs. 1-99) and the Senate's Machine Paper Ballot Count Report (Pgs. 1-36).

Summary of Maricopa County's Findings

After an in-depth analysis and review of the reports and presentations issued by the Senate's contractors, we determined that nearly every finding included faulty analysis, inaccurate claims, misleading conclusions, and a lack of understanding of federal and state election laws. Our review of the claims made by Cyber Ninjas, CyFIR, EchoMail, and the Senate's Audit Liaisons, found:

- 22 were misleading. The claims lead the reader to assume a conclusion that is not supported by the evidence.
- 41 were inaccurate. The claims include flawed or misstated analysis.
- 13 were false. The claims are demonstrably false and can be proven false using materials provided to the Senate.

Cyber Ninjas

The report produced by Senate contractor, Cyber Ninjas, inaccurately challenges the legitimacy of thousands of voters who participated in the November 2020 General Election and/or the validity of ballots counted and included in the official results. The Elections Department reviewed every finding included in Cyber Ninjas' Volume III report.

Our analysis found that Cyber Ninjas made faulty and inaccurate conclusions about more than 53,000 ballots in 22 different categories.

As shown in *EXEC Table #1* on the next page, Maricopa County election professionals found seven false claims, 23 inaccurate claims, and nine misleading claims made in Cyber Ninjas Volume III report. This includes faulty conclusions about voters who moved, early voting files, certified results, voter registration information, the County's ballot duplication processes, and ballots for military and overseas voters. At the heart of these inaccuracies is a basic misunderstanding or ignorance of election laws and procedures.

EXEC Table #1 – Summary of Maricopa County's Analysis of Cyber Ninjas' Findings					
Category		**Cyber Ninjas Volume III Report & Senate Machine Count Report (MCR)**			**County Response**
Topic	Page	Claim	Reference	Ballots	Analysis
Subpoena, Hand Count and Paper					
Audit Cooperation & Subpoenaed Items	9	Audit Interference	5.7.1 (pg. 48)	n/a	Misleading Claim
		Missing Subpoena Items	5.7.8 (pg. 56)	n/a	Misleading Claim
		Subpoenaed Equipment Not Yet Provided	6.5.3 (pg.78)	n/a	Misleading Claim
		Voter Registration System Audit Access	5.7.12 (Pg. 60)	n/a	Misleading Claim
Hand Count & Machine Count	13	Tally Results, Presidential & Senate Races	4-4.3 (pg. 2)	n/a	3 Misleading Claims
		Machine Count	MCR (pg. 4)	n/a	Misleading Claim
Paper and Printer Claims	17	High Bleed-Through Rates on Ballots	5.7.5 (pg. 52)	n/a	False Claim
		Improper Paper Utilized	5.7.6 (pg. 54)	n/a	False Claim
		Out of Calibration Ballot Printers	5.7.10 (pg. 57)	n/a	False Claim
		Questionable Ballots	5.7.13 (pg. 61)	n/a	False Claim
Voter Registration					
Voters that Moved & Soft Matching Techniques	51	Mail-in Ballot Voted from Prior Address	5.3.1 (pg. 6)	23,344	0
		Potentially Voted in Multiple Counties	5.4.2 (pg. 10)	5,295	5
		In-Person Voters Moved out of County	5.5.3 (pg. 14)	2,382	0
		Voters Moved Out-of-State Prior to Election	5.5.4 (pg. 16)	2,081	0
		No Record of Voters in Commercial Database	5.7.9 (pg. 56)	N/A	Inaccurate Claim
Other Voter Registration Claims	58	Voters with Incomplete Names	5.6.5 (pg. 27)	393	0
		Deceased Voters	5.6.6 (pg. 29)	298	26
		Late Registered Voters with Counted Votes	5.6.8 (pg. 32)	198	0
		Duplicate Voter IDs	5.6.10 (pg. 37)	186	6
		Multiple Voters linked by AFFSEQ	5.6.11(pg. 38)	101	0
Protected Voters, Early and Damaged Ballots, and UOCAVA Voters					
Protected Voter Claims	63	Official Results Do Not Match Who Votes	5.5.1 (pg. 12)	3,432	0
		Votes Counted in Excess of Voters Who Voted	5.5.5 (pg. 18)	1,551	0
Early Ballot Returns and Real-Time Check-in System	65	More Early Ballots Returned than Received	5.4.1 (pg. 8)	9,041	0
		Ballots Returned not in the final Voted File	5.6.3 (pg. 24)	430	0
		Mail-in Ballot Received Without Sent Record	5.6.4 (pg. 25)	397	0
		Early Votes Not Accounted For in EV33	5.7.4 (pg. 51)	n/a	False Claim
		Real-Time Provisional Ballots	5.7.11 (pg. 59)	n/a	Misleading Claim
		Voters not in precinct register	5.6.1 (pg. 20)	681	0
		Date of Registration Changes to Earlier Date	5.6.9 (pg. 34)	193	0
Damaged and Duplicated Ballots	81	More Duplicates than Original Ballots	5.5.2 (pg. 13)	2,592	0
		Duplicated Ballots & Missing Serial Numbers	5.6.2 (pg. 22)	~500	0
		Duplicate Ballots Reuse Serial Numbers	5.6.14 (pg. 47)	6	0
		Commingled Damaged and Original Ballots	5.7.3 (pg. 50)	n/a	Inaccurate Claim
Ballots and Batch Discrepancies	86	Double Scanned & Counted Ballots	5.6.12 (pg. 45)	50	50
		Batch Discrepancies	5.7.2 (pg. 48)	n/a	False Claim
UOCAVA Claims	88	UOCAVA Count Does Not Match the EAC	5.6.7 (pg. 30)	226	0
		UOCAVA Electronic Ballots Double Counted	5.6.13 (pg.46)	6	0
		Inaccurate Identification of UOCAVA ballots	5.7.7 (pg. 55)	N/A	False Claim
			Ballots Total	53,304	87
			Total Claims	40	7 False
					23 Inaccurate[1]
					9 Misleading

[1]*Maricopa County found that 21 of the 22 ballot claims were inaccurate. While Cyber Ninjas section 5.6.12 was included in the total claims (39), it was not assigned a category. For more information see page 86.*

Our analysis found 37 instances where a voter *may* have unlawfully cast multiple ballots. We have forwarded these instances to the Arizona Attorney General's Office for further investigation. We also found 50 instances in which a ballot was potentially double counted.

> **In total, we found fewer than 100 potentially questionable ballots cast out of 2.1 million. This is the very definition of exceptionally rare. None of these instances impacted the outcome of races and a thorough review by our election professionals confirmed there were no systemic issues related to ballot counting and processing in the November 2020 General Election.**

Additional analysis conducted by the County examined Cyber Ninjas' hand count of 2.1 million paper ballots. In their September 24 presentation to Senators Fann and Petersen, Cyber Ninjas reported that its hand count and the Senate's machine count largely matched Maricopa County's official canvass. While the County's official canvass and the Senate's machine count are almost identical, an analysis of hand count reports and procedures (see pg. 13) reveal discrepancies that call Cyber Ninjas' official numbers into question.

CyFIR

The Senate's contractor, CyFIR, reviewed Maricopa County's federally and state certified tabulation equipment and Election Management System (EMS).

> **There is not a single accurate claim contained in CyFIR's analysis of Maricopa County's tabulation equipment and EMS. This includes the allegation that county staff intentionally deleted election files and logs, which is not true.**

CyFIR looked for ballot images in the wrong areas and then wrongly assumed that the images were corrupt. CyFIR also aired inaccurate claims about routers being connected to the EMS and incorrectly concluded that the tabulation equipment was connected to the internet, leading to additional inaccurate or misleading claims about County cybersecurity measures. In its September 24, 2021 presentation, CyFIR accused County staff of intentionally deleting files and logs. That is not true. All 2020 General Election files have been preserved and archived. The County created 26 daily back-ups of the EMS server during the election, with the last one occurring after tabulation was completed on November 13, 2020.

> **All the backup hard drives and corresponding data files from the November 2020 General Election have been maintained and safely secured. Contrary to claims made by the Senate and its contractors, the Arizona Senate did not subpoena these archived files.**

These inaccurate and misleading claims continue to spread. This report goes into further detail about each claim. A summary of the County's analysis of CyFIR's claims is included in the *EXEC Table #2* below.

EXEC Table #2 – Summary of Maricopa County's Analysis of CyFIR's Findings					
Category		**Cyber Ninjas Volume III Report**			**County Response**
Topic	Page	Claim	Reference	Ballots	Analysis
Tabulation Equipment & Technology					
Election Management System Database and Files	21	EMS Database Purged	6.4.1 (Pg. 63)	n/a	Inaccurate Claim
		Election Files Deleted	6.4.2 (Pg. 65)	n/a	Inaccurate Claim
		EMS C:\ Drive	6.4.2.1.1 (Pg. 66)	n/a	Inaccurate Claim
		EMS D:\ Drive	6.4.2.1.2 (Pg. 67)	n/a	Inaccurate Claim
			6.4.2.1.2 (Pg. 67)	n/a	Inaccurate Claim
		Deleted Files & Directories	6.4.2.1.3 (Pg. 68)	n/a	Inaccurate Claim
		HiPro 1, HiPro 3, HiPro 4	6.4.2.1.4 (Pg. 69)	n/a	Inaccurate Claim
			6.4.2.1.5 (Pg. 69)	n/a	Inaccurate Claim
		Corrupt Ballot Images	6.4.3 (Pg. 70)	n/a	Inaccurate Claim
		Missing Ballot Images on EMS Server	6.5.1 (Pg. 73)	n/a	Inaccurate Claim
Operating System Logs	25	EMS Logs Not Preserved	6.5.6 (Pg. 85)	n/a	Inaccurate Claim
		User Log Deletions on 02/11/2021	6.5.6.1.1 (Pg. 86)	n/a	Inaccurate Claim
		User Log Deletions on 03/03/2021	6.5.6.1.2 (Pg. 86)	n/a	Inaccurate Claim
		User Log Deletions on 04/12/2021	6.5.6.1.3 (Pg. 87)	n/a	Inaccurate Claim
		Anonymous Logins	6.5.4 (Pg. 82)	n/a	False Claim
Election Management System & its Air Gapped Network	34	Internet Connections	7.5.5 (Pg. 89)	n/a	False Claim
		Internet Connections to the EMS	6.5.6.2 (Pg. 89)	n/a	False Claim
		Internet Connections to Client 1	6.5.6.3 (Pg. 89)	n/a	False Claim
		Internet Connections to Client 3	6.5.6.4 (Pg. 90)	n/a	False Claim
		Internet Connections to the REWEB	6.5.6.5 (Pg. 90)	n/a	Misleading Claim
		Internet Connections to the REGIS	6.5.6.6 (Pg. 91)	n/a	Misleading Claim
Hard Drives and Other Data	43	Dual Boot System Discovered	6.5.5 (Pg. 84)	n/a	Misleading Claim
		Election Data Found From Other States	7.6.1 (pg. 92)	n/a	Inaccurate Claim
Cybersecurity Best Practices	45	Failure to Follow Basic Cybersecurity	6.5.2 (Pg. 75)	n/a	Misleading Claim
		Software and Patch Management	6.5.2.1.1 (Pg 75)	n/a	Misleading Claim
		Credential Management	6.5.2.1.3 (Pg. 76)	n/a	Misleading Claim
		Lack of Baseline for Host and Network Activity	6.5.2.1.4 (Pg. 78)	n/a	Misleading Claim
			Total Claims	27	5 False
					15 Inaccurate
					7 Misleading

EchoMail

Senate contractor, EchoMail, reviewed the 1.9 million early ballot affidavit images from the November 2020 General Election.

> **EchoMail's analysis of the early ballot affidavit images is misleading at best. The "anomalies" EchoMail uncovered are due to a flawed understanding of signature verification laws and practices.**

EchoMail's analysis did not consider the signature curing process, which is when a voter corrects a signature issue by contacting the Elections Department. The thousands of "duplicate" early ballot envelope images that EchoMail claimed were "anomalies" have a simple answer. As voters cure signature issues, the Elections Department takes another image of the envelope. Only one ballot was counted for each envelope. In addition, EchoMail's findings included misleading claims about the County's signature verification process, which has been proven accurate in Court. EchoMail also fails to understand Arizona's elections laws related to the processing of early ballot affidavits, signature review and verification, and rights of voters to cure their signature. A summary of the County analysis of EchoMail's conclusions is included in the following *EXEC Table #3*.

EXEC Table #3 – Summary of Maricopa County's Analysis of EchoMail's findings

Category		EchoMail Report			County Response
Topic	Page	Claim	Reference	Envelopes	Analysis
Early Ballot Envelope Images	74	Canvass Requirements	Pg. 14	n/a	False Claim
	75	17,126 "Duplicate" Early Ballot Images		17,126	Misleading Claim
	75	More Envelopes Processed & Submitted than Identified by EchoMail		6,545	Misleading Claim
	76	No Signatures, Scribbles & Bad Signature Rates	Pg. 14-15	2,580	Inaccurate Claim
				9,589	Inaccurate Claim
	78	Increase in Envelopes but Decrease in Signature Rejections	Pg. 15	n/a	Inaccurate Claim
	78	Daily Duplicate Numbers	Pg. 74-75	7,797	Misleading Claim
	78	Stamped in Signature Region	Pg. 79	n/a	Misleading Claim
	79	Stamp Behind the Envelope Triangle	Pg. 84	n/a	Misleading Claim
	80	Two-Different Voter IDs	Pg. 85-86	n/a	Misleading Claim
				10	6 Misleading
					3 Inaccurate
					1 False

Post-election audits build trust and promote election integrity when they have bipartisan oversight and are conducted by experienced, unbiased professionals who use well-defined, proven processes to provide quantifiable, reproducible proof. These audits can also identify and explain any inconsistencies that arise so processes may be improved, or new laws may be considered.

Unfortunately, the Senate's election review and its contractors fell far short of those standards and instead promoted disinformation and distrust. This report details those shortcomings and corrects the record.

TABLE OF CONTENTS

Item #1: Audit Cooperation and Subpoenaed Items 9
Item #2: Cyber Ninjas Hand Count and Senate Machine Count 13
Item #3: Paper and Printer Claims 17
Item #4: Election Management System Database and Files 21
Item #5: Operating System Logs 25
Item #6: Election Management System & Its Air Gapped Network 36
Item #7: Hard Drives and Other Data 45
Item #8: Cybersecurity Best Practices 47
Item #9: Voters that Moved & Soft Matching Techniques 53
Item #10: Other Voter Registration Claims 60
Item #11: Protected Voters 65
Item #12: Early Ballot Returns and Real-Time Check-in System 67
Item #13: Early Ballot Envelope Images 75
Item #14: Damaged and Duplicated Ballots 83
Item #15: Ballots and Batch Discrepancies 88
Item #16: UOCAVA Ballots 90

Item #1: Audit Cooperation and Subpoenaed Items

(Cyber Ninjas Volume III Report Sections – 5.7.1, 5.7.8, 6.5.3)

Cyber Ninjas' Volume III report included four misleading claims about the County's cooperation with their review.

Cyber Ninjas Volume III		County Analysis
Reference	Claim	
5.7.1 (pg. 48)	"Audit Interference"	Misleading Claim
5.7.8 (pg. 56)	"Missing Subpoena Items"	Misleading Claim
6.5.3 (pg.78)	"Subpoenaed Equipment Not Yet Provided"	Misleading Claim
5.7.12 (Pg. 60)	"Voter Registration System Audit Access"	Misleading Claim

Maricopa County Findings

Despite claims to the contrary, the County complied with the Senate's subpoenas. Within days of the issuance of the January 12, 2021 subpoena, the County had gathered and provided the Senate with thousands of documents and over eight terabytes of data (see *Exhibit – SUBPOENA TRACKING*). In addition to the documents, the Senate's subpoena commanded the Maricopa County Board of Supervisors' Chairman, County Recorder and County Treasurer to attend a public hearing at the Senate on January 13 at 9 a.m. (less than 18 hours after the issuance of the subpoena). When the elected officials arrived, the Senate did not have a hearing scheduled and they turned the County's elected officials away.

The County asked for judicial clarification on the lawfulness of producing paper ballots, ballot images and tabulation equipment from the November 2020 General Election to the Senate. After the Maricopa County Superior Court ruled that the law allowed the production and that the subpoena requests were valid, the County did *not* appeal the ruling, but instead asked Senate President Karen Fann when the County could deliver the almost 2.1 million ballots to the Senate's chambers as commanded by the subpoena. The Senate requested that the County keep the ballots until the Senate could find an alternative location for delivery. As later stipulated by the Senate, the County delivered the ballots, equipment and other data subpoenaed by the Senate to the Arizona Veterans Memorial Coliseum on April 21 and 22, 2021. These items included all the information the Senate needed to validate the 2020 General Election results. A second subpoena was issued on July 26, 2021. The County provided even more data in response.

On September 17, 2021, over eight months after the subpoenas were originally issued and before the issuance of Cyber Ninjas' report, the County and Senate negotiated an agreement to appoint a special master to review the County's router logs, and the Senate confirmed that the County was in *full compliance* with all issued subpoenas (see *Exhibit – SUBPEONA AGREEMENT*).

Summary

5.7.1 (Audit Interference), 5.7.8 (Missing Subpoena Items), 6.5.3 (Subpoenaed Equipment Not Yet Provided)

> **Based on the County's good faith efforts to comply with the subpoenas and deliver commanded items, the Senate was provided with all the information they would need to validate the 2020 General Election results.**

Response and Analysis

In section 5.7.1, Cyber Ninjas accused the County of interfering with its review by instructing one of the County's vendors not to cooperate. That did not happen. Rather, the County asked its vendor to tell Cyber Ninjas that it should submit any questions to the County, because the County was in the best position to provide accurate responses to questions about the election. No questions were submitted.

In sections 5.7.8 and 6.5.3, Cyber Ninjas list the items that they believe should have been provided in response to the Senate's subpoenas. See *SUBPOENAED ITEMS Table #1* for the County's response.

SUBPOENAED ITEMS Table #1 – Items Cyber Ninjas Claim Were Subpoenaed by the Senate		
Cyber Ninjas Volume III Report		County Response
Reference	Item	
5.7.8	"Rejected Provisional Ballots" "Uncured Mail Ballots" "Ballots returned to the County as undeliverable"	The Senate's January 12 subpoena requested "Access to all original, paper ballots including but not limited to early ballots, Election Day ballots, and Provisionals." The County provided access to all original paper ballots counted and included in the results for the November 2020 General Election. This included early, Election Day, and provisional ballots. The rejected provisional affidavits and the rejected early ballot affidavits, cast by those ineligible to vote, were not provided because the envelopes containing rejected early ballots are never opened and the rejected ballots are never counted. At no point prior to the issuance of Cyber Ninjas' report did the Senate or its contractors clarify that they wanted these items.
6.5.3.1.1	Routers / "Network Related Data"	While there are no routers that were ever connected to the County's tabulation equipment or Election Management System (EMS), the Senate continued to request the County's other network routers that support over 50 County departments, most of which have no relationship to the Elections Department (e.g., Sheriff's Office, Superior Court, Public Health). Providing these routers or access to the logs would have disrupted County operations, exposed the County network to significant security risks, and jeopardized law enforcement operations. As a result, the County and the Senate negotiated an arrangement that allows for the Senate to securely get answers to its questions about the routers. As part of that agreement, the Senate stipulated that it had found the County fully complied with the subpoenas. If the routers had been provided and spoiled by Cyber Ninjas, the estimated replacement cost would have been $6 million.
6.5.3.1.2	"Poll Worker Laptops"	The laptops in reference are the laptops connected to the printers the County uses at its voting locations. The Senate never requested these items in its subpoena. At no point prior to the issuance of Cyber Ninjas' report did the Senate or its contractors ask for these items. The replacement cost of these laptops and printers, with installed proprietary software is estimated at $9,000 per unit. If Cyber Ninjas spoiled this equipment as they did the tabulation equipment, this would cost County taxpayers another $3.2 million before taxes ($9,000 x 360 printers/laptops).

SUBPOENAED ITEMS Table #1 – Items Cyber Ninjas Claim Were Subpoenaed by the Senate		
Cyber Ninjas Volume III Report		County Response
Reference	Item	
6.5.3.1.3	"ICP Administrator Credentials and Hardware Tokens"	The County does not have possession or access to this information, because it is not needed by the County to conduct elections.
6.5.3.1.4	"IPX and Other Devices"	Cyber Ninjas listed an IPX device in its report. We do not have a piece of equipment called an "IPX," but we do have an ICX, which we call an accessible voting device. These machines are ballot marking tools used at voting locations for voters that need additional assistance marking their ballots. They do not perform tabulation functions and were not requested in the Senate's subpoena. At no point prior to the issuance of Cyber Ninjas' report did the Senate or its contractors ask for these items. If Cyber Ninjas spoiled this equipment as they did the tabulation equipment, this would cost County taxpayers another $50,000 before taxes ($300 x 175 accessible voting devices).
6.5.3.1.5	"Other Devices Connected to the Election Network"	The Senate subpoenaed tabulation equipment used during the November 2020 General Election. The other devices stated in this section of Cyber Ninjas' report are the back-up server and peripheral printers used to print reports. The backup server was not used during the November 2020 General Election. The peripheral printers are not tabulation equipment. The Senate did not request this equipment in its subpoena. At no point prior to the issuance of Cyber Ninjas' report did the Senate or its contractors ask for these items. If Cyber Ninjas spoiled this equipment as they did the tabulation equipment, this would cost County taxpayers another $6,900 before taxes.

Summary

5.7.12 (Voter Registration System Audit Access)

The County complied with the Senate's subpoenas, providing all servers that interface with the voter registration database, as well as the servers that support the website. There was no breach of the voter registration database. The unauthorized access to the public website was not a breach of the secure voter registration system.

Response and Analysis

Cyber Ninjas' report questions the security of Maricopa County's voter registration database, claiming on page 60 of the report that the "audit team has been denied access required to complete this portion of the audit." This is not true. The Senate was provided with all the servers that interface with the voter registration database. Additionally, the Senate was also provided with the servers that support the Recorder's Office and Elections Department website (see *Exhibit* -

SUBPOENA). Further, as stated above the County and Senate negotiated a settlement agreement, and the Senate confirmed that the County was in full compliance with all issued subpoenas.

The voter registration database is hosted on a separate network and is isolated from the Election Management System. It is also separate from the Elections Department's website. As standard practice, all development and use of the voter registration database and the Recorder's Office and Election Department website follows Open Web Application Security Project (OWASP) protocols. Many of these security controls and configurations are not public information to protect the security and integrity of the system. Below is a summary of what can be shared publicly.

- The voter registration database is only accessible by authorized systems and personnel. Multiple layers of authentication and security controls are in place to ensure the voter registration database is not accessed by bad actors. All development code is written and reviewed by quality assurance personnel for usability and security. It is also run through independent code security scan and verification services, which are remediated prior to going into production. The County has made substantial investments over the past decade in software, services and personnel in order to ensure the voter registration system delivers the citizens of Maricopa County best in class service.
- On the website, the Recorder's Office uses tiered security control configurations and services. While voters can securely access some pieces of their voter information through online portals, the website does not have access or authority to make changes to the voter registration database. These controls ensure automated attacks by bad actors on the website are discovered quickly and shut down. This is evidenced by a November 2020 incident when our Information Technology Security Department determined that an unauthorized person accessed publicly available information from a page on the Recorder's Office website. We secured the page and took immediate action to prevent this from happening in the future. This person never gained access to the voter registration database. Of the unauthorized data gathered, our team determined 859 of those individuals were protected voters (judges, law enforcement officers, survivors of domestic violence and other types of harassment or abuse). No sensitive personal information such as Social Security or Driver License numbers were obtained and none of the information identified the individuals as protected voters. This incident also had no impact on any ballot, or tabulation of ballots.

With these security measures, and the cooperation from multiple federal, state and county security operations partners, the County has not had a breach in security within the voter registration database. The unauthorized access to the website was not a breach of the voter registration system.

Item #2: Cyber Ninjas Hand Count and Senate Machine Count

(Cyber Ninjas Volume III Report Sections – 4, 4.1 & 4.3; Machine Paper Ballot Count Report)

Cyber Ninjas' report included three claims about the Maricopa County's certified election results based on the results of a hand count. The Senate also performed a machine count of the total number of ballots.

Cyber Ninjas Volume III and Senate Machine Count Report			County Analysis
Reference	Claim	Ballots	
4 (pg. 2)	"Tally Results"	N/A	*Misleading Claims:* While the Senate's machine count confirmed the accuracy of the County's tabulation equipment and certified results, the County's analysis of Cyber Ninjas' hand count reports and procedures revealed significant discrepancies.
4.1 (pg. 2)	"Presidential Race"	N/A	
4.3 (pg. 3)	"Senate Race"	N/A	
Machine Count Report (pg. 4)	"Machine Count"	N/A	

State & Federal Laws

A.R.S. § 16-602(B) describes the process for hand counts. The Arizona Elections Procedures Manual (pgs. 213-234) describe the legally allowed procedures for hand counts.

Maricopa County Findings

Maricopa County's tabulation equipment is reliable, accurate, and secure. This has been confirmed by ten separate statutorily required logic and accuracy tests, three separate hand counts performed by the political parties, and two audits completed by federally certified Voting System Test Laboratories.

Summary

On November 23, 2020, Maricopa County delivered the November General Election certified canvass results to the Arizona Secretary of State. The Maricopa County Elections Department stands by the certified results submitted to the County Board of Supervisors and transmitted to the Arizona Secretary of State. The accuracy, reliability, and trustworthiness of the processes used by Maricopa County and the results reported have been confirmed through statutorily required accuracy tests, hand counts, 14 court cases, and two separate independent contractor post-election audits.

Maricopa County 2020 Election – Certification, Accuracy Tests, Hand Counts, and Audits

Transparency, accuracy, and accountability are paramount to Maricopa County and its Elections Department. The County followed all statutorily required pre- and post-tests, audits and reviews of elections administered in 2020. The County also welcomes objective and unbiased scrutiny and reviews of its elections processes. Throughout the 2020 elections, political party observers were present at voting locations, followed ballot courier routes and observed signature verification, ballot processing and tabulation. In addition to strict physical security protocols including limited badge access, all rooms with ballots were monitored by surveillance cameras 24-7.

The following is summary of some of the statutory requirements and other steps taken to ensure the integrity of the tabulation processes used for the November 2020 General Election:

- In **December 2019**, after a competitive bidding process and pilot test during the November 2019 Jurisdictional Elections that confirmed the tabulator results with a 100% hand count, the County finalized a contract with Dominion Voting Systems to lease tabulation equipment. The Contract was awarded after Dominion obtained both federal and state certification. As part of the certification process, the equipment underwent extensive testing for reliability, accuracy, and security. Find the federal Certificate of Conformance for Dominion Voting Systems Democracy Suite 5.5-B here.
- On **October 6, 2020**, the Elections Department and the Arizona Secretary of State's Office performed a logic and accuracy test on the tabulation equipment in accordance with state law (A.R.S. § 16-449). The test date was published in the newspaper, open to the public and observed by political party representatives, city/town clerks, school and health care district representatives. The law requires an errorless count before tabulators and software can be used in an election. The tests confirmed the equipment was tabulating ballots accurately, paving the way for the November 2020 General Election.
- On **November 4, 2020**, a hand count audit of election results performed by Maricopa County political parties, to include the Republican, Democratic and Libertarian parties, found a 100% match to the vote tabulation equipment. The hand count audit, which is required by law, covered a statistically significant sample of ballots. The hand count was viewable on the Elections Department's website and the results were shared publicly. Two prior 2020 hand counts (March Presidential Preference Election and August Primary Election) performed by these same recognized political parties also found a 100% match between the tabulation equipment and the hand count results.
- On **November 18, 2020**, the Elections Department and the Arizona Secretary of State's Office performed a post-election logic and accuracy test on the equipment to ensure it was not changed or tampered with during the election. Members of all three political parties and a representative from the Arizona Attorney General's Office observed the test. Including the pre-election logic and accuracy tests, this was the tenth public test performed in 2020 that confirmed the accuracy of the tabulation system (a pre and post logic and accuracy test were performed for the March 2020 Jurisdictional Elections, March 2020 Presidential Preference Election, May 2020 Jurisdictional Election, August 2020 Primary Election, and November 2020 General Election).
- On **November 20, 2020**, the Board held a nearly three-hour public meeting to discuss concerns and questions raised by Maricopa County residents. Only after these questions were answered in a public forum did the Board certify the results of the election. The canvassing of the November 2020 General Election was completed in accordance with state laws (A.R.S. §§ 16-642 (A)(B), 16-643, 16-646). This meeting was broadcast live and is still available to the public.
- On **February 24, 2021**, the Board held a public meeting to review the results of two post-election audits that were completed by U.S. Election Assistance Commission certified Voting System Test Laboratories (VSTL). The audits found the equipment and software were the unaltered certified versions, no malicious hardware or software were detected, no evidence of internet connectivity was identified, and that the equipment was accurately tabulating. This meeting was broadcast live and is still available to the public.

Post-election court challenges

Many allegations about the November 2020 General Election made their way to court and Maricopa County clearly presented the facts to judges at both the local and federal level. Fourteen different times complaints about election fraud, manipulation, or tampering in Maricopa County's 2020 election were brought against the County. Each case was dismissed by the courts or withdrawn by the plaintiffs. For a complete listing of all court cases, see *Exhibit - COURT CASES*.

Response and Analysis

4 (Tally Results), 4.1 (Presidential Contest), 4.3 (Senate Contest), & Machine Count Report (pg. 4, 20-36)

The County's official canvass and the Senate's machine count closely match. However, an analysis of Cyber Ninjas' hand count reports and procedures reveal discrepancies that call the hand count findings into question. Hand count procedures changed over time, were inconsistent with Arizona law, and over 28% of hand count batch totals did not match the Senate's machine count.

Cyber Ninjas took nearly six months to count and report just two contests from Maricopa County's 2,089,563 ballots from the November 2020 General Election. On July 13, 2021, Arizona Senate President Karen Fann said publicly that their tally did not match the county's canvass and that she didn't know how much the two numbers differed. However, she ordered a separate machine count as a result. The Senate's Machine Count Report states on page 4: "*These results show the machine count confirms Maricopa County's reported ballots total for the 2020 election.*"

An incorrect hand count would impact other parts of Cyber Ninjas' report, including inaccurate ballot findings and claims related to duplicate ballots (*Item 14 – Damaged and Duplicate Ballots, pg. 83*). Our analysis of Cyber Ninjas' hand count results and reported hand count procedures reveal some of the inaccuracies, inconsistencies, and problems with Cyber Ninjas' hand count. Below is a summary of some of the issues:

- Ballot Totals Don't Match – As the U.S. Senate race and Presidential contest are on every ballot, the total number of ballots should be the same. Cyber Ninjas' hand county reported a 173-ballot difference between the two contests:
    - Presidential Contest - 2,088,569
    - U.S. Senate Contest - 2,088,396

  If the hand count was performed accurately and consistently, the vote totals for official candidates, write-in candidates, and under/over votes for these two contests would match perfectly.

- Hand Count Totals Don't Match Machine Count – The machine count performed by the Senate found a total of 2,089,442 ballots, which is 873 ballots *more* than was hand counted by Cyber Ninjas in the Presidential contest and 1,046 ballots *more* than was hand counted by Cyber Ninjas in the U.S. Senate contest. There are dozens of other discrepancies between Cyber Ninjas' hand count and the Senate's machine count documented in pages 20-36 of the Machine Paper Ballot Count Report.
    - 51 of the 180 (28.3%) batches in the report for which there was both a Cyber Ninjas' ballot count and a machine count entry show a different number of ballots counted by Cyber Ninjas than the Senate's machine count. In this analysis, we included batches for boxes in which one Cyber Ninjas' ballot count entry was missing, but the remaining batches were included, and all machine count batches were included. The missing batches were included because it is an indication that Cyber Ninjas missed counting or recording an entire batch during their hand count.
    - When comparing the total ballot counts for each box that were entered by Cyber Ninjas and the machine count entries, there were 14 total instances when the total box count between Cyber Ninjas and the

machine count differed. The absolute difference for these boxes totaled 1,657 ballots. The net difference for these boxes totaled 249 ballots.

- Hand Count Inconsistent with Arizona Law – Cyber Ninjas used a tally method to perform their hand count process. This method is not authorized for hand counts under state law. State statute (A.R.S. § 16-602) and the 2019 Arizona Elections Procedure Manual (Chapter 11, Pages 213-234) detail the authorized methods for performing a hand count. The only authorized method for performing a hand count of paper ballots is to use a stacking method. This requires that one contest be counted at a time and the ballots with votes for each candidate in that contest be sorted so an accurate count can be obtained. Additionally, how to determine voter intent is also outlined on page 233 of the Elections Procedures Manual, including that the three-member board made up of differing political parties reach a unanimous decision, rather than a majority of the counters, as was done in Cyber Ninjas' hand count.
- Hand Count Procedures Continuously Changed – During Cyber Ninjas' hand count, observers from the Arizona Secretary of State's office noted "*that the hand tally began before written procedures were shared and were only made available after litigation.*" Observers also noted that the "*implementation of the procedures as written was inconsistent and changes were made to the procedures regularly and in the middle of ongoing processes*." These observations are documented in a report by the Arizona Secretary of State's Office titled, *Report on the Partisan Review of the 2020 General Election in Maricopa County*. Additional issues identified by the Secretary of State's observers are included below.
    - Voter Intent (pages 32-33) – "*Cyber Ninjas' staff performing the counting were not provided with a copy of the Arizona state laws or procedures that govern voter intent rules. Each member of the counting crew were told to look at the ballot and determine for whom they believed the voter intended.*"
    - Hand Tally Error Rate (pages 28-30) – "*While the written policies require batches of 100 ballots, in practice, there were a variety of circumstances that resulted in batches of under 100 ballots... There were no standards in place for addressing any discrepancies, recording the tally often came down to the opinion of the table lead... The fluctuating batch size was a significant concern because it created an unacceptably high potential for error, or error rate.*"

Cyber Ninjas' inaccurate and inconsistent reporting of results contrasts with Maricopa County's official canvass of the November 2020 General Election. While it took Cyber Ninjas six months to count two contests and release a report with information contradictory to the Senate's machine count, the County completed its canvass of over 2,089,563 ballots by November 20, 2020 (17 days after Election Day), reporting results for over 227 separate contests.

As part of the canvass, the County created a Summary Report, a Full and Complete Canvass, and a text file of detailed precinct level results. The County also created a Cast Vote Record, that lists the results tabulated for every contest on every ballot. These four separate documents include the certified results for the November 2020 General Election and reconcile perfectly.

Item #3: Paper and Printer Claims

(Cyber Ninjas Volume III Report Sections - 5.7.5, 5.7.6, 5.7.10, 5.7.13)

Cyber Ninjas made four claims that the County used questionable ballot paper and out-of-calibration printers. All four claims are false.

Cyber Ninjas Volume III		County Analysis
Reference	Claim	
5.7.5 (pg. 52)	"High Bleed-Through Rates on Ballots" due to not using VoteSecur paper	False Claim
5.7.6 (pg. 54)	"Improper Paper Utilized"	False Claim
5.7.10 (pg. 57)	"Out of Calibration Ballot Printers"	False Claim
5.7.13 (pg. 61)	"Questionable Ballots" with anomalous characteristics	False Claim

State & Federal Laws

A.R.S. § 16-502 (A) describes the form and contents of ballots.

Maricopa County Findings

The County prepared and printed all official ballots used in the November 2020 General Election in accordance with state laws. This included printing ballots on white paper with black ink. All paper was of sufficient thickness to prevent the printing from being discernible on the opposite side. While not a requirement, the County used certified 80lb VoteSecur paper for all ballots during the 2020 Elections. The VoteSecur paper is the preferred paper type recommended by Dominion Voting Systems for use with the Democracy Suite 5.5-B tabulation equipment, which is the equipment that the County currently leases.

Summary

5.7.5 (High-Bleed Through Rates) & 5.7.6 (Improper Paper Used)

> **Cyber Ninjas' report included inaccurate and faulty information about the paper used for official ballots and the calibration of printers. The County has not identified a single instance when an official ballot was printed on anything but 80lb VoteSecur Paper.**

Response and Analysis

Cyber Ninjas claim they identified "10 different papers" used for ballots. Maricopa County used 80lb VoteSecur paper for every ballot (early, Election Day, provisional and printed from accessible voting devices) issued to voters during the November 2020 General Election. Election Day, early and provisional ballots are printed on 19 inch, 80lb VoteSecur paper. Ballots cast on accessible voting devices are printed on 8.5x11 inch 80lb VoteSecur paper. Our purchase and inventory/delivery records confirm that only VoteSecur paper was used for official ballots mailed to voters and for ballots printed at in-person voting locations.

The County used other types of paper for office use in three instances, but none included paper for tabulated ballots.

- Control Slips & Envelopes – At the voting locations, control slips and affidavit envelopes are also printed. The paper used for these other purposes is too small and not formatted correctly to be used for printing a ballot.
- Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) ballots — Military and Overseas voters may return ballots by mail, fax, or a secure portal. Ballots returned by fax or the secure portal must be printed on standard printer paper, as it is not currently possible to print these ballots in a tabulatable format. The ballots are then duplicated onto a standard ballot using 80lb VoteSecur paper for tabulation. The original UOCAVA ballots were subpoenaed by the Senate and included in the production of items provided to Cyber Ninjas.
- Large Print & Braille Ballots – Tabulation equipment cannot read braille, and large print ballots are printed on large sheets of paper. Both of these ballot types are duplicated onto a standard ballot using 80lb VoteSecur paper for tabulation. The original braille and large print ballots were subpoenaed by the Senate and included in the production of items provided to Cyber Ninjas.

In the November 2020 General Election and all subsequent elections, we have identified zero instances of ballots counted by the tabulation equipment and printed on paper other than 80lb VoteSecur paper.

Cyber Ninjas also incorrectly state that bleed through cannot happen when VoteSecur paper, the recommended paper, is used. They did not confirm their incorrect assumption with the paper manufacturer (see *Exhibit – PAPER #1 and Exhibit - PAPER #2*). According to the manufacturer (Roland), the VoteSecur paper that the County used in the November 2020 General Election did not have any special properties that would prevent bleed-through from felt or Sharpie pens. Because bleed-through can occur, the County designed ballots with offset columns to prevent it from impacting tabulation. Cyber Ninjas confirmed that bleed through did not impact tabulation, as stated on page 52 in their report, "*Out of the several thousand ballot images that were manually reviewed we could not find any images where bleed-through was close enough to a ballot oval to cause mistabulation, nor did we see any immediate correlation with adjudication.*"

Summary
5.7.10 (Printer Calibration)

> **All of the County's Ballot-on-Demand printers used at voting locations are calibrated and tested prior to deployment and when onsite at a voting location.**

Response and Analysis
The Elections Department uses a detailed checklist when preparing Ballot-on-Demand printers for use at voting locations. This includes a series of tests to confirm toner levels and proper calibration. During setup at a voting location, the setup teams also perform a series of test prints to verify the printers are functioning properly. These tests were completed for all printers and voting locations. However, as printers are used throughout the election, it is possible that they can run low on toner or paper and may become misaligned when replacing these items. For these reasons, the County has a technical assistance hotline and a team of technical support staff members that can be dispatched to voting locations.

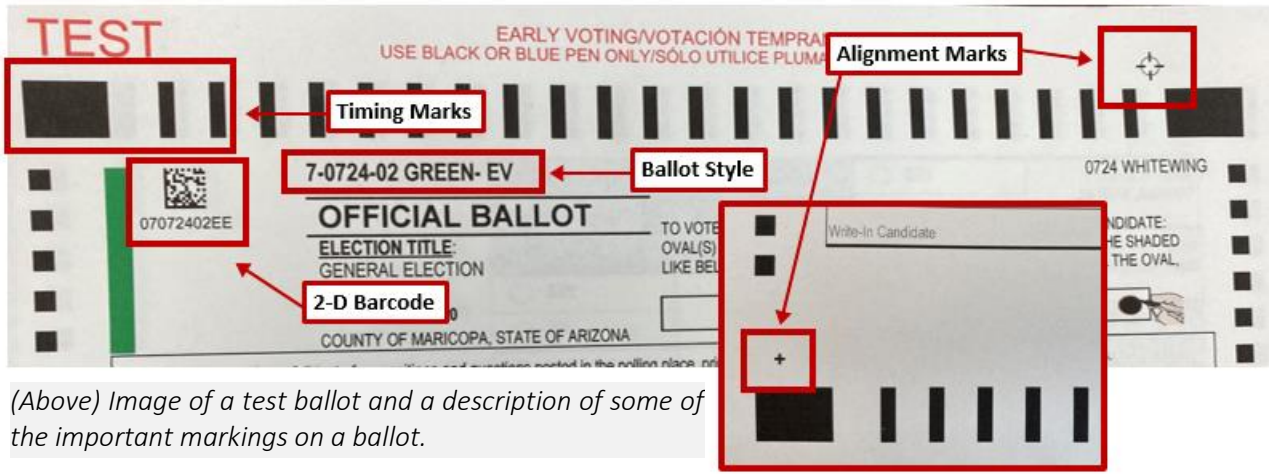
There are several markings on each ballot (see *PAPER Image #1*). Some are very important for tabulation and reporting purposes, and others are used for printing and ballot identification purposes. These markings include:

- Timing Marks — The tabulation equipment does not actually read the ballot text or handwriting from voters. To count voters' choices, the tabulation equipment is programmed to use the timing marks around the edge of the ballot to determine where the ovals should be, and then looks for a voter's mark in those target areas. If the timing

marks are damaged, the tabulation equipment will be unable to read the ballot, and it must be duplicated by bipartisan teams of two onto a new ballot.

- Ballot Style – Ballots are customized for each area of Maricopa County to ensure that voters only vote for the candidates and ballot questions for which they are lawfully entitled to cast their ballots. So, for example, voters who reside in Legislative District 1 are not offered ballots listing candidates for Legislative District 4, because they cannot lawfully vote for them. There were over 10,920 ballot styles in the 2020 General Election and some voters had more than 60 contests on the ballot. When a color is included, it means there are different ballot styles within a precinct.
- 2-D Barcodes – These barcodes provide the County with a quick way to identify the ballot style and are primarily used to identify the ballot for printing. They do not contain any information other than the ballot style and even include the human readable information below it.
- Alignment Guides – There are four alignment guides (two circles with cross hairs and two crosses) in the corners of the ballot that are only for printing purposes and do not impact tabulation.

PAPER Image #1 – Ballot Markings



(Above) Image of a test ballot and a description of some of the important markings on a ballot.

Summary

5.7.13 (Questionable Ballots)

> **The presence or absence of microscopic yellow dots has no bearing on the legitimacy of a ballot. The County uses a variety of commercial grade printers to print ballots and some add microscopic yellow dots that do not impact tabulation.**

Response and Analysis

The Elections Department and its print vendor use a variety of printers (large scale HP printing press, Indigo 12000, Lexmark 923, Oki 9650, Oki B432) to print ballots. These commercial printers come with different settings and features, but they all ensure the same high level of security around ballot creation, printing, verification and counting no matter how a voter

chooses to cast a ballot. Depending on the printer, the instructions in the header on some ballots are printed in color and others are printed in black and white.

While there are no watermarks programmed on Maricopa County ballots or on the paper, approximately 9% of the printers (Lexmarks 923) used at Vote Centers during the 2020 General Election have a standard feature that adds microscopic yellow dots to everything printed on that machine. The HP large scale printing press used for 99.7% of all mail ballots also print a series of random yellow dots to service the toner print nozzles. These dots are invisible to the human eye, do not impact tabulation, and have no bearing on whether the ballot is legitimate or not. They are simply a function of those particular printers. The remaining printed ballots do not have any randomly placed yellow dots. These ballots without microscopic yellow dots include the .91% of Vote Center ballots that were printed on the Oki devices and the less than one percent (.003%) of mail ballots printed on the Indigo 12000 (see *Exhibit – PRINT #1 and Exhibit – PRINT #2*).

Item #4: Election Management System Database and Files

(Cyber Ninjas Volume III Report Sections - 6.4.1, 6.4.2 & 6.5.1)

Senate contractor, CyFIR, included nine inaccurate claims about Maricopa County deleting files from the Election Management System (EMS) database and other tabulation equipment in Cyber Ninjas' report. These claims are inaccurate and not supported by the County's records and images of the database.

Reference	Claim	County Analysis
Section 6.4.1 (Pg. 63)	"Election Management System Database Purged"	*Inaccurate Claim* - All data was archived per standard policy. Archival procedures followed by the County are in compliance with federal and state laws.
Section 6.4.2 (Pg. 65)	"Election Files Deleted"	
Section 6.4.2.1.1 (Pg. 66)	"Deletion Activity on the EMS C:\ Drive"	
Section 6.4.2.1.2 (Pg. 67)	"Deletion Activity on the EMS D:\ Drive"	
Section 6.4.2.1.3 (Pg. 68)	"Deleted Directories and Files From HiPro 1" "HiPro 3" "HiPro 4"	*Inaccurate Claim* - The County provided ballot images to the Senate on 4/22/2021. Using a copy of the hard drive that the County provided to the Senate, we have confirmed that all ballot images are saved and can be opened without issue.
Section 6.4.2.1.4 (Pg. 69)		
Section 6.4.2.1.5 (Pg. 69)		
Section 6.4.3 (Pg. 70)	"Corrupt Ballot Images"	
Section 6.5.1 (Pg. 73)	"Missing Ballot Images"	

State & Federal Laws

The Help America Vote Act, a federal law, provides certification requirements for tabulation equipment, including allowing states to adopt Voluntary Voting System Guidelines. Arizona law requires counties follow federal guidelines on certification as well as governs how digital images of ballots should be stored. Applicable Arizona laws include:

- A.R.S. § 16-442 (B)(C)
- A.R.S. § 16-1004 (B)
- A.R.S. § 16-625
- A.R.S. §16-624 (A)
- A.R.S. §16-624 (A)(B)

Maricopa County Findings

CyFIR made a variety of false claims beginning in May 2021 alleging County staff deleted election databases or files. In some cases, the items that contractors could not find were items the Senate did not subpoena and therefore wouldn't have. In other cases, the "missing" data was exactly where it was supposed to be, as proven by copies of the EMS server and images that the County cloned prior to providing those materials to the Senate.

The County debunked one such allegation in a May 17 Technical Response to Arizona Senate President Karen Fann after she claimed in a letter that County staff deleted a directory full of election databases. Our analysis showed the files were still present on the server provided to the Senate. Despite this knowledge, similar allegations made it into Cyber Ninjas' final report and CyFIR's September 24 presentation. The inaccurate claims about Maricopa County deleting files from the EMS database and other tabulation equipment are not supported by the County's records and images of the database. The County has in its possession the EMS databases, software, and files from the November 2020 General Election.

The Maricopa County Elections Department follows state and federal laws and best practices in election administration. These laws and best practices were followed in the maintenance and archiving of 2020 election files and in the way the EMS server, software, and files were delivered to the Senate.

Summary

6.4.1 (Election Management System Purged), 6.4.2 (Election Files Deleted), 6.4.2.1.1 (EMS Server C:\ Drive), and 6.4.2.1.2 (EMS Server D:\ Drive), 6.4.2.1.3, 6.4.2.1.4, 6.4.2.1.5 (Deleted Ballot Images from HiPro Scanners), 6.4.3 (Corrupt Ballot Images), 6.5.1 (Missing Ballot Images)

Maricopa County did not delete the Election Management System database, software, or corresponding files for the November 2020 General Election. The Election Management System database and files were archived. The information subpoenaed by the Senate was provided on 4/21/2021.

Response and Analysis

As stated in the January 12, 2021 subpoena, the Arizona Senate commanded production of "the software for the equipment… and the election management system used." Senate contractors falsely claim that staff "purged" the Election Management System (EMS) database prior to turning it over to the Senate. They claim many election-related files were deleted in the process.

The County reviewed cloned copies of the EMS server *as it was* when we delivered it to the Senate. These copies were made in March 2021, as the County readied a backup server to use in the March 2021 Jurisdictional Election.

The cloned copies show the EMS database and software used for the November 2020 General Election were installed on the server and tabulation equipment that was provided to the Senate on 4/21/2021, the date that the Senate requested that the County provide delivery of the tabulation equipment (see *Exhibit – SENATE REQUEST*). In other words, the County delivered the EMS servers exactly as commanded by the subpoena. The County delivered all tabulation equipment, including the four Hi-Pro Scanners, as they were at the time the Maricopa County Superior Court ruled the subpoena was valid. The only time the County accessed the equipment after the court ruling, was to comply with the Senate's subpoenas and to clone the server for the statutorily required March 2021 Jurisdictional Election.

During the November 2020 General Election, the County created 26 daily back-ups of the EMS server, with the last one occurring after tabulation was completed on November 13, 2020. All the backup hard drives and corresponding data files have been maintained and safely secured. Contrary to claims made by the Senate and their contractors, the Arizona Senate did not subpoena these archived files (see *Exhibits - SUBPOENA*). The election data stored in the archives contain sensitive and statutorily protected information that cannot be disclosed through a Public Records Request and would require a court order or subpoena to be produced.

Due to space constraints on the EMS server, the County archived the November 2020 General Election tabulation data. It is standard procedure for the County to remove and relocate election-specific files from the U.S. Election Assistance Commission (EAC) certified EMS server once it nears its two-terabyte storage capacity. The uncompressed files associated with the November 2020 General Election exceeded 1.9 terabytes of data, or 1.3 terabytes in a compressed format. Using

the certified Dominion Democracy Suite 5.5-B archival program, elections-specific files were archived and relocated from the primary storage location (D: Drive) and saved on external backup hard drives. The Senate did not subpoena the backup drives that contain the archived files.

CyFIR also claims there are missing ballot images on the forensic images of the primary Dominion EMS server. In response to the Senate's subpoena, the County provided copies of the ballot images from the 2020 General Election on a separate hard drive delivered to the Senate on April 22, 2021. The County delivered all central count scanners, including the four HiPro Scanners as they were at the time the Maricopa County Superior Court ruled on February 26, 2021 that the Senate's January 12, 2021 subpoena was valid.

The Senate and its contractors have accused the County of deleting files from the EMS on three separate dates. Below are the actions taken on the dates County staff was wrongly accused of deleting files:

- February 2, 2021—The County took the standard data archival steps to ready the server and tabulation equipment for use in the statutorily required March 2021 Jurisdictional Election. Ballots for that election were sent to military and overseas (Uniformed and Overseas Citizens Absentee Voting Act) voters on January 23, 2021. Tabulation began after the February 22, 2021 logic and accuracy test. In addition, the County needed to prepare the equipment for the audits performed by SLI Compliance and Pro V&V, both EAC certified Voting System Test Laboratories. As part of Pro V&V's scope of work, they were contracted to perform a logic and accuracy test of the tabulation equipment and election program used for the November 2020 General Election. The fact that CyFIR has insinuated that the County intentionally deleted files prior to their audit to hide information demonstrates the CyFIR's lack of understanding of the purpose of a logic and accuracy test.

  > *"A logic and accuracy (L&A) test is intended to confirm that votes are attributed to the correct candidates and ballot measures in the election management system (EMS) and that each candidate and ballot measure receives the accurate number of votes."* (Arizona 2019 Elections Procedures Manual Pg. 100)

  In order to complete a reliable accuracy test of the EMS program used in the November 2020 General Election, Pro V&V, needed to "reset any vote totals" to ensure no votes were on the database (Arizona 2019 Elections Procedures Manual Pg. 105). This is only possible if the results from the November 2020 General Election were archived per the County's standard policy. To confirm accuracy of the actual EMS program used in the November 2020 General Election, Pro V&V tested over 1.5 million ballot positions using the very same election program that was used to tabulate every ballot for that election. Pro V&V found no evidence of vote switching and concluded that the equipment tabulated and adjudicated ballots accurately (see *Exhibit - PRO V&V AUDIT)*.
- March 3, 2021—After a court ruling on February 26, 2021, staff members were complying with the Senate's subpoena by gathering the subpoenaed ballot images from the archives and tabulation equipment. On March 3, 2021, the County used the November 2020 General Election archives to restore ballot images onto the Election Management System. This action was taken to comply with the Senate's subpoena commanding the production of the November 2020 General Election ballot images. During this process, the County consolidated all images onto a single location on the server and performed an inventory to verify that all 2,089,563 ballot images were present. The County transferred these restored ballot images onto a hard drive that was provided to the Arizona Senate on April 22, 2021. The hard drive with the ballot images was transferred to the custody of the Senate and recorded on the delivery manifest signed by both parties (see *Exhibit - MANIFEST*).

  To ensure the County had an exact copy of what was provided to the Senate, the County also created a clone of the hard drive on March 3, 2021. The second hard drive was retained by the County. Since the release of Cyber Ninjas' report, we have reviewed the County's copy of the hard drive and confirmed that all images are present.

We randomly selected image files from the date periods that CyFIR claimed included corrupted images. In all instances the County was able to open the image files.

- April 12, 2021—Staff was complying with the Senate's subpoena and packing up the server and other tabulation equipment for delivery to the Senate.

Item #5: Operating System Logs

(Cyber Ninjas Volume III Report Sections - 6.5.4, 6.5.6, 6.5.6.1.1, 6.5.6.1.2, & 6.5.6.1.3)

Senate contractor, CyFIR, included five inaccurate or false claims in Cyber Ninjas' report that Maricopa County did not preserve the operating system logs from the Election Management System (EMS) server. The County found all of these claims were inaccurate or false based on the records retained by the County and, additionally, the analysis of an independent, third-party cyber forensics firm.

Reference	Claim	County Analysis
6.5.6 (Pg. 85)	"EMS Operating System Logs Not Preserved"	*Inaccurate Claim* - Logs were provided in separate deliveries to the Arizona Senate on January 15 and April 21, 2021. Additionally, security logs found on the County's cloned copy of the server date back to November 18, 2020.
6.5.6.1.1 (Pg. 86)	"User Log Deletions on 02/11/2021"	*Inaccurate Claim* - Work was being performed on the EMS server to prepare it for legitimate audits by SLI Compliance and Pro V&V. The security log events were normal course-of-business automated actions actuated from the Dominion Democracy Suite 5.5-B EMS application.
6.5.6.1.2 (Pg. 86)	"User Log Deletions on 03/03/2021"	*Inaccurate Claim* - The EMS server was being prepared to have a clone made to facilitate the 2021 March Jurisdictional Elections. The SQL Service, DHCP/DNS services, and the Dominion application suite all show that the server was being shut down in preparation for cloning activities.
6.5.6.1.3 (Pg. 87)	"User Log Deletions on 04/12/2021"	*Inaccurate Claim* - The EMS server was being prepared for packaging and delivery to the Arizona Senate as commanded by the January 12,2021 subpoena. SQL Services, applications and other server functions were being shut down.
6.5.4 (Pg. 82)	"Anonymous Logins"	*False Claim:* An analysis of the security logs concluded these logins were legitimate, typical Microsoft server actions. Additionally, the EMS server implements "hardening" scripts throughout the operating system configuration that increases the frequency and types of events found within the security log.

Maricopa County Findings

CyFIR accused County employees of intentionally deleting or overwriting user security logs, which are baseless claims. These spurious allegations may stem from a misunderstanding of closed network systems and basic Microsoft Server 2012r2 configurations, as well as a failure to do simple fact checking. In many cases, the events that contractors falsely attributed to a nefarious remote user running "scripts" to purge files were standard, automated actions from the EMS application meant to manage space on the server.

An experienced IT professional familiar with Microsoft Server Logs understands the concept of a "first in, first out" configuration in which older events are pushed out of event log files as new files are added. This configuration is common, and it is often the baseline configuration for closed network systems like the one used by the Elections Department. For Microsoft Server 2012r2 configurations, many log files have a default limited to 20 megabytes of storage capacity before older files begin to fall off as new are added.

In several instances, CyFIR cites specific dates and times where it believes County employees intentionally deleted user logs. However, the security logs and surveillance footage from the dates and times in question contradict those claims. Each instance is, in fact, explained by something far more pedestrian: employees and machines doing the routine work of the day, in accordance with law and Elections Department procedures.

Summary

6.5.6 (EMS Operating System Logs Not Preserved), 6.5.6.1.1 (User Log Deletions on 2/11/2021), 6.5.6.1.2 (User Log Deletions on 03/03/2021), 6.5.6.1.3 (User Log Deletions on 04/12/2021)

> **Maricopa County security logs were retained following the federally certified build requirements. No data was purposefully deleted by County staff. CyFIR's claim that an individual ran scripts against a machine in order to "flood" the security logs is inaccurate and is indicative that the Senate's contractor may not understand Microsoft Server based protocols and logging.**

Response and Analysis

Logs were provided in separate deliveries to the Arizona Senate on January 15, 2021, and April 21, 2021. Security logs found on the County's cloned copy of the server date back to November 18, 2020. In addition to our review and analysis of the logs, the County took another step to seek an independent third-party cyber forensics firm for comment and independent analysis, contracting with PacketWatch in October of 2021 to review prior reports and technical findings related to the November 2020 General Election.

PacketWatch is a cybersecurity and incident response firm based in Scottsdale, Arizona. Staffed by former FBI officials, US military, and various government organizations, PacketWatch has expertise in the public and private sectors and is well qualified to provide a detailed analysis of these claims. PacketWatch reviewed the Microsoft Server event logs and came to the same conclusions as the County. Microsoft Server 2012r2 has a default maximum event log size is 20MB (see *Exhibit - PACKETWATCH*).

In order to modify the log size setting, it would require federal approval from the EAC for a de minimis change to the server configurations. Given the 20MB limit, and substantial number of log entries generated by the Dominion Democracy Suite 5.5-B during election processes, it is expected older log entries would be overwritten by the system as newer events are logged. This is an operating system function using a default setting. Microsoft Server event logs, including security logs, are preserved on the system on a first in, first out basis and limited to the maximum size setting in the operating system. The County requested Dominion pursue this EAC de minimis change for future elections.

Throughout sections 6.5.6.1-6.5.6.3, CyFIR repeatedly reported instances of a user "utilizing the emsadmin account remotely logged into the EMS server… and began executing a script… that checked for blank passwords." This is refuted by professional analysis of what is being recorded in the EMS Server security logs. The Dominion Democracy Suite 5.5-B application has several functions that use automated scripts to perform repetitive actions. The application uses a Microsoft Server function called "Microsoft Message Queuing" (MSMQ) to systematically connect from the EMS Server to the EMS tabulation, adjudication, and admin computers to ask if these devices have any data that can be passed back to the server. This is all done in the secure, air gapped tabulation room, which is not connected to the internet. In simplified terms, the

tabulators and adjudication stations will hold onto their changes and updates in a data cache and queue them up for when the EMS server application reaches out and asks for the queue data.

LOGS Image #1 – Screenshots of EMSAdmin Security Log

Event 4797, Microsoft Windows security auditing.

General | Details

An attempt was made to query the existence of a blank password for an account.

Subject:
Security ID: S-1-5-21-3765983672-4180476312-3453754044-1002
Account Name: emsadmin
Account Domain: EMSSERVER
Logon ID: 0x3203B7

Additional Information:
Caller Workstation: EMSSERVER
Target Account Name: iccadmin06
Target Account Domain: EMSSERVER

The MSMQ service call out to a client machine originating from the Dominion EMS Server

Target EMS Tabulation Machine

Log Name:	Security		
Source:	Microsoft Windows security	Logged:	2/11/2021 1:07:25 PM
Event ID:	4797	Task Category:	User Account Management
Level:	Information	Keywords:	Audit Success
User:	N/A	Computer:	EMSSERVER
OpCode:	Info		
More Information:	Event Log Online Help		

(Above) Screenshot security log that are claimed to be a user running a script that checks accounts for blank passwords.

LOGS Image #2 – Screenshots Unique Security Log


```
<Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event">
- <System>
    <Provider Name="Microsoft-Windows-Security-Auditing" Guid="{54849625-5478-4994-a5ba-
      3e3b0328c30d}" />
    <EventID>4797</EventID>
    <Version>0</Version>
    <Level>0</Level>
    <Task>13824</Task>
    <Opcode>0</Opcode>
    <Keywords>0x8020000000000000</Keywords>
    <TimeCreated SystemTime="2021-02-11T18:25:48.9437340Z" />
    <EventRecordID>10345638</EventRecordID>
    <Correlation />
    <Execution ProcessID="688" ThreadID="9092" />
    <Channel>Security</Channel>
    <Computer>EMSSERVER</Computer>
    <Security />
  </System>
- <EventData>
    <Data Name="SubjectUserSid">S-1-5-21-3765983672-4180476312-3453754044-1002</Data>
    <Data Name="SubjectUserName">emsadmin</Data>
    <Data Name="SubjectDomainName">EMSSERVER</Data>
    <Data Name="SubjectLogonId">0x3203b7</Data>
    <Data Name="Workstation">EMSSERVER</Data>
    <Data Name="TargetUserName">adjadmin01</Data>
    <Data Name="TargetDomainName">EMSSERVER</Data>
  </EventData>
</Event>
```


(Above) Unique security log for EMSSERVER MSMQ Call to client machine adjadmin01 02/11/2021 at 10:25:48 AM

MSMQ utilizes a series of log events it writes to the security log in the format listed below. MSMQ goes through security account auditing tasks that get listed as "An attempt was made to query the existence of a blank password for an account." This is a standard process within Microsoft Server 2012r2 when utilizing this kind of MSMQ call. Within 1-2 minutes of initiation, the application utilizes MSMQ protocols to poll 67 user accounts on connected tabulators and adjudication stations to gather changes and updates. This process happens several times per day, depending on how much data needs to be transferred over and how much activity is being conducted, whether there is an election being conducted or not. CyFIR was aware of this logging behavior during the public event held by the Arizona Senate President and Judiciary Chairman in July 2021, where it referenced this action as being innocuous and explained.

These calls (see *LOGS Image #1*) account for 396 out of 412 unique security log entries in the time periods listed in sections 6.5.6.1-6.5.6.3. Each unique instance has a different "Target Account Name" listed and the MSMQ polling automation always starts with client machine "adjadmin01." In this instance, the Dominion application automated processes utilized MSMQ polling.

Logging is a standard function of Microsoft Server 2012r2 and the Dominion Democracy 5.5-B software suite. Thousands of logs are created every day the EMS server is in operation, whether there is an election being conducted or not.

These automated actions are easily identified when auditing the logs and should be something that cyber experts know how to correlate to legitimate actions. The lack of attention to detail in recording the proper timeframes, actual event occurrence quantities and event contents for this claim is troubling.

Below are further details about sections 6.5.6, 6.5.6.1.1, 6.5.6.1.2, and 6.5.6.1.3.

EMS System Logs

6.5.6 (EMS Operating System Logs Not Preserved)

Cyber Ninjas' report included the claim on page 85; "In the case of the security.evtx file on the EMS server, the earliest retained log entry was dated 2/5/2021 10:37:49 AM (the last day of the Pro V & V audit) and the latest entry was dated 4/12/2021 4:53:16 PM."

LOGS Image #3 – Screenshots of Security Logs from November 18, 2020

Security Number of events: 36,587

Level	Date and Time	Source	Event...	Task Category
Information	11/18/2020 3:18:18 PM	Microsoft Windows security auditing.	5061	System Integrity
Information	11/18/2020 3:18:18 PM	Microsoft Windows security auditing.	5058	Other System ...
Information	11/18/2020 3:17:59 PM	Microsoft Windows security auditing.	4625	Logon
Information	11/18/2020 3:17:59 PM	Microsoft Windows security auditing.	4625	Logon
Information	11/18/2020 3:17:59 PM	Microsoft Windows security auditing.	5061	System Integrity
Information	11/18/2020 3:17:59 PM	Microsoft Windows security auditing.	5058	Other System ...
Information	11/18/2020 3:17:59 PM	Microsoft Windows security auditing.	4625	Logon
Information	11/18/2020 3:17:59 PM	Microsoft Windows security auditing.	4625	Logon
Information	11/18/2020 3:17:59 PM	Microsoft Windows security auditing.	5061	System Integrity
Information	11/18/2020 3:17:59 PM	Microsoft Windows security auditing.	5058	Other System ...
Information	11/18/2020 3:17:59 PM	Microsoft Windows security auditing.	5061	System Integrity
Information	11/18/2020 3:17:59 PM	Microsoft Windows security auditing.	5058	Other System ...

Event 5061, Microsoft Windows security auditing.

General | Details

Cryptographic operation.

Subject:
Security ID: S-1-5-21-3765983672-4180476312-3453754044-1038
Account Name: AdjSys
Account Domain: EMSSERVER
Logon ID: 0x6A6B0

Cryptographic Parameters:
Provider Name: Microsoft Software Key Storage Provider
Algorithm Name: RSA
Key Name: {716520BD-A4D0-431B-B830-076866B68E70}
Key Type: Machine key

Log Name:	Security		
Source:	Microsoft Windows security	Logged:	11/18/2020 3:17:56 PM
Event ID:	5061	Task Category:	System Integrity
Level:	Information	Keywords:	Audit Success
User:	N/A	Computer:	EMSSERVER
OpCode:	Info		
More Information:	Event Log Online Help		

(Top) Screenshot from the primary Dominion EMS server clone shows security logs show the oldest log from 11/18/2020. (Bottom) Screenshot from the primary Dominion EMS server clone shows a detailed view of event 5061 with a log date of 11/18/202 at 3:17:56 p.m.

The report stated that the Dominion Election Management System Server security log was configured to the standard 20MB capacity limit found in Microsoft Server 2012r2 default configurations. This is true and is common. This configuration does not violate any federal or state laws as it relates to elections. What is not true however, is that CyFIR did not have logs that dated prior February 5, 2021. An analysis of the County's cloned copy of the EMS Server (created on March 5, 2021) identified preserved security logs dating back beyond December 2020 (see *LOGS Image #3*). This log has over 5,300 logs between November 18, 2020, and the March 3, 2021 clone date.

CyFIR stated on page 85 of Cyber Ninjas' report that they "did not discover any enabled external log aggregation functionality nor were historical logs beyond those that were contained on the operating systems provided to the digital examination team." This statement is not applicable and the recommendation of adding an external logging configuration would

introduce unnecessary vulnerabilities into the County's air gapped Election Management System.

Further, during the Senate Hearing on September 24, 2021, CyFIR commented that the County's installation of the Dominion EMS does not follow Cybersecurity and Infrastructure Agency (CISA) guidelines in relation to the central transition of server and client logs (CyFIR Presentation, slide 4). While this is a common and recommend practice for server installations that connect to broader networks and the internet, these standards do not pertain to an air gapped system. The County's Ballot Tabulation enter uses an air gapped network. The infrastructure design and the installation of an additional third-party piece of equipment into the secure Election Management System server room and connected to the air gapped system would introduce more risks than benefits. This is due to the simple nature of the EMS design, where one server and connected client machines are the only items on the network.

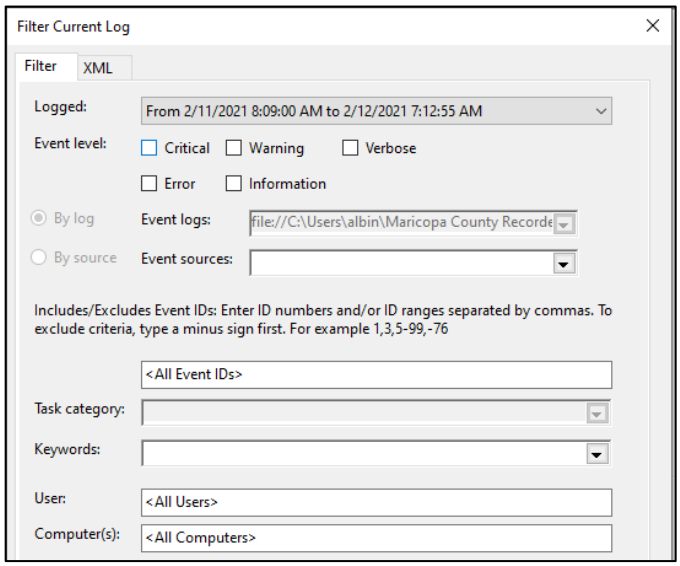
CyFIR also claimed "*security logs for the EMS server were in fact intentionally deleted such that the logs no longer covered the time period for the 2020 General Election.*" **The statement is baseless and insinuates malfeasance. There is no evidence to support this claim.** As described above, the EMS server event logs were using the standard Microsoft Server 2012r2 configuration of 20MB of cached event storage. This default configuration uses a "first-in, first-out" principal where older events are pushed out of the event logs files as new events are added. This configuration is common, and it is often the baseline configuration for closed network systems.

User Logs – February 11, 2021

6.5.6.1.1 (User Log Deletions on 2/11/2021)

The Cyber Ninja Volume III audit report, CyFIR claims: "A user leveraging the emsadmin account remotely logged into the EMS server at 2/11/2021 9:08:27 AM via terminal services and began executing a script at 2/11/2021 9:09:04 AM that checked accounts for blank passwords… Between 2/11/2021 8:09:04 AM and 2/12/2021 7:12:55 AM this user ran this check 462 times." During the Senate Hearing on September 24, 2021, CyFIR claimed that scripts were run as a "Clear Intentional Overwriting of the Security Logs by the EMSADMIN Account" (CyFIR Presentation, slide 12) with the purpose to cover unauthorized database deletions. These claims are false.

LOGS Image #4 – Screenshot of Server Results



(Above) Screenshot of settings from Windows Server Event Viewer and results

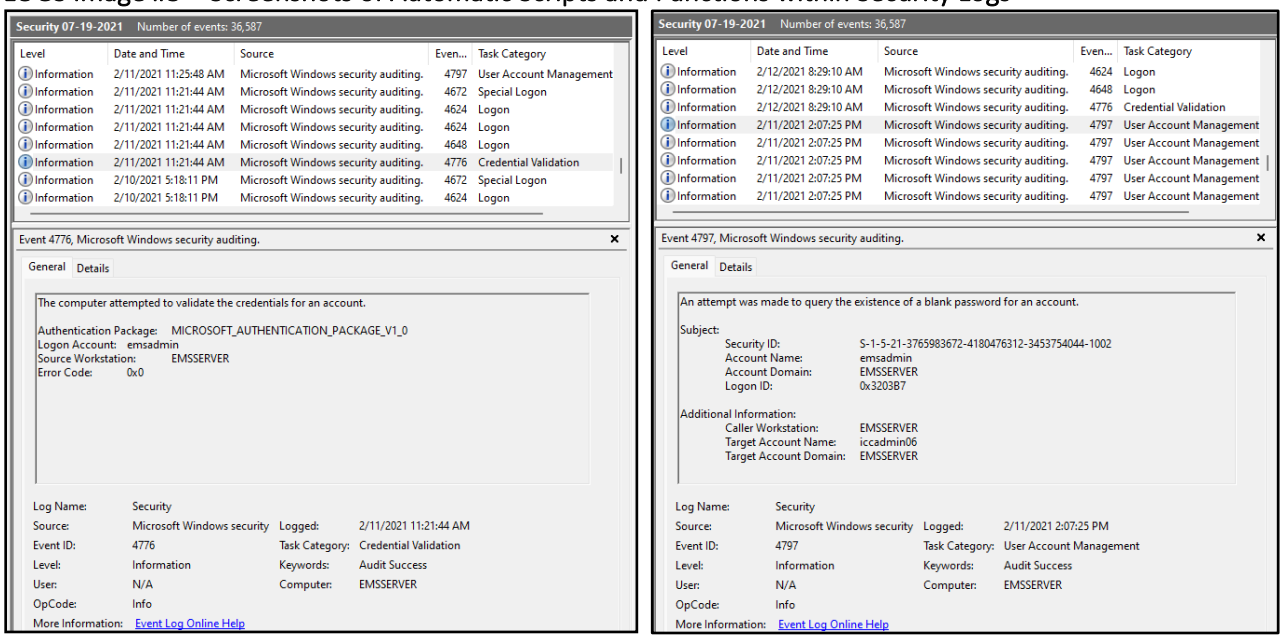
The County's review of the EMS server security log between February 11, 2021 at 8:09:04 a.m. and February 12, 2021 7:12:55 a.m. found 412 events, which is 50 fewer than CyFIR's claim. There is also no evidence of a security log showing a remote user logged in at the claimed "2/11/2021 9:08:27 AM" time period.

The entire security log from that day happened in a much shorter period than the Senate contractors claim. These 412 logs occurred on February 11, 2021, from 11:21:44 a.m. and 2:07:25 p.m. (Arizona Time). This disproves the claim that these scripts and

log actions were run on "2/11/2021 9:09:04 AM," because the earliest security log recorded on that day was two hours and 12 minutes later than CyFIR stated. On February 12, 2021, the earliest security log filed was at 8:29:10 a.m., which is 77 minutes later than the stated time CyFIR reported.

The events that CyFIR claimed were "scripts" it believes County employees used to intentionally delete user logs were actually automated actions by the Dominion EMS Democracy Suite 5.5-B application to conduct its primary function of managing the tabulation of ballots. This is done without user interaction. These functions are recorded in the security log and are often identifiable based on the patterns visible in the security logs themselves. Sometimes the application will add hundreds of entries into the security log within a few minutes. All of this is a standard function of the application.

LOGS Image #5 – Screenshots of Automatic Scripts and Functions within Security Logs



Security 07-19-2021 Number of events: 36,587

Level	Date and Time	Source	Even...	Task Category
Information	2/11/2021 11:25:48 AM	Microsoft Windows security auditing.	4797	User Account Management
Information	2/11/2021 11:21:44 AM	Microsoft Windows security auditing.	4672	Special Logon
Information	2/11/2021 11:21:44 AM	Microsoft Windows security auditing.	4624	Logon
Information	2/11/2021 11:21:44 AM	Microsoft Windows security auditing.	4624	Logon
Information	2/11/2021 11:21:44 AM	Microsoft Windows security auditing.	4648	Logon
Information	2/11/2021 11:21:44 AM	Microsoft Windows security auditing.	4776	Credential Validation
Information	2/10/2021 5:18:11 PM	Microsoft Windows security auditing.	4672	Special Logon
Information	2/10/2021 5:18:11 PM	Microsoft Windows security auditing.	4624	Logon

Event 4776, Microsoft Windows security auditing.

General Details

The computer attempted to validate the credentials for an account.

Authentication Package: MICROSOFT_AUTHENTICATION_PACKAGE_V1_0
Logon Account: emsadmin
Source Workstation: EMSSERVER
Error Code: 0x0

Log Name: Security
Source: Microsoft Windows security Logged: 2/11/2021 11:21:44 AM
Event ID: 4776 Task Category: Credential Validation
Level: Information Keywords: Audit Success
User: N/A Computer: EMSSERVER
OpCode: Info
More Information: Event Log Online Help

Security 07-19-2021 Number of events: 36,587

Level	Date and Time	Source	Even...	Task Category
Information	2/12/2021 8:29:10 AM	Microsoft Windows security auditing.	4624	Logon
Information	2/12/2021 8:29:10 AM	Microsoft Windows security auditing.	4648	Logon
Information	2/12/2021 8:29:10 AM	Microsoft Windows security auditing.	4776	Credential Validation
Information	2/11/2021 2:07:25 PM	Microsoft Windows security auditing.	4797	User Account Management
Information	2/11/2021 2:07:25 PM	Microsoft Windows security auditing.	4797	User Account Management
Information	2/11/2021 2:07:25 PM	Microsoft Windows security auditing.	4797	User Account Management
Information	2/11/2021 2:07:25 PM	Microsoft Windows security auditing.	4797	User Account Management
Information	2/11/2021 2:07:25 PM	Microsoft Windows security auditing.	4797	User Account Management

Event 4797, Microsoft Windows security auditing.

General Details

An attempt was made to query the existence of a blank password for an account.

Subject:
Security ID: S-1-5-21-3765983672-4180476312-3453754044-1002
Account Name: emsadmin
Account Domain: EMSSERVER
Logon ID: 0x3203B7

Additional Information:
Caller Workstation: EMSSERVER
Target Account Name: iccadmin06
Target Account Domain: EMSSERVER

Log Name: Security
Source: Microsoft Windows security Logged: 2/11/2021 2:07:25 PM
Event ID: 4797 Task Category: User Account Management
Level: Information Keywords: Audit Success
User: N/A Computer: EMSSERVER
OpCode: Info
More Information: Event Log Online Help

(Left) Screenshot showing the earliest security log file from the cloned server, recorded at February 11, 2021 11:21:44 a.m., which is significantly later than the stated timeframe of "2/11/2021 9:09:04 AM" from CyFIR. (Right) Screenshot showing last security log file from the cloned server, recorded at February 11, 2021 2:07:25 p.m., which is significantly earlier than the stated timeframe of "02/12/2021 7:12:55 AM" from CyFIR.

As explained in *LOGS Image #5*, on February 11, 2021, County election staff were preparing the server and other client machines for the scheduled certified auditors to perform audit test work. These audits were well documented and performed by experts certified to evaluate tabulation equipment and verify it functions properly.

CyFIR's claim that a County employee would maliciously run scripts to cover up evidence of other actions is demonstrably false. The surveillance footage also shows an SLI Compliance auditor was in the server room with County elections staff members at that time. The evidence obtained from event logs and surveillance footage clearly refutes CyFIR's findings. The claims they made were baseless and reckless.

LOGS Image #6 – Screenshots of Surveillance Footage from February 11, 2021

(Above Left) Blurred surveillance footage screenshot from the exact timestamp CyFIR falsely claimed the scripts were running to cover-up nefarious activity. (Above Center) Blurred surveillance footage screenshot of a Voting System Test Laboratory auditor and two authorized County elections employees. The auditor was at the Dominion EMS server's keyboard video monitor (KVM) conducting their audit tasks on the system. (Above Right) Blurred surveillance footage screenshot of the auditor and an authorized County elections employee checking on the backup copies and other analysis that was left running during lunch.

User Logs – March 3, 2021

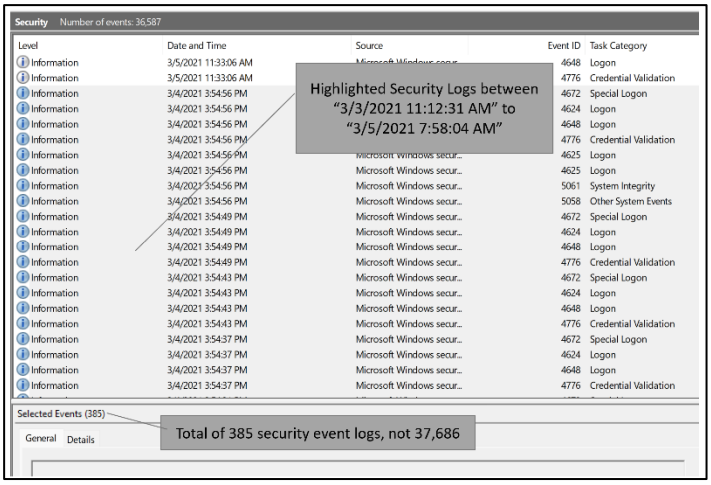
6.5.6.1.2 (User Log Deletions on 03/03/2021)

The response to this claim is much the same as 6.5.6.1.1. The Senate contractors did not understand what was being done to the Dominion EMS server and construed the actions as nefarious. The Senate contractors claim an employee ran a script from "3/3/2021 11:12:31 AM" to "3/5/2021 7:58:04 AM" that produced 37,686 log files, which in turn purged the older logs to hide their actions. This is inaccurate. Our review of the Dominion EMS system logs during the same timeframe shows a total of 385 logs, not 37,686 (see *LOGS Image #7*). These logs were not created to hide anything, as CyFIR claimed, but rather as a result of necessary operations to gather materials for the Senate's subpoena and to conduct a statutory required election.

Below is a timeline of actions for reference.

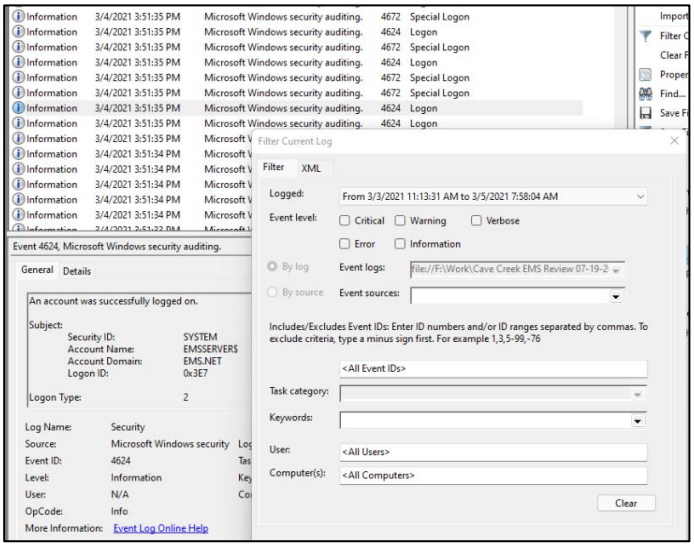
- March 3, 2021 — Gathering the subpoenaed ballot images from the archives and tabulation equipment for delivery to the Arizona Senate. This data needed to be compiled by running actions on the Dominion EMS server and application. The application produced several entries in the security log file during normal operation.

LOGS Image #7 –Security Logs from March 3-5, 2021



(Above) Screenshot from cloned server security logs showing the number of events from March 3-5, 2021.

LOGS Image #8 – Screenshots of Security Logs



(Above) User logs from the cloned EMS Server from April 12, 2021.

- March 4, 2021 — Began making a clone copy of EMS server using Acronis. This was just five days before the statutorily mandated March 2021 Jurisdictional Election. The purpose of cloning was to prepare a new replacement EMS server for the election, which was already in process.
- March 5, 2021 — Finished EMS Server clone. Installed Dominion Democracy Suite 5.5-B application to the new server.

The County also performed a review of the cloned EMS server that we have continued to use to conduct ongoing statutorily required elections. In reviewing the security logs that spanned from November 18, 2020 to July 19, 2021 (the day this security log screenshot was taken), there was a total of 36,587 logs (see *LOGS Image #8*). It would be impossible for 37,686 logs to be produced in less than 48 hours when it took almost nine months to generate 36,587 of security logs.

Furthermore, due to the described 20MB storage limit, the security logs can only hold between 35,000 and 38,000 events at one time. On page 85 of Cyber Ninjas' report, CyFIR contradicts its own statements on these "flooded" events by stating that events were preserved back to February 5, 2021. If 37,686 events were "flooded" into the security log in that short amount of time, there would only be room enough for logs starting on March 3, 2021. More than 37,000 events would have certainly overflowed the security logs 20MB storage capacity. CyFIR's admission to having security logs back to February 5, 2021 and this claim of 37,686 flooded logs within 48 hours do not comport with logical configurations and capabilities of Microsoft Server 2012r2 security logs.

User Logs – April 12, 2021

6.5.6.1.3 (User Log Deletions on 04/12/2021)

LOGS Image #9 –April 12, 2021 Surveillance Video Screenshots

(Above Top) Blurred screenshot of County elections staff shutting down the primary Dominion EMS server. (Above Center) Blurred screenshot of County elections staff outside of the server room, about 10 minutes after the shutdown process was started. (Above Bottom) Blurred screenshot of County elections staff boxing up the primary Dominion EMS Server for delivery to the Arizona Senate.

Much the same as the responses for 6.5.6.1.1 and 6.5.6.1.2, this claim is not corroborated by the security logs or the surveillance footage for timelines. CyFIR claims an employee ran a script 330 times from "4/12/2021 12:39:38 PM" to "4/12/2021 12:45:13 PM." Even the Senate contractor's timeline contradicts itself because it states the scripts were started on "4/12/2021 1:39:38 PM," which is 54 minutes after their stated time when the scripts had run 330 times. They also stated that "330 older log entries were deleted via this method," which is proven false by the fact that events in the security log, as previously shown in *LOGS Image #3* above, were available for review.

On April 12, 2021, County elections staff began the process of shutting down the Dominion Democracy Suite 5.5-B application to prepare it for delivery to the Senate. This entailed shutting down SQL database services and other dependencies so Microsoft Server 2012r2 could shut down properly. It is County elections policy to require two people in the server room whenever someone is using the server room keyboard video monitor (KVM).

This video footage shows there was an additional staff member in the room at the time of CyFIR's claim. The server shut down process began at 12:41:06 p.m. Elections Department staff continued readying other tabulation equipment over the course of the few hours, when the server was eventually unracked, boxed, and packed up for delivery (see *LOGS Image #9 series*).

On 04/12/2021, after the Dominion EMS server was shut down, it was unplugged, unracked and packed into a box (at 5:01 p.m.) for delivery to the Arizona Senate. Then it was put onto a pallet to wait for shipment to the Arizona Senate.

Anonymous Logins

6.5.4 (Anonymous Logins)

CyFIR's "anonymous logins" claim is patently false. These logged actions are simply part of the EMS server protocols and standard Microsoft functions.

Response and Analysis

Cyber Ninjas' report and the presentation by Senate contractor, CyFIR, on September 24, 2021 included claims that an "anonymous user" accessed the EMS server. This is false. These logins were presented by CyFIR as evidence of potential nefarious actions, but an analysis of the security logs by an independent cybersecurity firm, PacketWatch, concluded these logins were legitimate and was part of typical behavior for a Microsoft Server 2012r2 (see *Exhibit - PACKETWATCH*).

Microsoft Server 2012r2 has several reasons it would legitimately log instances of "Anonymous Logon" events. CyFIR admitted this in Cyber Ninjas' report on page 82: "There are common functions in Microsoft Windows that will record an anonymous login activity into the windows." While Figure 21 on page 83 of Cyber Ninjas' report was redacted, the County reviewed an unredacted version which showed EMS logs from February 11, 2021 at 4:07:19 p.m. After reviewing the same logs from the County's cloned server, no log exists from the "Logon ID: 0x2ACBE," which would be unique to that event. The system tracks every task. Entries from that day do not include any logs during that time period (see *LOGS Image #10*).

LOGS Image #10 –Security Logs from February 10, 2021

Level	Date and Time	Source	Event ID	Task ...
Information	2/10/2021 4:50:25 PM	Microsoft Windows security auditing.	4624	Logon
Information	2/10/2021 4:50:22 PM	Microsoft Windows security auditing.	4624	Logon
Information	2/10/2021 4:50:20 PM	Microsoft Windows security auditing.	4624	Logon
Information	2/10/2021 4:50:20 PM	Microsoft Windows security auditing.	4624	Logon
Information	2/10/2021 4:50:20 PM	Microsoft Windows security auditing.	4624	Logon
Information	2/10/2021 4:50:20 PM	Microsoft Windows security auditing.	4624	Logon
Information	2/10/2021 4:50:19 PM	Microsoft Windows security auditing.	4624	Logon
Information	2/10/2021 4:50:19 PM	Microsoft Windows security auditing.	4624	Logon
Information	2/10/2021 4:50:18 PM	Microsoft Windows security auditing.	4624	Logon
Information	2/10/2021 3:21:46 PM	Microsoft Windows security auditing.	4624	Logon
Information	2/10/2021 3:21:44 PM	Microsoft Windows security auditing.	4624	Logon
Information	2/10/2021 3:21:44 PM	Microsoft Windows security auditing.	4624	Logon
Information	2/10/2021 3:21:27 PM	Microsoft Windows security auditing.	4624	Logon
Information	2/10/2021 3:21:27 PM	Microsoft Windows security auditing.	4624	Logon
Information	2/10/2021 3:21:27 PM	Microsoft Windows security auditing.	4624	Logon
Information	2/10/2021 3:21:27 PM	Microsoft Windows security auditing.	4624	Logon

Cyber Ninjas Report Figure 21: log from 4:07:19 PM does not exist.

(Above) Screenshot of security logs from the County's cloned server that show logs on February 10, 2021 during the time period of CyFIR's claim.

When reviewing this claim, the County also considered potential variances in CyFIR's computer time zone setting (3:07:19 p.m., 5:07:19 p.m., and 6:07:19 p.m.) and other events with similar matching times. The County found no matches for an Event ID 4624 with a Logon Type 3. The closest event was 86 minutes earlier at 3:21:27 p.m. The event ID matches and the network information that CyFIR claims is evidence of an "atypical anonymous logon" is also included. More detailed information is available in *LOGS Image #11*. This is a standard occurrence that Microsoft includes in its details, stating: "Workstation name is not always available and may be left blank in some cases."

LOGS Image #11 – Standard Microsoft Actions

Event 4624, Microsoft Windows security auditing.

General Details

An account was successfully logged on.

Subject:
Security ID: NULL SID
Account Name: -
Account Domain: -
Logon ID: 0x0

Logon Type: 3

Impersonation Level: Impersonation

New Logon:
Security ID: ANONYMOUS LOGON
Account Name: ANONYMOUS LOGON
Account Domain: NT AUTHORITY
Logon ID: 0x2A799
Logon GUID: {00000000-0000-0000-0000-000000000000}

Process Information:
Process ID: 0x0
Process Name: -

Network Information:
Workstation Name: -
Source Network Address: -
Source Port: -

Detailed Authentication Information:
Logon Process: NtLmSsp
Authentication Package: NTLM
Transited Services: -
Package Name (NTLM only): NTLM V1
Key Length: 0

This event is generated when a logon session is created. It is generated on the computer that was accessed.

The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a

The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network).

The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on.

The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases.

The impersonation level field indicates the extent to which a process in the logon session can impersonate.

The authentication information fields provide detailed information about this specific logon request.
- Logon GUID is a unique identifier that can be used to correlate this event with a KDC event.
- Transited services indicate which intermediate services have participated in this logon request.
- Package name indicates which sub-protocol was used among the NTLM protocols.
- Key length indicates the length of the generated session key. This will be 0 if no session key was requested.

(Above) Screenshot of the standard wording in a security log from February 10, 2021 at 3:21.27 p.m. See yellow highlighted text.

LOGS Image #12 – Credential Check After Logon

EMS Security Number of events: 36,587

Level	Date and Time	Source	Eve...	Task Category
Information	2/10/2021 3:21:44 PM	Microsoft Windows security auditing.	4648	Logon
Information	2/10/2021 3:21:44 PM	Microsoft Windows security auditing.	4776	Credential Validation
Information	2/10/2021 3:21:27 PM	Microsoft Windows security auditing.	4624	Logon
Information	2/10/2021 3:21:27 PM	Microsoft Windows security auditing.	4672	Special Logon
Information	2/10/2021 3:21:27 PM	Microsoft Windows security auditing.	4624	Logon
Information	2/10/2021 3:21:27 PM	Microsoft Windows security auditing.	4672	Special Logon
Information	2/10/2021 3:21:27 PM	Microsoft Windows security auditing.	4624	Logon

Event 4776, Microsoft Windows security auditing.

General Details

The computer attempted to validate the credentials for an account.

Authentication Package: MICROSOFT_AUTHENTICATION_PACKAGE_V1_0
Logon Account: emsadmin
Source Workstation: EMSSERVER
Error Code: 0x0

Log Name: Security
Source: Microsoft Windows security
Logged: 2/10/2021 3:21:44 PM
Event ID: 4776
Task Category: Credential Validation
Level: Information
Keywords: Audit Success
User: N/A
Computer: EMSSERVER
OpCode: Info
More Information: Event Log Online Help

(Above) Screenshot of the credential validation in a security log from February 10, 2021 at 3:21.44 p.m. See yellow highlighted entry.

It's common for a Microsoft Server 2012r2 to document these logs, and it is common for the workstation name to be left blank. Microsoft says it's an automated action where the EMS server is acting on behalf of the user.

What CyFIR claims is suspicious, can be explained, is typical for a Microsoft Server 2012r2, and is well documented online. The direct statement from Microsoft within the log file highlighted in *LOGS Image #11* should be enough for most cyber forensics companies to confirm this event as routine.

CyFIR also states there is a lack of authentication history following this type event. This is also false. Just 17 seconds after the event at 3:21.27 p.m., a credential validation attempt is logged under Event ID 4776 (see *LOGS Image #12*). Every Event ID 4624 with a Logon Type 3 had a similar 4776 credential validation event immediately afterward.

CyFIR provided an example of other Server 2012r2 servers not showing similar behavior for Logon types 3 and 10. This comparison has no weight because the Dominion EMS server uses additional configurations on Microsoft Server 2012r2, MSSQL and security settings. These settings are referred to as "hardening" scripts and they shore up SQL configurations, increase event logging in both Microsoft Server 2012r2 and Microsoft SQL Server. The hardening scripts also set specific values for registry items, administrative templates, group policy configurations and uses several ADMX toolkit options to enhance security protocols. All these scripts and configurations add to server behavior that would not be represented on other Microsoft Server 2012r2 servers unless they also had the scripts enabled.

Item #6: Election Management System & Its Air Gapped Network

(Cyber Ninjas Volume III Report Sections - 7.5.5 & 6.5.6)

Cyber Ninjas' report included six findings that made false and misleading claims about Maricopa County's tabulation system being connected to the internet.

Reference	Claim	County Analysis
Section 7.5.5 (Pg. 89)	"Internet Connections"	*False Claim* - The Election Management System's (EMS) network is 100% air gapped without external connection to the County network or the internet. This has been verified multiple times by qualified independent third-party vendors.
Section 6.5.6.2 (Pg. 89)	"Internet Connections to the EMS"	*False Claim* - The EMS server is only connected to the County's air gapped EMS network and the URLs referenced by CyFIR correspond to a Microsoft service that attempts to send reporting and error logs from Microsoft Visual Studio. These attempts fail to connect because of the air gapped system.
Section 6.5.6.3 (Pg. 89)	"Internet Connections to the EMS Client 1"	*False Claim* - EMS Client 1 and 2 are only connected to the EMS air gapped network. It was used to configure a printer via the built-in HTTP configuration portal from a web browser. The embedded wireless chip was disabled prior to system EAC certification, and it meets all current requirements.
Section 6.5.6.4 (Pg. 90)	"Internet Connections to the EMS Client 3"	
Section 6.5.6.5 (Pg. 90)	"Internet Connections to the REWEB 1601 System"	*Misleading Claims* - These are web servers that host the recorder.maricopa.gov website. This server legitimately connects to the internet. It is not connected to the EMS air gapped network.
Section 6.5.6.6 (Pg. 91)	"Internet Connections to the REGIS 1202 System"	

State & Federal Laws

The Help America Vote Act, a federal law, provides certification requirements for tabulation equipment, including security testing required to before equipment is certified. Arizona law requires counties follow federal guidelines on certification and additional requirements on maintaining the security and integrity of tabulation equipment. Additionally, the Arizona Elections Procedures Manual 2019 requires counties to follow security measure procedures for electronic voting systems (pages 95-100). Applicable Arizona laws include:

- A.R.S. § 16-442
- A.R.S. § 16-1004

Maricopa County Findings

Summary

Sections 7.5.5, 6.5.6.2, 6.5.6.3, 6.5.6.4, 6.5.6.5 & 6.5.6.6 (Internet Connections)

The Election Management System's network is 100% air gapped without external connection to the County network or the internet. This has been verified multiple times by qualified independent third-party vendors.

Response and Analysis

Maricopa County's air gapped network prevents the tabulation system from connecting to the internet. In February 2021, two sperate audits performed by independent certified Voting System Test Laboratories confirmed that the County's EMS air gapped network was not connected to the internet (see *Exhibit - PRO V&V AUDIT* and *Exhibit - SLI AUDIT*).

The claims made by CyFIR in Cyber Ninjas Volume III report and during the September 24, 2021, presentation about the County's tabulation equipment and internet access are false. CyFIR also made misleading statements that profess the website servers (REWEB1601 and REGIS1202) are connected to the Dominion EMS air gapped network. They are not. There is no communication between the website and the EMS air gapped network. CyFIR also said that while they reviewed the County's public statements on the topic, the County did not provide a network diagram. That document has been available to the public at JusttheFacts.Vote since July.

During the presentation, CyFIR uses the word "attempts" to describe the activities on the EMS server. A simple analysis of the EMS server, its accompanying U.S. Election Assistance Commission (EAC) certified installed applications, and corresponding logs explain these attempts and confirms that no internet connections occurred. This basic research and analysis would have better served the public to ensure only accurate information is provided. Furthermore, CyFIR's conclusion that the operating system had not been updated since the date of installation refutes their own claim the EMS ever had internet connectivity.

In October 2021, the County also hired PacketWatch, a cybersecurity and incident response firm. PacketWatch reviewed the County's air gapped network and confirmed it was not connected to the internet, documented in Sections 2 and 3 of the PacketWatch Audit Findings Report (see *Exhibit - PACKETWATCH*). PacketWatch confirmed what the County has stated. There are several technical indicators showing lack of internet connectivity:

- No Antivirus updates. AVAST was set to auto update.
- No Java updates. Java was set to auto update.
- Failed DNS requests. DNS was unable to resolve queries.
- No successful entries in the Network Connectivity Status Indicator (NCSI) log (see *NETWORK Image #5*). This log file records Microsoft Server performing automatic checks for internet connectivity.
- Internet Explorer Enhanced Security (IESC) was enabled. No websites were on the "Trusted Sites." This means any web page would be blocked unless that location was added to the "Trusted Sites."
- Log entries show the network traffic for EMS Client 1 and other devices is an attempt to reach out to the admin page of a Canon printer.
- The URLs https://go.microsoft.com "fwlink" and https://www.bing.com "SearchBox&Form" are identified by the default start page and default for the Internet Explorer search box. It is typical of a mistyped address being typed in the Internet Explorer search box with a redirect to bing.com as the resource was not resolved.
- Provided tables show many of the URLs listed were directed at hosts on the 192.168.100.X subnet. Host would be reachable by clients on the EMS network and could connect successfully even without internet connectivity.

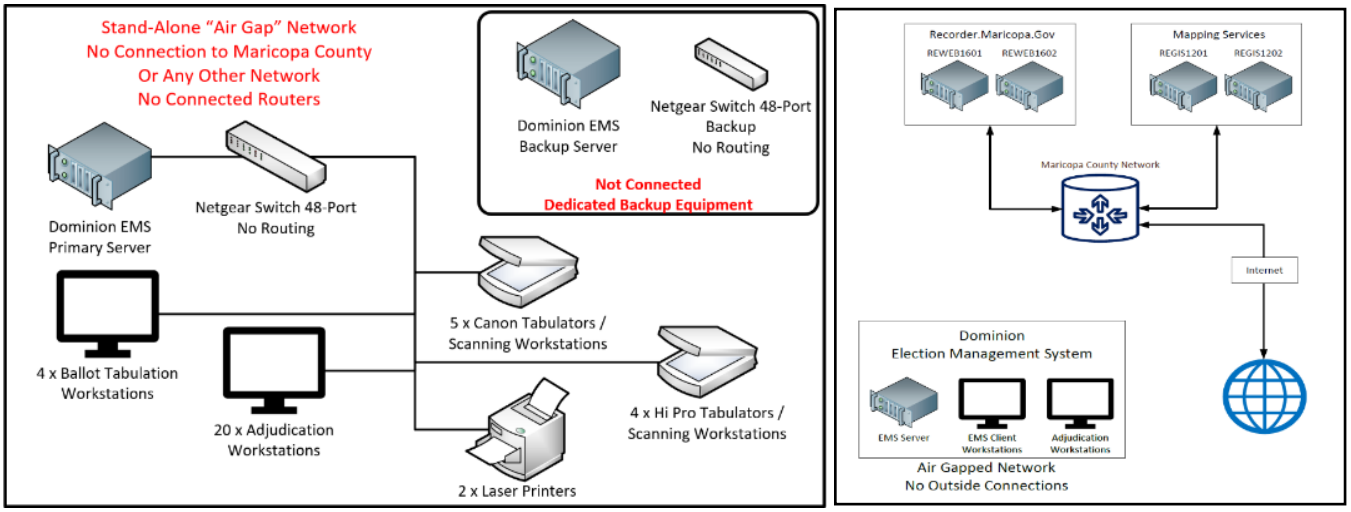
Below are further details about sections 7.5.5, 6.5.6.3, 6.5.6.4, 6.5.6.5 and 6.5.6.6.

Air Gapped Network

7.5.5 (Internet Connections)

To demonstrate the design of the air gapped network, we've included a series of diagrams describing the different components of the EMS network, which can only "speak" to each other within the network. It cannot access the internet or other County systems. This can be evidenced by the air gapped network's hard-wired lines visible through the glass windows into the County's Ballot Tabulation Center. The diagrams also demonstrate that the EMS network exists separately from the County's network at large, including the servers supporting webpages for the Recorder's Office and Elections Department's website.

NETWORK Image #1 – Screenshots Unique Security Log



(Left) A network diagram of the County's Election Management System air gapped network design with no connections to the internet. (Right) A network diagram of the Recorder's web servers, which shows a clear separation between the website and the tabulation equipment.

When CyFIR made the false claims about internet connectivity, they did not attempt to explain obvious and legitimate reasons why the EMS server may attempt to reach the internet. Because it's an air gapped network, none of these attempts ever reached the internet. The EMS Server has several log files that can be referenced to prove this statement. One of these logs is the Component-Based Services log (cbs.log) that records system activities, including those of SQL databases services and dependencies. Using copies of the same logs that were provided to the Senate, the cbs.log demonstrates multiple requests of the SQL Database Management Service (SQM) trying to upload logs to a Microsoft Server and receiving a failure message (see *NETWORK Table #1*). If the EMS server was connected to the internet, this log upload would not show failures since it uses standard opened ports to communicate to Microsoft. These attempts and corresponding failure messages once again demonstrate the integrity of the County's air gapped EMS network.

NETWORK Table #1 – Election Management System cbs.log from August 13, 2019	
Date	Entries
2019-08-13 02:36:32	Info CBS SQM: **Request upload of all unsent reports.**
2019-08-13 02:36:32	Info CBS SQM: **Failed to start upload with file pattern**: C:\Windows\servicing\sqm*_std.sqm, flags: 0x2 [HRESULT = 0x80004005 – E_FAIL]
2019-08-13 02:36:32	Info CBS SQM: Failed to start standard sample upload. [HRESULT = 0x80004005 – E_FAIL]
2019-08-13 02:36:32	Info CBS SQM: Failed to start upload with file pattern: C:\Windows\servicing\sqm*_all.sqm, flags: 0x6 [HRESULT = 0x80004005 – E_FAIL]
2019-08-13 02:36:32	Info CBS SQM: **Failed to start always sample upload.** [HRESULT = 0x80004005 - E_FAIL]
2019-08-13 02:36:32	Info CBS SQM: **Warning: Failed to upload all unsent reports.** [HRESULT = 0x80004005 - E_FAIL]

These processes and the log entries are explained in the Dominion Democracy Suite 5.5-B certified test plan publicly available on the U.S. Elections Assistance Commission website found in the Pro V&V Test Review from 2019 and 2018. To gain an understanding of the processes and log entries, CyFIR could have looked up copies of these documents. Instead of becoming familiar with the certified build of the Dominion Tabulation Equipment, CyFIR's inaccurate speculation in a public meeting led to misinformation on this topic.

NETWORK Image #2 – Screenshot of CyFIR Presentation

Process Name	Process File Path	Process ID	Dest IP	Dest Port	Whois
system	system	4	192.168.100.1	445	N/A Local Lan
avastsvc.exe	c:\program files\avast software\avast business\avastsvc.exe	320	23.194.212.49	80	Akamai
avastsvc.exe	c:\program files\avast software\avast business\avastsvc.exe	320	23.194.212.56	80	Akamai
svchost.exe	c:\windows\system32\svchost.exe	988	8.252.68.126	80	Level 3 Parent, LLC
svchost.exe	c:\windows\system32\svchost.exe	988	72.21.81.240	80	Edgecast
svchost.exe	c:\windows\system32\svchost.exe	988	13.107.4.50	80	Microsoft
svchost.exe	c:\windows\system32\svchost.exe	988	23.194.212.104	80	Akamai
svchost.exe	c:\windows\system32\svchost.exe	988	8.240.49.254	80	Level 3 Parent, LLC
svchost.exe	c:\windows\system32\svchost.exe	988	8.252.36.126	80	Level 3 Parent, LLC
svchost.exe	c:\windows\system32\svchost.exe	1272	64.4.54.254	443	Microsoft
svchost.exe	c:\windows\system32\svchost.exe	1272	52.137.106.217	443	Microsoft
svchost.exe	c:\windows\system32\svchost.exe	1272	20.72.205.209	443	Microsoft
jusched.exe	c:\program files (x86)\common files\java\java update\jusched.exe	4680	184.86.196.202	443	Akamai
avastemupdate.exe	c:\program files\avast software\avast business\avastemupdate.exe	8092	104.99.72.230	80	Akamai

(Above) A screenshot from CyFIR's September 24, 2021 presentation. The orange and green outlines were added for clarity by the County.

NETWORK Image #2 (above) is a screenshot from CyFIR's September 24, 2021, presentation that shows 13 separate processes as examples of the County's EMS server attempting to connect to the internet. In all instances, the

referenced process is a legitimate process as described in the certification documentation available on the EAC's website. None of the processes made a successful connection to the internet. Attempts are not considered proof of connection.

Outlined in orange on the first line of *NETWORK Image #2* is a process named "system." This system does not connect to the internet and is part of the internal local area network as indicated by the term "N/A Local Lan" in the far right column. While it's included on the list, CyFIR commented during its September 24, 2021 presentation that these are connection attempts from known applications and weren't successful in connecting to the internet.

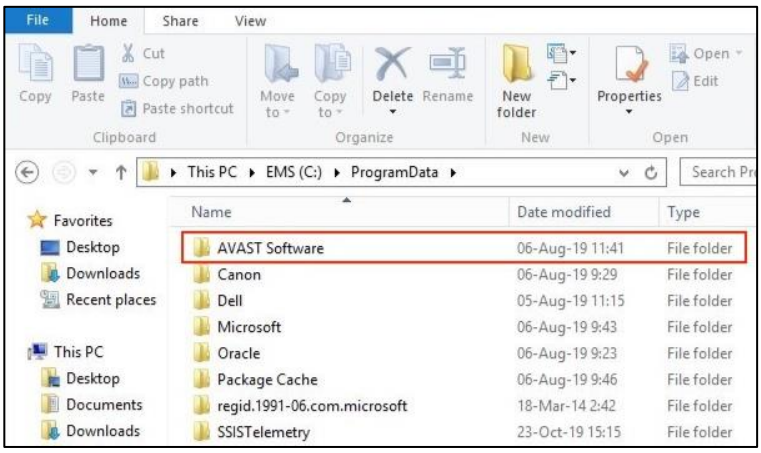
Another example from *NETWORK Image #2* is "avastsvc.exe" and "avastemupdate.exe" outlined in green. This is the EMS process that correlates to an EAC certified installed application, AVAST Antivirus. This system was installed on August 6, 2019, during the initial configuration of the primary Dominion EMS server.

Like most software, AVAST Antivirus attempts to connect to the internet to update itself. These attempts are written to the cbs.log, referenced in *NETWORK Image #2,* but all attempts failed because the County's EMS server is intentionally not connected to the internet due to the closed air gapped network design.

The other applications included in *NETWORK Image #2* behave similarly to the AVAST antivirus application. After the application is installed, it attempts to contact their vendor update servers through the internet but are met with a non-response due to lack of internet connectivity within the County's air gapped EMS network.

The Senate contractors confirmed this in Section 6.5.2.1.1 Software and Patch Management of their report when they stated "Neither the operating system nor the antivirus had been patched or updated since August 2019 (the date of the installation of the Democracy Suite)." With this statement, CyFIR contradicts their assertion that the Dominion EMS server was connected to the internet. If the EMS air gapped network environment facilitated internet connections, the AVAST virus definitions, the Microsoft Server 2012r2 operating system, and other installed applications would have successfully accessed the internet, been updated, and a record of that interaction would be visible in the cbs.log or other EMS logs (see *Exhibit - PACKETWATCH*). Because the County conforms to state law and EAC standards of operating an air gapped network, these attempts failed.

NETWORK Image #3 – Screenshot of AVAST Antivirus Installation



(Above) A screenshot from the EMS server showing the installation date for AVAST Antivirus.

EMS Server

6.5.6.2 (Internet Connections and the EMS Server)

Cyber Ninjas Volume III report was highly redacted, blacking out the support of their findings and the URL that CyFIR claims the server accessed multiple times on "02/02/2021." However, the redacted content is available for review in CyFIR's presentation to the Senate on September 24, 2021 (CyFIR presentation, slide 18).

NETWORK Image #4 – Screenshot of "Errormarker" URL

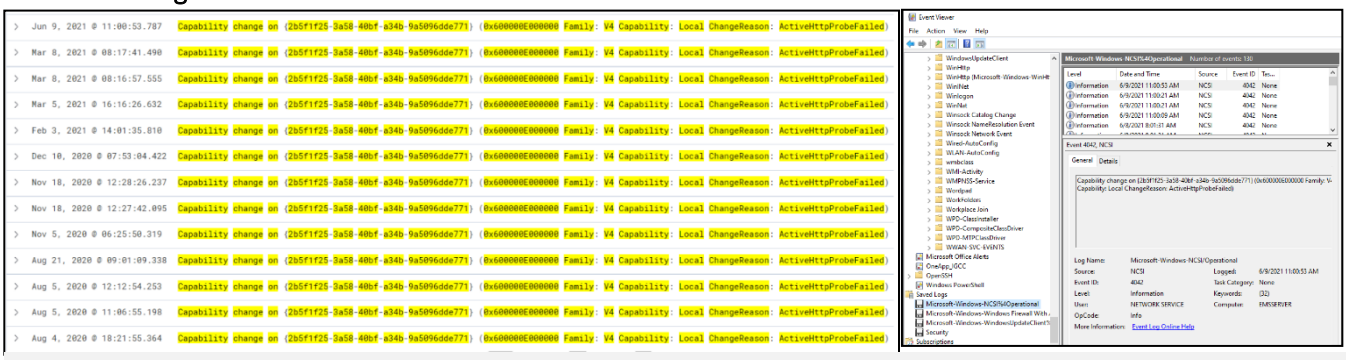
Date Visited [UTC]	Date Visited [Local]	Visits	URL
2021-02-02 00:17:30.906	2021-02-01 17:17:30.906	1	https://az700632.vo.msecnd.net/pub/ExtMgr/CompatList/CompatibilityList.xml.errormarker
2021-02-02 00:17:33.935	2021-02-01 17:17:33.935	2	https://az700632.vo.msecnd.net/pub/ExtMgr/CompatList/CompatibilityList.xml.errormarker

(Above) Slide 18 from the Senate contractor's presentation to the Arizona Senate on September 24, 2021 showing the "errormarker" URL.

In the presentation, CyFIR claims that this URL was accessed multiple times and was proof that the EMS server was able to reach the internet. The example URL they provided, ends with ".../CompatibilityList.xml.errormarker", which is an indication that an unsuccessful attempt was made. The URL would end in ".../CompatibilityList.xml" if a successful connection is made.

If internet connectivity had occurred, there would also be evidence captured in another Microsoft log, called NCSI Operational. On a server connected to the internet, there will be active pings asking for a response from various Microsoft services. Our review of the County's EMS server NCSI logs shows that these pings fail to connect because of the closed air gapped network (see *NETWORK Image #5*).

NETWORK Image #5 – Screenshot of "Errormarker" URL



((Above) Screenshot of the NCSI logs from the Dominion EMS server showing "ActiveHTTPProbeFailed" connection ping failed on multiple dates. (Right) Screenshot of the NCSI Event Viewer showing the Dominion EMS server "ActiveHTTPProbeFailed" connection ping failing on 6/9/2021.

EMS Workstations

6.5.6.3 & 6.5.6.4 (Internet Connections and the EMS Client 1 & 3 Workstations)

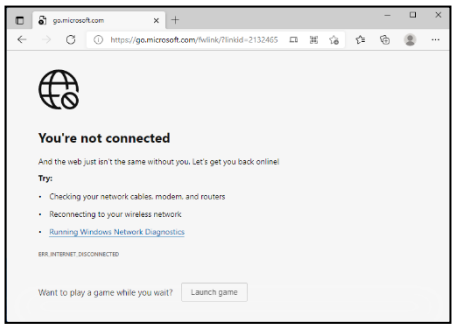
During the September 24, 2021, presentation to the Senate, CyFIR pointed out several URLs as an indication that the EMS client workstations #1 and #3 successfully connected to the internet (CyFIR presentation, slide 19). However, this is not evidence of a connection to the internet or a website. As with any system that uses Microsoft Windows or Edge, the default search engine is *bing.com*. If any operator opens the search function on the computer through the default Microsoft Edge web browser or the built-in Microsoft search functionality through Cortana Assistant, the system automatically logs an attempt to contact bing.com (see *NETWORK Image #6*). This is an indication of an attempted connection by Windows 10, which is part of the operating system's base functionality.

This is not evidence of nefarious intent to reach the internet by an internal bad actor either. In these instances, the attempt to contact *bing.com* failed. Microsoft Edge was part of the EAC certified build. Even though the equipment is not connected to the internet, when a user typed into the search bar on Edge or the start menu, the system defaults to searching that text string with the bing.com search engine. This is evident from the top screenshot highlighted in *Network Image #6*, which includes "SearchBox&FORM" within the URL. This bing search criteria is in the URL itself of "192.138.100.11". When the printer was initially configured, the IP address for the printer was mistyped with a 3 instead of a 6. This simple key stroke caused the Microsoft Edge browser to search for this mistyped IP address. Because of the air gapped system, this attempt failed to connect to the internet as demonstrated by *NETWORK Image #6*.

NETWORK Image #6 – Screenshot of EMS Client Logs & No Internet Connection

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=192.138.100.11&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

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



(Left) Screenshots from CyFIR's September 24, 2021 presentation to the Senate. (Top Left) EMS Client #1 workstation logs. (Bottom Left) EMS Client #3 workstation logs. (Right) A screenshot of Microsoft Edge search URL when the computer is not connected to the internet. The URL is the same "fwlink" as the images on the left.

CyFIR also indicated that EMS Client workstation #1 had significant interactions with a device using the internal IP address of 192.168.100.11 (see *NETWORK Image #7*). This is true. However, the delivery of this claim was misleading as it implied that this was an indication of internet connectivity. CyFIR said during the September 24, 2021 presentation that this was not an internet-based IP address and the IP scheme matched those of the EMS air gapped network (CyFIR presentation, slide 20).

NETWORK Image #7 – EMS Client Logs & Printer IP Address

Date Visited [UTC]	Date Visited [Local]	Visits	URL	User
10/30/2019 17:00:49	10/30/2019 10:00:49	2	http://192.168.100.11/p_preference.html	emsadmin01
10/30/2019 17:00:54	10/30/2019 10:00:54	2	http://192.168.100.11/m_network.html	emsadmin01
10/30/2019 17:00:58	10/30/2019 10:00:58	2	http://192.168.100.11/m_network_tcpip.html	emsadmin01
10/30/2019 17:01:46	10/30/2019 10:01:46	2	http://192.168.100.11/m_system.html	emsadmin01
10/30/2019 17:01:50	10/30/2019 10:01:50	2	http://192.168.100.11/m_security.html	emsadmin01
10/30/2019 17:02:02	10/30/2019 10:02:02	2	http://192.168.100.11/m_network_ethernet.html	emsadmin01
10/30/2019 17:02:46	10/30/2019 10:02:46	2	http://192.168.100.11/m_network_ipv4.html	emsadmin01
10/30/2019 17:03:38	10/30/2019 10:03:38	2	http://192.168.100.11/m_network_snmp.html	emsadmin01
10/30/2019 17:03:46	10/30/2019 10:03:46	2	http://192.168.100.11/m_network_port.html	emsadmin01
10/30/2019 17:03:51	10/30/2019 10:03:51	2	http://192.168.100.11/m_network_port_edit.html	emsadmin01
10/30/2019 17:04:00	10/30/2019 10:04:00	2	http://192.168.100.11/m_network_starttime.html	emsadmin01
10/30/2019 17:04:21	10/30/2019 10:04:21	2	http://192.168.100.11/m_network_wirelesslan.html	emsadmin01

(Left) Screenshot of EMS Client #1 workstation logs from CyFIR's September 24, 2021 presentation. (Right) Canon Image Class LBP6230dw Desktop LaserJet Printer.

The IP address shown to the left belongs with Canon Image Class LBP6230dw Desktop LaserJet Printer. This printer was connected and configured on the primary Dominion EMS server for several months before it was replaced by the MCTEC06 HP LaserJet printer. These printers are used to support routine operations like building ballots and printing daily reports or other needed information within the closed air gapped network (see *Network Image #1*).

NETWORK Image #8 – Printer Not Connected to Wireless Network

1.Product Information	
Product Name	LBP6230dw
2.Select Wired/Wireless LAN	
Select Wired/Wireless LAN	Wired LAN
3.Ethernet Driver Settings	
Auto Detect	Off
MAC Address	[redacted]
Communication Mode	Full Duplex
Ethernet Type	10BASE-T
4.TCP/IP Settings	
IPv4 Settings	
Auto Obtain	Off
Select Protocol	Off
Auto IP	Off
IP Address	192.168.100.11
Subnet Mask	[redacted]
Gateway Address	
5.Wireless LAN Settings	
MAC Address	–
SSID Settings	–
Security	WPA/WPA2-PSK
WPA/WPA2-PSK Settings	
Encryption for WPA/WPA2	Auto
Entry Format	ASCII (8-63 Char.)
WPA/WPA2-PSK	–
Wireless LAN Status	Inactive

(Above) Printer configuration scan from the 192.168.100.11 Canon network printer.

As with most printers, these printers host an internal IIS URL such as the http://192.168.100.11/portal_top.html. This URL is hosted exclusively by the printer itself and is used to configure printer features that aren't available from the front panel input on the printer. This URL configuration page is standard for all modern printers. CyFIR said that the URL, specifically "network_wirelesslan.html," was a source of concern because the County says there are no wireless networks connected to the EMS air gapped system. While the Canon printer has an embedded (non-removable) wireless card, the wireless configuration was disabled in the Canon system settings when it was set up. This means that the printer does not broadcast any wireless signals and is not connected to any wireless signals. It is disabled and serves no function. This conforms to the EAC standards of operating an air gapped network. An independent review of this printer by PacketWatch also concluded that the wireless on the printer is disabled and no signals are being broadcast (see *Exhibit - PACKETWATCH*)

CyFIR's reference to a wireless card that had been disabled since it was installed in 2019, is not evidence of internet connectivity or a security issue. If the EAC tabulation certification documentation was referenced by CyFIR during this analysis, they would have been able to identify a distinct pattern like this.

Elections & Mapping Website

6.5.6.5 & 6.5.6.6 (REWEB1601 & REGIS1202 Connected to the Internet)

The REWEB1601 and REWEB1202 are the servers that support Recorder.Maricopa.Gov, which hosts the official website of the Maricopa County Elections Department. These servers are not part of the air gapped EMS network, even though CyFIR incorrectly claimed they were during the September 24, 2021 presentation to the Senate (CyFIR presentation, slide 22). Both of these servers are indeed connected to the internet because they provide the public

access to the Recorder's Office and Elections Department website. Refer to *NETWORK Image #1* for a diagram of the web servers' relation to the EMS air gapped network.

- REWEB1601 - Resides on the Maricopa County network (MC Network) and is the website hosting server that provides County constituents access to the recorder.maricopa.gov website.
- REWEB1202 resides on the Maricopa County network (MC Network) and is the website hosting server that provides County constituents access to the Recorder.Maricopa.Gov/electionmaps website, among other pages that require mapping data. This server differs from REWEB1601 in that the primary purpose is to serve up Geographic Information System (GIS) content within the Recorder's Office websites such as maps, jurisdictional boundaries, etc.
- Both REWEB1601 and REWEB1202 have companion servers configured in a "load balanced" state. REWEB1602 and REWEB1201 are configured to help spread the load of the Recorder.Maricopa.Gov website and distribute traffic evenly. Clones of these load balancing servers were also provided to the Senate and the servers include the same data and perform the same function as REWEB1601 and REWEB1202 servers. However, CyFIR did not include these load balancing servers in Cyber Ninjas' report or CyFIR presentation.

Item #7: Hard Drives and Other Data

(Cyber Ninjas Volume III Report Sections – 6.5.5 & 7.6)

CyFIR included misleading claims about two hard drives on one computer used for adjudication and then made untrue claims that the second hard drive could have allowed this computer to access the internet. This is not true. While there were two hard drives, only one was connected to the EMS system. The second hard drive was not plugged into the computer, had no wireless card, was not connected to the EMS, and had no impact on tabulation.

Cyber Ninjas Volume III		County Analysis
Reference	Claim	
6.5.5 (pg. 84)	"Dual Boot System Discovered"	*Misleading Claim* – While there was a second hard drive on one computer, the drive was not powered on or used at any time while in Maricopa County's possession. This drive did not play a role in any Maricopa County election as it was not plugged into the computer, and therefore not operational.
7.6.1 (pg. 92)	"Election Data Found From Other States"	

Maricopa County Findings

Summary

6.5.5 (Dual Boot System), 7.6 (Election Data from Other States)

> **CyFIR misled the public when it claimed an inoperable hard drive could be connected to the internet. The second hard drive in an adjudication station was not connected to the computer and was never turned on or used by Maricopa County.**

A dual boot computer is a system that contains two hard drives (or partitions) with two independent operating systems installed on them. Further analysis of CyFIR's claims prove the "dual boot" claim was misleading. In the report, CyFIR claims that "...this system contained two bootable hard drives." CyFIR then goes onto mislead the public by speculating that these hard drives "could act as a '"jump box"' where one system could access the internet and the other system would be restricted to an isolated network." The evidence does not support this unsubstantiated speculation.

While CyFIR reported the existence of a second hard drive, they make no mention and provide no evidence that it was operational or capable of dual booting. During Maricopa County's audit performed by SLI Compliance in February 2021, the federally certified Voting System Test Laboratory confirmed the presence of this drive on an adjudication station labeled "ADJ-54." During the audit, the drive was photographed, and a forensic clone was created for analysis.

SLI Compliance determined that the drive was not plugged into the motherboard and that it was last used on July 31, 2019. This was prior to the tabulation equipment and this computer being delivered to the County in August 2019. SLI Compliance's analysis of the drive identified what appeared to be mock election data from different states. This information is not evidence of the drive being connected to the internet, but rather that this device, which was never used by Maricopa County, was previously used to test and demonstrate system functionality.

The presence of a second hard drive in a machine, although not standard, would not have posed a risk to the EMS air gapped network because the hard drive was not connected to the adjudication station and therefore not operational. SLI did not include this finding in the report because the drive was not connected and had no data from 2020.

Item #8: Cybersecurity Best Practices

(Cyber Ninjas Report Volume III Sections – 6.5.2, 6.5.2.1.1, 6.5.2.1.3 & 6.5.2.1.4)

Cyber Ninjas' report and the presentation by Senate contractor, CyFIR, on September 24, 2021 included four misleading claims about the County's adherence with cybersecurity best practices. The inclusion of some of these claims and recommendations demonstrate CyFIR's misunderstanding of how cybersecurity best practices are implemented and managed for closed network, air gapped, election systems.

Reference	Claim	County Analysis
Section 6.5.2 (Pg. 75)	"Failure to Follow Basic Cyber Security Practices"	*Misleading Claims:* None of these suggestions are applicable in an air gapped network without internet connection. Some of the best practices that CyFIR recommends could introduce security and operational vulnerabilities into the closed network Election Management System (EMS).
Section 6.5.2.1.1 (Pg 75)	"Software and Patch Management"	
Section 6.5.2.1.3 (Pg. 76)	"Credential Management"	
Section 6.5.2.1.4 (Pg. 78)	"Lack of Baseline for Host and Network Activity"	

State & Federal Laws

The Help America Vote Act, a federal law, provides certification requirements for tabulation equipment, including security testing required before equipment is certified. Arizona law requires counties follow federal guidelines on certification and additional requirements on maintaining the security and integrity of tabulation equipment. Additionally, the Arizona Elections Procedures Manual 2019 requires counties to follow security measure procedures for electronic voting systems (pages 95-100). Applicable Arizona laws include:

- A.R.S. § 16-442
- A.R.S. § 16-1004(B)

Maricopa County Findings

Summary

6.5.2 (Basic Cybersecurity), 6.5.2.1.1 (Software and Patch Management) & 6.5.2.1.4 (Network Activity)

> **The equipment has the latest U.S. Election Assistance Commission (EAC) approved software and patches installed. The EAC requires that any software and security updates to tabulation equipment must first be authorized by the tabulation vendor and thoroughly tested. The updates listed in the Senate presentation are part of the federally certified "trusted build" that must be installed during set up.**

Response and Analysis

CyFIR reported that the County installed Dominion Election Management System does not follow Cybersecurity and Infrastructure Agency (CISA) guidelines for software and patch management. In Cyber Ninjas report, they quote, CISA:

"Failure to deploy patches in a timely manner can make an organization a target of opportunity." CyFIR cites recommendations from CISA to patch systems and ensure that antivirus definitions are up to date. While these are great recommendations for normal computer systems that the County already follows, these are not considered best practice for air gapped election systems.

Maricopa County is a member of CISA's Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC), and CISA is a critical partner to Maricopa County in ensuring cyber and physical security of our elections. However, this recommendation repeated by CyFIR is taken out of context when it is intended to apply to enterprise networks where many users can access multiple systems, not as a best practice for closed, air gapped election management systems. CISA coordinates with various federal partners to develop resources for state and local governments, including the U.S. Election Assistance Commission (EAC) for election administration and National Institute of Standards and Technology (NIST) for election infrastructure security best practices, to which Maricopa County's practices adhere.

The County follows all EAC guidelines for tabulation equipment as required by state law. The EAC's Testing & Certification Program (Version 2.0, Section(s) 1.16, 3.42, 3.43) requires that any software and security updates to tabulation equipment must first be authorized by the tabulation vendor and thoroughly tested by federally certified Voting System Test Laboratories. If the County were to implement a software or security update without it being tested and approved by the EAC, the County's tabulation equipment would lose its federal and state certification. **This is not only a requirement, but it is also a best practice to thoroughly test software patches prior to implementation to ensure that each update does not pose a risk to the tabulation system.**

Credential Management

On page 75, CyFIR also misunderstands the EAC certification process by claiming that because "4 EXE packages were created, 45 EXE packages were updated and/or modified, 377 Dynamic Link Libraries (DLL) were created, and 1053 Dynamic Link Libraries were modified on the EMS server" after the Dominion software was installed in August 2019, that those updates "would have invalidated the voting certification."

The inclusion of this claim demonstrates a lack of understanding of the EAC certification process. When readying the Dominion EMS hardware (Dell 2U Server) for use, the County and Dominion installed EAC certified patches for the Microsoft Server 2012r2 package. CyFIR's claims are not true and are easily refuted by the review of the Dominion Democracy Suite 5.5 EAC application that outlines all actions and software currently found on the Dominion EMS.

All patching or updates were performed manually on the EMS Server in accordance with EAC certification requirements. In *CYBERSECURITY Table #1* below, all patches have associations with Microsoft services from SQL Databases to Microsoft Visual Studio. As shown in the EAC Certification Testing Plan, this is an EAC certified software program approved for use with the Dominion Democracy Suite 5.5-B. All patches were completed in 2019 on August 5 and 6, when the County was initially setting up the server. No subsequent patches were applied after final certification.

CYBERSECURITY Table #1 – Patch Analysis			
Server Patch	Patch On EMS Server	EAC Certified Patch Description	Patch Release Date
KB4505221	08/06/2019	Service Pack 1 for Microsoft SQL Server Browser included in Security Update for SQL Server 2016 Service Pack 1 CU	7/02/2019

CYBERSECURITY Table #1 – Patch Analysis			
Server Patch	Patch On EMS Server	EAC Certified Patch Description	Patch Release Date
KB3182545	08/06/2019	SQL Server 2016 Service Pack 1 on Microsoft SQL Server 2016	11/15/2016
KB2565063	08/06/2019	Security Update for Microsoft Visual C++ 2010 Service Pack 1 Redistributable Package on Microsoft Visual C++ 2010	4/04/2012
KB3095681	08/06/2019	Update for Microsoft Visual Studio 2015 on Microsoft Visual Studio 2015	10/08/2015
KB3182545	08/06/2019	Service Pack 1 for Microsoft SQL Server VSS Writer included in SQL Server 2016 Service Pack 1 on Microsoft SQL Server 2016	11/15/2016
KB4507005	08/05/2019	Security Update for Microsoft .NET Framework 3.5 on Microsoft Server 2012r2 for x64-based Systems	7/08/2015
KB3127222	08/05/2019		2/07/2015
KB3097992	08/05/2019		11/09/2015
KB3074545	08/05/2019		9/04/2015
KB3072307	08/05/2019		8/10/2015
KB3037576	08/05/2019		4/13/2015
KB3023219	08/05/2019		5/11/2015
KB2973114	08/05/2019		9/08/2014
KB2972213	08/05/2019		9/08/2014
KB2972103	08/05/2019		10/13/2014
KB2968296	08/05/2019		10/13/2014
KB2966828	08/05/2019		10/07/2014
KB2966826	08/05/2019		08/12/2014
KB2894852	08/05/2019		09/09/2014

Microsoft Server 2012r2 has a service called "Features on Demand (FOD)," where installed services or dependencies for SQL server and other services were turned on for the machine. It is standard practice for Voting Systems to push an installation image with SQL services *after* initial setup. The patches, service packs and additional items installed on August 5-6, 2019 were related to the initialization of Microsoft SQL servers. Consistent with the Dominion EMS configuration process, the County's SQL server was configured and software and related patches were installed after the initial EAC certified Microsoft Server 2012r2 was delivered to the County. The SQL server needed several 2019 EAC certified patches installed to operate as approved and tested during the EAC certification process. The County and Dominion did not make any additional updates or changes that were not included in the 2019 EAC Certification testing plan.

These configuration and installation processes are explained in the Dominion Democracy Suite 5.5-B certified test plan publicly available on the EAC website found in the Pro V&V Test Review from 2019 and 2018.

In October 2021, the County hired PacketWatch, a cybersecurity and incident response firm. They reviewed the County's EMS system (see *Exhibit - PACKETWATCH*). PacketWatch is familiar with and recognizes the need for best practices guidelines from CISA and found that these are guidelines, not absolutes. PacketWatch asserts the EMS network is a purpose-built network meant to allow communication between the necessary components to facilitate ballot tabulation and adjudication. Given the rigid certification levels and requirement to review all changes, it is expected the software levels would be static until such time as an update window is scheduled for EAC certification. Regular patching would not be expected on this network while being used to facilitate an election.

Network Activity

CyFIR claims that the County's EMS does not have whitelisting, monitoring, baselining, or network programs that could have been used to establish a baseline for host and network activity. CISA recommends that counties leverage software and monitoring functions to establish and enforce a software and a network baseline of approved programs, communications protocols, and communications devices for voting systems. These suggestions would be valid and necessary for systems that are connected to the internet and outside an air gapped network.

The County's EMS air gapped network consists of equipment and applications approved and certified by the EAC. There is no other monitoring function or software unless approved in a future EAC certification. The monitoring in the Ballot Tabulation Center (BTC) is accomplished in many ways. Multi-factor authentication, live video feeds, building access logs, Arizona Secretary of State mandated logic and accuracy test before and after every election, and an internal post-election logic and accuracy test.

Summary

6.5.2.1.3 (Credential Management)

Maricopa County has a robust set of physical security controls to prevent unauthorized access to the tabulation equipment, including controlled restricted access and security cameras. 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. Observers are present during tabulation and all totals are reconciled at the end of each shift.

On page 76 of Cyber Ninjas' Volume III report, CyFIR claims that the County "*violates every principle of password management guideline as published in every cyber security framework that currently exists.*" This is misleading as the County has implemented a robust set of security controls for restricting access to the tabulation system, managing credentials, and monitoring user access. Before any of the County ballot tabulation staff enters the BTC to work at their assigned stations, they must go through several security checks.

1. The BTC is in a secure building that requires authorized badge access and is monitored by Maricopa County Security Services. Both inside and outside, the building has 24/7 surveillance cameras also monitored by security services. While ballots are onsite at the Maricopa County Tabulation and Elections Center (MCTEC) the County has 24/7 physical security officers monitoring cameras, doors, and performing employee badge checks.
2. Once in the building, higher level badge access is required for any door leading into the BTC. This elevated badge access is only provided to designated staff with a business need to enter. Badge access into the BTC and surveillance cameras are also monitored by security services.
3. Along with the surveillance system cameras inside and outside MCTEC, the County live streams all access points into the BTC on its website 24/7.
4. All the central count tabulation equipment is within the BTC, which requires authorized, elevated badge access to enter. Only those whose jobs require them to be in the BTC have this level of access. Within the BTC is another room that holds the EMS servers. This is a glass room that requires elite-level badge access to enter. Only a few of

the most senior election officials have this access. The glass tabulation server room is also live steamed on the County's website and onsite security officers are monitoring who comes in and out of the server room.

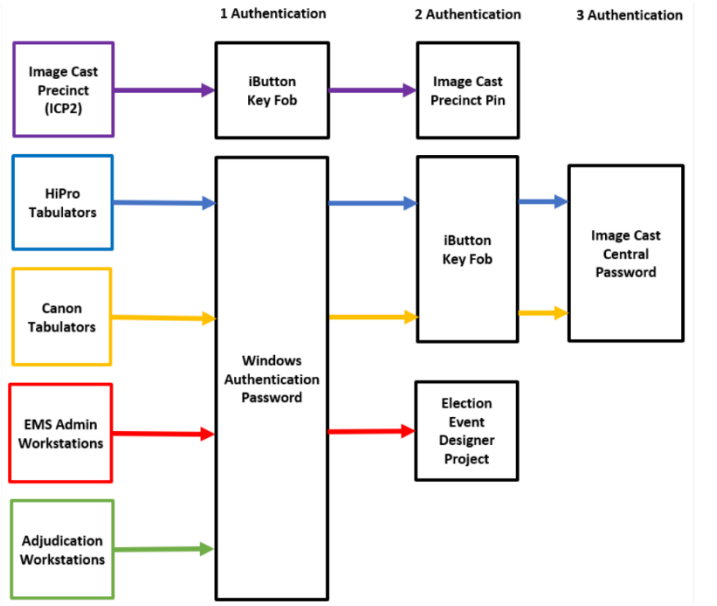
5. In addition, ballots are only tabulated when political party observers are present. Tabulation staff and political party observers perform a reconciliation of total ballots tabulated before and after each shift by comparing and confirming the totals on the tabulator screens to the totals collected in the previous shift. This process independently validates that ballots are only counted when political party appointees are observing the process.

CyFIR claimed during its September 24, 2021 presentation that the County's precinct-based tabulators (ICP2) — used to count ballots in voting locations on Election Day — are the only systems that require additional passwords and authentication beyond the shared Windows password. This is not true. The tabulators in the BTC (HiPro and Canon), used to tabulate all 1,915,487 early ballots during the 2020 General Election require the following three forms of authentication to gain access to the tabulators and Image Cast Central (ICC) program.

1. Windows Login Authentication password
2. iButton Key Fob two-factor authentication (2FA)
3. The program ICC password

The EMS workstations running the Election Event Designer and used to create the official certified results, also have more than one form of authentication for access. The EMS workstations use two forms of authentication, Windows login and the project password to the EED (Election Event Designer) to gain access.

CYBERSECURITY Image #1 – Tabulation Credential Management



(Above) The County's credential and multi-form factor design for the programs and equipment in the BTC, showing each device and its authentication steps.

CyFIR also claims that the passwords for the EMS were not changed since the system was setup in August of 2019. This claim is misleading and untrue.

Prior to every election, the County changes the Election Event Designer Project password, Precinct Based Tabulator Password, and the Image Cast Central passwords. These frequently updated passwords are required to tabulate ballots, run reports, and generate results.

CyFIR also claims that the usernames and accounts of these systems were not assigned to specific individuals but were shared between various people. The County has implemented many security measures that function similar to how a password functions for credential management and logging system access. Tabulation staff have many layers of physical security to enter the BTC. This includes restricted badge access that logs when staff enter the BTC. Staff members must also use an iButton Security Key Fob in addition to their system password to log into a tabulator. The iButton Key Fob is a password in a physical form. Determining which tabulation staff member was logged into a tabulator can be verified by reviewing paper tabulation operator logs and also by video time stamps. These two external sources of information can be matched with system generated logs to determine who was operating or using a tabulator at any point during the election.

The PacketWatch review states the software requires matching accounts on both the Microsoft Server resources and the Democracy Suite tools and services. Since access to the network is closed to outside resources and access to the BTC is controlled and monitored, it is understandable why Maricopa County chose to use generic accounts and passwords (see *Exhibit - PACKETWATCH*).

Item #9: Voters that Moved & Soft Matching Techniques

(Cyber Ninjas Report Sections - 5.3.1, 5.4.2, 5.5.3, 5.5.4)

Cyber Ninjas' report includes five claims based on their use of a third-party commercial database that resulted in claims that voters may have illegally voted because they moved prior to or during the election cycle. Our analysis found that the report's conclusions are contradicted by actual records in the County Recorder's Voter Registration Database.

Cyber Ninjas Volume III			County Analysis
Reference	Claim	Ballots	
5.3.1 (pg. 6)	"Mail-in Ballot Voted from Prior Address"	23,344	0
5.4.2 (pg. 10)	"Voters that Potentially Voted in Multiple Counties"	5,295	5
5.5.3 (pg. 14)	"In-Person Voters Who Had Moved Out of Maricopa County"	2,382	0
5.5.4 (pg. 16)	"Voters Moved Out-of-State During 29-day Period Preceding Election"	2,081	0
Total(s)		33,102	5
5.7.9 (pg. 56)	"No Record of Voters in Commercial Database"	N/A	Inaccurate Claim

State & Federal Laws

For decades, federal and state laws have recognized that voters move, and these laws provide protection so that voters can still lawfully cast a ballot when relocating prior to or during an election. The Federal Government passed the 1993 National Voter Registration Act (NVRA), which allows voters to move between jurisdictions and states during an election cycle. It affords those voters the right to cast a ballot for president from their prior residence if they missed the registration deadline in their new residence. The Federal Government also recognized that voters may need to vote absentee, and this allowance ensures residents who live out of their state of residence while serving in the military (1986 Uniformed and Overseas Citizens and Absentee Voting Act - UOCAVA) retain their right to vote. Arizona law outlines the restrictions about voter eligibility when they move and penalties for voting more than once. Applicable Arizona laws include:

- A.R.S. § 16-135 (B)(E)
- A.R.S. § 16-1016
- A.R.S. § 16-547

Maricopa County Findings

Summary

5.3.1 (Mail-in Ballot Voted from Prior Address), 5.4.2 (Voted in Multiple Counties), 5.5.3 (Moved Out of County), 5.5.4 (Moved Out-of-State), & 5.7.9 (Commercial Database)

> **Faulty data analysis and lack of understanding of federal and state laws appear to have resulted in Cyber Ninjas incorrectly claiming thousands of legally registered voters may have cast ballots illegally.**

Response and Analysis

Cyber Ninjas' report included six data sets of voters identified through limited or soft matching techniques (three data points used to identify the voter, such as first name, last name, and birth year) as support for their claim(s) that some

Maricopa County voters potentially voted illegally because the voters had moved prior to or during the election cycle. Cyber Ninjas also included a seventh data set that used soft matching to identify voters who may have voted in multiple Arizona counties. The flaw in relying on soft matches is obvious: many people share the same data points of first name, last name, and birth year. For example: there might be a "John Smith" who was born in 1976 who moved out of the county prior to the election cycle, but that does not mean that there was not another "John Smith" who was also born in 1976 who lived in the County and lawfully cast a ballot in the County's election.

Cyber Ninjas' soft matches used three data points: last name, first initial and year of birth. In a County with more than 4 million people, this is clearly not sufficient. In one case for example they identified twins as the same voter. In the County's review of Cyber Ninjas' dataset, we used matching criteria that included: full name (first, middle, last), full date of birth, Social Security number (4 digits), Arizona Driver License or state issued ID, residential history, signature and in some cases we had the voter's occupation and the father's last name or the mother's maiden name.

The County reviewed voters from these seven data sets and found that the methodologies and claims were inaccurate. In Maricopa County, as with election administrators statewide, we rely on the voter's affirmation of their residential address until we are informed otherwise by the voter or by another trusted resource like the United States Postal Service (USPS) or the National Change of Address (NCOA) report. Even these trusted sources can have errors, and that is why the County is legally required to send voters identified in these "official" resources two separate official, non-forwardable pieces of mail to allow the voter to confirm if they have actually moved. A real-time database that tracks the day-by-day movements and residency changes of every person in the state or in the nation does not exist and, by law, no voter can be denied their right to vote because their information may not be correctly listed in a database of individuals who have supposedly relocated.

The analysis that Cyber Ninjas performed relied on the use of a third-party commercial database. The combination of the use of this commercial database and the soft matching techniques are likely a key reason Cyber Ninjas made incorrect conclusions. In findings below, we found many other problems with Cyber Ninjas' methodology and conclusions. Below is a detailed review of the information analyzed.

23,344 Ballots

5.3.1 (Mail-in Ballot Voted from Prior Address)

Within this category, Cyber Ninjas provided three separate data sets in Appendices B1, B2 and B3. Out of the 23,344 voters that Cyber Ninjas identified as having moved to a new address, we found no occurrences of a voter voting more than one ballot. We did find 1,256 of the addresses Cyber Ninjas used from the third-party data set were U.S. Post Office Boxes (P.O. Box). It is not possible for a voter to move to a P.O. Box. The Elections Department uses the residential address to determine residency and the opening of a P.O. Box is not an indicator that would warrant an individual being removed from the voter rolls or that they have moved (see *Exhibit – PO BOX*).

There are also 1,331 Uniformed and Overseas Citizens and Absentee Voting Act (UOCAVA) voters who were included in Cyber Ninjas' data sets. These voters live outside of Maricopa County and may have submitted an address change with the U.S. Postal Service (USPS). Despite living at an address in another state or outside the United States, these military and overseas voters are legally allowed to maintain registration status at their last known address and are legally allowed to vote in Maricopa County under laws within the 1993 National Voter Registration Act.

It is also not uncommon for only some occupants (e.g., family members, divorced couples, roommates) of a residence to move, while others continue to live at that address. In these instances when the occupants that move submit an address

change with USPS, it is not uncommon for the registered voters that did not move to be incorrectly flagged as moving by the USPS or other commercial databases. This, then, produces a "false positive" indicating that voters have moved when, in fact, they did not.

These three situations are obvious problems with Cyber Ninjas' analysis and should have been an indicator that any conclusions drawn from this data would be faulty. This is also why the County is legally required to rely on the voter's signed affidavit informing us of their legal residence for voting purposes. The breakdown of Cyber Ninjas' 23,344 impacted ballots claim comprised of the three following data sets:

15,035 Ballots

5.3.1– Cyber Ninjas Appendix B1 (Voters Who Moved within Maricopa County)

When an already registered voter moves within his or her county prior to, during and after an election, state law dictates the voter is still registered and eligible to vote in that county. We conducted an analysis of the B1 data set from Cyber Ninjas (see *Exhibit – B1 ANALYSIS*). None of the scenarios described in the summary of our analysis below would automatically disqualify a voter from participating in the 2020 General Election. The Maricopa County Recorder's Office Voter Registration Database shows the following:

- 7,866 voters have a change of address prior to the court-ruled voter registration cutoff of 10/15/2020. In some of these cases, Cyber Ninjas data showed the voter moved several years or a decade prior to the cutoff. However, our records show the voters' address had changed much more recently. In all instances, the updated address is within Maricopa County. These voters are legally allowed to cast a ballot in Maricopa County.
- 5,512 voters with no record of submitting an address change. As required by law, Maricopa County relies on the voter attestation of a move or a trusted source (like USPS or the NCOA report) when updating voter registration information. These voters were likely incorrectly identified due to the soft matching techniques used by Cyber Ninjas.
- 1,096 voters who submitted an address change, but after the 10/15/2020 voter registration cutoff. Voters are allowed to move during or after the election cycle. In all instances, the updated address is within Maricopa County. These voters are legally allowed to cast a ballot in Maricopa County.
- 435 UOCAVA voters registered at an address in Maricopa County but are living elsewhere. This is a requirement under federal law to establish residency. The ballot is not mailed to the Maricopa County address. Instead, a separate process guided under law is used. These voters are legally allowed to cast a ballot in Maricopa County.
- 108 voters who have a cancelled record due to a death, move, voter request or other. In all instances the change occurred after the November 2020 General Election except for one. A deeper analysis of that one record shows the voter returned the ballot on 10/10/2020. A review of the signature shows deterioration from the August 2020 Primary Election affidavit envelope signature, but it is a match. The County received notification from the Arizona Secretary of State's Office that the voter died on 10/27/2020. Arizona has no law deeming the ballot invalid if the voter voted and returned their early ballot before their death but passed away before Election Day.
- 18 voters who had a cancelled record because the Arizona Secretary of State identified a duplicate record and merged the record into a single voter registration record. In all of these cases, only one ballot was cast by each voter.

We've completed a deeper review of a random sample of 982 records from the 15,035 offered by Cyber Ninjas (see *Exhibit – B1 DETAILED REVIEW*). The review included a seven-point "hard match" check of the voter's full name, address, full date of birth, social security number, voter ID, voting history, and signature with official records, which is obviously much more reliable than a "soft match" check as used by Cyber Ninjas. Our review did not find any voter ineligible to vote from their residential address during the November 2020 General Election and found no evidence of double voting.

6,591 Ballots

5.3.1– Cyber Ninjas Appendix B2 (Voters Who Moved out of Arizona)

We conducted an analysis of the B2 data set from Cyber Ninjas (see *Exhibit – B2 ANALYSIS*). None of the scenarios described in the summary of our analysis below would automatically disqualify a voter from participating in the 2020 General Election. The Maricopa County Recorder's Office Voter Registration Database shows the following:

- 2,801 voters with no record of submitting an address change. As required by law, Maricopa County relies on the voter attestation of a move or a trusted source when updating voter information. These voters were likely incorrectly identified due to the soft matching techniques used by Cyber Ninjas.
- 2,686 voters who have a change of address prior to the court-ruled voter registration cutoff of 10/15/2020. Cyber Ninjas' data showed the voter moved out of Arizona, but in all instances, the voter's updated address was within Maricopa County. These voters are legally allowed to cast a ballot in Maricopa County.
- 847 UOCAVA voters registered at an address in Maricopa County but are living elsewhere. This is a requirement under federal law to establish residency. The ballot is not mailed to the Maricopa County address. Instead, a separate process guided under law is used.
- 134 voters who have a cancelled record due to a death, move, voter request or other. In all instances the event occurred after the 2020 General Election.
- 121 voters who submitted an address change, but after the 10/15/2020 voter registration cutoff. Cyber Ninjas' data showed the voter moved out of Arizona, but in all instances, the voter's updated address was within Maricopa County. These voters are legally allowed to cast a ballot in Maricopa County.
- 2 voters who had a cancelled record because the Arizona Secretary of State identified a duplicate record and merged the record into a single voter registration record. In both cases, only one ballot was cast by each voter.

1,718 Ballots

5.3.1– Cyber Ninjas Appendix B3 (Voters Who Moved within Arizona but out of Maricopa County)

We conducted an analysis of the B3 data set from Cyber Ninjas (see *Exhibit – B3 ANALYSIS*). None of the scenarios described in the summary of our analysis below would automatically disqualify a voter from participating in the 2020 General Election. The Maricopa County Recorder's Office Voter Registration Database shows the following:

- 631 voters with no record of submitting an address change. As required by law, Maricopa County relies on the voter attestation of a move or a trusted source when updating voter information. These voters were likely incorrectly identified due to the soft matching techniques used by Cyber Ninjas.
- 513 voters who have a change of address prior to the cutoff. Cyber Ninjas data showed the voter moved to another Arizona county, but in all instances, the voter's updated address was within Maricopa County. These voters are legally allowed to cast a ballot in Maricopa County.

- 369 voters who have a cancelled record due to a death, move, voter request or other. In all instances the event occurred after 10/15/2020.
- 79 voters who submitted an address change:
    - 34 voters moved within the county after the 10/15/2020 voter registration cutoff. Cyber Ninjas data showed the voter moved to another Arizona county, but in all instances, the voter's updated address was within Maricopa County. These voters were eligible to vote in Maricopa County for the General Election.
    - 43 voters moved out of the county after the 2020 General Election. These voters were eligible to vote in Maricopa County for the General Election.
    - 2 voters moved out of the County after the 10/15/2020 voter registration cutoff. Federal law provides additional protections for voters that move during an election cycle. These voters were eligible to vote in Maricopa County for the General Election.
- 77 voters who had a cancelled record because the Arizona Secretary of State systematically identified a duplicate record and merged the record into a single voter registration record. In all cases, only one ballot was cast by each voter.
- 49 UOCAVA voters registered at an address in Maricopa County but are living elsewhere. This is a requirement under federal law to establish residency. The ballot is not mailed to the Maricopa County address. Instead, a separate process guided under law is used.

We completed a deeper review of a random sample of 242 records from the 1,718 offered by Cyber Ninjas (see *Exhibit – B3 DETAILED REVIEW*). The review included a seven-point check of the voter's full name, address, full date of birth, social security number, voter ID, voting history, and signature with official historical records. Our review did not find any voter ineligible to vote from their residential address during the November 2020 General Election and found no evidence of double voting. Below are the results of our detailed review of 242 records:

- 195 records are still active registered voters that have not informed the Maricopa County Recorder's Office of a move. In addition, the County has not received returned official election mail. We confirmed only one ballot was cast per voter and that each voter was eligible for the November 2020 General Election.
- 40 records have been cancelled due to a move, felony conviction, or other voter registration file update that occurred after the election. We confirmed only one ballot was cast per voter and that each voter was eligible for the 2020 General Election.
- 7 voters have moved from active status to inactive status since the November 2020 General Election due to the County receiving a returned piece of official election mail. We confirmed only one ballot was cast per voter and that each voter was eligible for the 2020 General Election. It is important to note voters in inactive status may still be qualified electors upon confirmation of their residency.

5,295 Ballots

5.4.2 – Cyber Ninjas' Appendix D1 (Voters that Potentially Voted in Multiple Counties)

Cyber Ninjas' analysis used soft or partial matching criteria, which resulted in false duplicates statewide. Over 3.4 million registered voters participated in the November 2020 General Election in Arizona. For a true analysis, a hard match comparison of all voter information such as full date of birth, middle name, social security and driver license numbers should have been used.

We've completed a detailed review of 1,815 of the 5,295 voters that Cyber Ninjas' identified as potentially voting in more than one county (see *Exhibit - D1 DETAILED REVIEW*). We determined that Cyber Ninjas incorrectly identified 1,810 voters due to soft data matching practices. When using additional data points such as full date of birth or social security numbers, we confirmed that these voters were two separate people. However, we did find five potential instances of double voting. The five cases have been turned over to the Arizona Attorney General's Office for further review. It is very rare that a voter would be able to have more than one in-state active voter registration record, but it could occur if a voter registered many decades ago and the older record does not have a sufficient amount of data points to result in a hard match if they register in another county.

2,081 Ballots

5.5.4 – Cyber Ninjas' Appendix I1 (Voters that moved Out-of-State During 29-Day Period Preceding Election)

Cyber Ninjas' analysis used soft or partial matching criteria, which resulted in false duplicates statewide. Over 3.4 million registered voters participated in the November 2020 General Election in Arizona. For a true analysis, a hard match comparison of all voter information such as full date of birth, middle name, social security and driver license numbers should have been used.

We completed a detailed review on a random sample of 644 records from Cyber Ninjas' data set of 2,081 voters see *Exhibit - H1 DETAILED REVIEW*. In this sample of 644 records, we found no evidence of votes cast illegally. The review included a seven-point check of the voter's full name, address, full date of birth, social security number, voter ID, voting history, signature and found the following:

- 573 records are still active registered voters who have not informed the Maricopa County Recorder's Office of a move. In addition, the County has not received returned official election mail. We confirmed only one ballot was cast per voter and that voter was eligible for the November 2020 General Election.
- 24 records have been cancelled at the request of the voter after the election. We confirmed only one ballot was cast per voter and that each voter was eligible for the November 2020 General Election.
- 12 records have been cancelled due to death of voter. However, each of those voters legally cast their November 2020 General Election ballot prior to their date of death. We confirmed only one ballot was cast and that each voter was eligible for the November 2020 General Election.
- 14 records were cancelled due to a move outside the county after the election. We confirmed only one ballot was cast per voter and that each voter was eligible for the November 2020 General Election.
- 2 were cancelled due to a move outside the state after the election. We confirmed only one ballot was cast per voter and that each voter was eligible for the November 2020 General Election.
- 19 voters have moved from active status to inactive status since the November 2020 General Election due to the County receiving a returned piece of official election mail. We confirmed only one ballot was cast per voter and that each voter was eligible for the November 2020 General Election.

2,382 Ballots

5.5.4 – Cyber Ninjas Appendix D1 (In-Person Voters Who Had Moved Out of Maricopa County)

We did not receive the data set of voters that were included in this finding. Based on our review of data included in other similar sections above, we have not been able to substantiate the report's claims based on Cyber Ninjas' use of soft data matching techniques (i.e.; use of only year of birth instead of full date of birth) and use of a commercial third-party data set.

Informational

5.7.9 (No record of Voters in Commercial Database)

We can't attest to the accuracy of the third-party commercial database and the analysis that Cyber Ninjas used to compare the County's data with the third-party commercial data, the Melissa.com website, or the data that was entered into the site by Cyber Ninjas. A commercial database is not a trusted resource for confirming voters' residential addresses for voting purposes.

In Maricopa County, we rely on the voter's affirmation of their residential address until we are informed otherwise by the voter or by another trusted resource like the United States Postal Service or the National Change of Address report. A real-time database that tracks the day-by-day movement of every person in the state or in the nation does not exist. In a county with 2.6 million registered voters, people are constantly moving. Election experts across the country would tell you that the voter registration database is always changing, and in a jurisdiction the size of Maricopa County, voters make thousands of changes each week.

By law, no voter can be denied the right to vote because they are not in a commercial database. All eligible voters in Maricopa County have provided documented proof of their residential address, have had a validating "return service requested" mailing sent to that listed address to verify its authenticity, and have attested they are not felons and that they are a U.S. citizen. Through the statewide voter registration database and because we are an Electronic Registration Information Center (ERIC) member state, we check all records against the Motor Vehicle Division, Arizona Department of Health Services Vital Records, National Change of Address, other ERIC member state databases and dozens of other state and local trusted sources to keep the voter registration database as up to date as possible. We also receive monthly updates from the Arizona Secretary of State's Office informing us of individuals who have been legally declared ineligible to vote either through criminal act or incapacitation.

Item #10: Other Voter Registration Claims

(Cyber Ninjas Volume III Report Sections – 5.6.5, 5.6.6, 5.6.8, 5.6.10, and 5.6.11)

Cyber Ninjas' report included five claims that information in the voter registration database allowed ineligible voters to vote an official ballot. Our review found that the voter registration system is sound. However, in a County with over 2.6 million active voters reliant on disparate systems and sources of data and information, there is the possibility for a small amount of data entry errors and timing issues.

Cyber Ninjas Volume III			County Analysis
Reference	Claim	Ballots	
5.6.5 (pg. 27)	"Voters with Incomplete Names"	393	0
5.6.6 (pg. 29)	"Deceased Voters"	298	26
5.6.8 (pg. 32)	"Late Registered Voters with Counted Votes"	198	0
5.6.10 (pg. 37)	"Duplicate Voter IDs"	186	6
5.6.11(pg. 38)	"Multiple Voters linked by AFFSEQ"	101	0
Total(s)		1,370	32

State & Federal Laws

Arizona Law governs what information is needed to be included on a voter registration form and causes for cancellation of a voter record and how often death records are shared. Applicable Arizona laws include:

- A.R.S. § 16-121.01(A)
- A.R.S. § 16-152
- A.R.S. § 16-165

Maricopa County Findings

Summary

5.6.5 (Voters with Incomplete Names)

> **Voters are legally allowed to register with only a first name, last name, or single letter in their first or last name. A voter with a short name, no first name, or last name is not an indicator of an invalid voter.**

Response and Analysis

Cyber Ninjas' report questions the legality of 393 votes on the basis of the registered voter not having a first or last name or a first or last name with only a single initial. There is no federal or state law that requires a voter to have both a first and last name, let alone a name that is more than one letter. While uncommon, there are a few thousand legal voters in Maricopa County who have such names. Our analysis of the November 2020 General Election Voted File (VM55) found the following number of voters with a short and/or no first or last name (see *OTHER VOTERS* Table #1):

OTHER VOTERS Table #1 - Voted File (VM55) Name Analysis of the November 2020 General Election	
Category	Amount
Voters with only a First Name	0
Voters with only Last Name & Last Name is 1 Letter	0
Last Name and First Name of 1 Letter	0
Voters with only a Last Name	14
Voter with First Name of 1 Letter & Last Name More than 1 Letter	2,623
Last or First Name of One Letter and Middle Name of More than One Letter	2,066

Summary

5.6.6 (Deceased Voters)

In a County with over 2.6 million voters, there are several thousand voters that pass away each month. Cyber Ninjas claim to have found 282 instances of deceased individuals voting but did not provide the County with a data set to research. The County Recorder's independently directed analysis of voter records disproves the figures cited in Cyber Ninjas' conclusion.

Response and Analysis

Arizona law outlines the process by which a voter's registration is cancelled due to death (A.R.S. § 16-165(D)). This law requires that the Arizona Department of Health Services (ADHS) transmit on a monthly basis vital record information of the death of every resident of the state reported to the department within the preceding month to the Arizona Secretary of State. The statute does not provide for the use of a commercial database to obtain this information, and public access to the records is prohibited. As required by statute, the Arizona Secretary of State's Office validates and processes this information as soon as it's received from ADHS and notifies the appropriate County Recorder. Because the requirement in law stipulates ADHS provide the deceased records file only monthly, the County Recorder functionally processes deceased records reported to the state a month prior unless other notices and affidavits of death are received via separate methods. The County Recorder as a standard practice regularly researches county obituary notices to augment this process and keep the voter rolls up to date.

The information received from ADHS is used for the sole purpose of cancelling deceased Arizona residents from the statewide voter registration database. The Arizona Secretary of State's system initiates a matching process with the monthly file received from ADHS against the statewide voter registration database and will result in a "hard" or "soft match" on registered voter records. A "hard match" occurs if the first three letters of the first and last name, date of birth, and last four of the social security number of a deceased resident exactly match a registrant record in the statewide voter registration database. The statewide system will automatically cancel the voter registration record and immediately notify the County Recorder, which automatically cancels the voter in the County's voter registration database. A "soft match" occurs if the first three letters of the first and last name and date of birth match. If the system finds a "soft match" between the deceased record and a registrant record, it will flag the records and notify the appropriate County Recorder of the need to review and compare the records. The County Recorder's Office is then tasked with performing research to determine if a "true match" exists. If a true match is found, the name of each deceased person is cancelled from the voter registration database.

The County may also cancel a registrant's record if the County Recorder determines that the registrant is deceased based on other reliable sources including notices and affidavits of death.

There is no real-time database of vital records available to County Recorders and due to the statutory process listed above, there is a reasonable lag time before the County receives notices of death from the State. Early ballots are mailed to voters twenty-seven days before Election Day, and the County must prepare its ballots for printing several weeks prior to that mailing deadline. This results in a limited window during an election cycle that may result in family or household members receiving ballots for recently deceased voters. Recognizing these conditions, the County Recorder proactively directed an additional review of deceased voter records from the months immediately preceding the 2020 November General Election. All statutory requirements were met in the conduct of the 2020 November General Election, and this internal audit initiative was undertaken to help inform potential policy updates and ensure continuing improvement and integrity of the voter registration database.

The County Recorder's internally directed review began with the creation of a report of voter registration record changes related to deceased voters from the period of September 1, 2020 through November 7, 2020. The Office identified 4,623 voters who passed away during this timeframe. The Office also created a query to cross-check the VM55 Voted File (official public list of voters credited with participating in the November 2020 General Election) against the deceased lists received via the Arizona Secretary of State during this same time period. The query generated by Maricopa County identified 619 voters who have a date of death on or before Election Day and returned an early ballot during the November 2020 General Election (see *Exhibit - DECEASED*). In all cases, the County was notified of late September (post-25th), October, and November 2020 death records in files received via the Secretary of State in November and December 2020 (with one record received January 2021). Of the 619 voters, we found the following:

- 493 voters were confirmed to have returned their ballot to the Elections Department prior to the date of death (DOD). This is allowed for under state law. A registrant who passes away after casting a valid ballot is entitled to have his/her ballot tabulated and votes counted. See the 2019 Arizona Secretary of State Procedures Manual (Page 34).
- 100 instances are still under review due to affidavit envelope date being received near the voter's date of death (DOD). Most of these instances relate to affidavits that appear to be signed before the DOD, but were received by the County after the DOD.
- 26 possible instances of a ballot being processed and potentially counted for a voter that passed away prior to the ballot being returned. The County forwarded this information to the Arizona Attorney General's Office for further review.

Cyber Ninjas claims to have identified 282 ballots illegally cast by voters that were deceased but did not provide a data set to support these conclusions. The County cannot research Cyber Ninjas' claims but has undergone an independent analysis of deceased voter records. The figures cited in Cyber Ninjas' conclusion are not supported by documented records of deceased voters in Maricopa County.

Voter registration list maintenance is a vital function and is necessary to ensure fair elections. The Recorder's Office is always looking for ways to improve the process while maintaining the integrity of the rolls. In that effort, Maricopa County and all other Arizona counties are now receiving monthly deceased reports from ERIC, the Electronic Registration Information Center. These deceased reports include records from the Social Security Administration and will supplement the monthly

deceased reports received by the Arizona Department of Health Services. The Recorder's Office will also continue its practice of researching county obituary notices.

Additionally, we are reviewing our system's soft match criteria to see if changes made can elicit more possible matches between records with the data points available in our voter registration system. This will cast a wider net in an attempt to catch older system records that may be a match with newer system records.

Summary
5.6.8 (Late Registered Voters)

> **The law requires that voters who want to vote, but who are not identified in the SiteBook as properly registered, must be allowed to vote a provisional ballot. This includes those who registered to vote after the registration deadline. In accordance with federal and state law, these voters were issued a provisional ballot. None of the provisional ballots cast by those who registered after the deadline were counted.**

Response and Analysis
Cyber Ninjas identified 198 voters who participated in the November 2020 General Election but registered after the October 15, 2020 registration deadline. In a detailed review of these 198 voters, we found that all voted using a provisional ballot. This complies with federal (Help America Vote Act of 2002) and state law (A.R.S. § 16-513.01), that requires the Elections Department to provide a voter the right to vote provisionally, even if the voter is not registered to vote in that election. All provisional ballots are placed in a signed and sealed affidavit envelope and deposited in the ballot box. Each voter that casts a provisional ballot is researched to determine if the ballot should be counted. Because these voters registered to vote after the deadline, they were ineligible to vote and their provisional ballot was not counted.

Summary
5.6.10 – Cyber Ninjas Appendix Q1 (Duplicate Voter IDs)

> **Cyber Ninjas soft data matching techniques resulted in them incorrectly identifying potential voters who had two assigned voter registration numbers. As part of our review, the County had identified six potential instances of double voting. The information was forwarded to the Attorney General.**

Response and Analysis
The data we received in Cyber Ninjas Appendix Q1 had only 164 individuals, not 186 as listed on page 37 of the report. Cyber Ninjas claim voters in this category shared a First Name, Last Name, Address and Year of Birth, suggesting these are the same individuals. In a detailed review of the 164 voters with similar names that were included in Cyber Ninjas data, a total of 139 were confirmed to be different voters assigned different voter identification numbers. The search conducted

by Cyber Ninjas used a soft matching criterion with four data points: last name, first name, year of birth (within 10 years) and may have potentially shared an address in the past. This resulted in a false identification and incorrect conclusion that these voters shared a voter identification number. We used a seven-point search criterion to review the data including full name (first, middle, last), full date of birth, Social Security number (four digits), Arizona Driver License or state issued ID, residential history, signature and in some cases we had the voter's occupation and the father's last name or the mother's maiden name. As part of this detailed review, we identified 12 total voters that had two voter IDs. These voters had been previously identified by the County during a post 2020 General Election Review. These records have since been merged. Of the 12 voters, six potentially voted twice. The County forwarded this information to the Arizona Attorney General's Office for further review.

Summary

5.6.11 (Multiple Voters Linked by AFFSEQ)

> **The Affidavit Sequence Number is not an indicator of whether a voter cast more than one ballot. While there are a small percentage of situations where a sequence number was assigned to two voters, this does not impact the integrity of the election process.**

Response and Analysis

An Affidavit Sequence Number (AFFSEQ) is a unique transaction number that is system generated and assigned to a voter any time the voter updates his/her information. The AFFSEQ functions as a unique identifier to assign a transaction and trace the record back to a voter. Because each voter can have many AFFSEQs, there are tens of millions currently assigned within the voter registration system.

There are instances when voters update their voter registration information and provide a partially completed voter registration form. Since the registration form is not complete, there may not be sufficient information to identify a hard match with another voter. In these situations, the voter is assigned a system generated AFFSEQ. However, after research is completed and the voter registration team identifies the identity of the actual voter, the form must be reassigned. In these situations, the AFFSEQ is manually assigned. While rare, this manual assignment can result in data entry errors. However, the AFFSEQ is not what the Elections Department uses to determine if a ballot should be issued, and it was incorrect for Cyber Ninjas to categorize this issue of an incorrectly assigned AFFSEQ as having impacted ballots.

We completed a detailed review of all 5,711 records (2,854 unique affidavit sequence numbers) identified in Cyber Ninjas' data set as being assigned to multiple voters. We found the following:

- 2,782 of the AFFSEQs were assigned to one unique voter who had two unique voter registration numbers. This was the result of a voter submitting a voter registration form or request through Service Arizona with insufficient or incorrect identifying information. In these instances, the voters were assigned temporary voter registration numbers until the actual voter could be identified. We've confirmed that none of these voters had more than one ballot counted.
- 72 instances where two voters were assigned one unique affidavit number. Since ballots are not issued based on affidavit sequence numbers, this did not result in a voter casting more than one ballot.

Item #11: Protected Voters

(Cyber Ninjas Volume III Report Sections – 5.5.1, 5.5.5)

Cyber Ninjas' report included two claims that the official certified results (Canvass) do not match the official public list of voters credited with participating in the November 2020 General Election (VM55 Voted File). These two claims are inaccurate and are likely a misunderstanding on the part of Cyber Ninjas about what information is included in the VM55 Voted File.

Cyber Ninjas Volume III			County Analysis
Reference	Claim	Ballots	
5.5.1 (pg. 12)	"Official Results Do Not Match Who Voted"	3,432	0
5.5.5 (pg. 18)	"Votes Counted in Excess of Voters Who Voted"	1,551	0
Total(s)		4,981	0

State & Federal Laws

A.R.S. § 16-153(A)(B.1)(J)(K1-12) requires that the confidentiality of protected voters be maintained.

Maricopa County Findings

Summary

5.5.1 (Official Results Do Not Match Who Votes) & 5.5.5 (Votes Counted in Excess of Voters Who Voted)

> **Cyber Ninjas did not consider that there are over 3,000 protected voters in Maricopa County who participated in the November 2020 General Election. As required by state law these voters are not included in any public voter files.**

Response and Analysis

Cyber Ninjas' report claims 3,432 more ballots reported in the official canvass than there were voters reported in the Official VM55 Voted File (dated 11/19/2020). On page 18, Cyber Ninjas claim that there were 1,551 more votes cast in the election than the total number of voters who participated. The reason for these incorrect assumptions is simple: state law prevents counties from including protected voters (judges, law enforcement officers, survivors of domestic violence and other types of harassment or abuse) in any public voting file, including the VM55 Voted File. Maricopa County has over 3,000 protected voters that participated in the November 2020 General Election and they are not listed on the VM55 Voted File. To protect the identify of these voters, the County does not create public reports or lists that show the exact number of protected voters.

Two other situations may contribute to alleged discrepancies identified Cyber Ninjas' analysis. The first occurs when a voter returns an affidavit envelope that is empty, containing no ballot. In this situation during the November 2020 General Election, the voter would be listed in the VM55 Voted File for returning a signed affidavit envelope, but since there was no ballot, the canvass count would not include a ballot. For the November 2020 General Election there were 68 instances of this occurring.

The other situation involves a voter who checks into an in-person voting location but chooses not to vote his/her ballot. While this is very rare, it can happen on occasion. If the poll workers know the identity of the voter, they are trained to work with our poll worker hotline to back out the voter's check-in from the system. This process may not always be followed when a voter does not stay to assist with the process to reverse the check-in. Our post-election analysis identified 17 instances where we believe this occurred. This represented .0091% (nine-one-thousandths of a percent) of in-person voters who voted on Election Day. The voting locations where this occurred are listed in *FLED VOTERS Table #1*.

FLED VOTERS Table #1 - Fled Voters on Election Day by Voting Location	
Locations	Fled Voter
All Saints Lutheran Church	1
Apache Wells Homeowners Association	1
Veterans Memorial Coliseum	1
Church At Litchfield Park	1
LDS Church	2
Lutheran Church of The Master	1
Murphy School District Office	1
Paradise Valley Community College	1
Sheraton Phoenix Crescent	2
Surprise City Hall	1
Youngker High School	5
Total Fled Voters (Percent of Total In-Person Voters)	**17 (.0091%)**
Total In-Person Voters on Election Day including Provisional Voters	**186,756**

Item #12: Early Ballot Returns and Real-Time Check-in System

(Cyber Ninjas Volume III Report Sections - 5.4.1, 5.6.3, 5.6.1, 5.6.4, 5.6.9, and 5.7.4)

Cyber Ninjas' report included five claims that speculated that some entries in the Early Voting Request file (EV32) and Early Voting Return file (EV33) were a possible indication of voters who were allowed to cast multiple ballots. These claims demonstrate a lack of understanding of the statutory purpose of the EV32 and EV33 files and how the County's data tracking controls prevent voters from casting multiple ballots. The report also included a finding that questioned the County's use of "real-time provisional ballots." All the claims below have been thoroughly reviewed and confirmed as unsubstantiated or false.

Cyber Ninjas Volume III			County Analysis
Reference	Claim	Ballots	
5.4.1 (pg. 8)	"More Early Ballots Returned by Voter Than Received"	9,041	0
5.6.3 (pg. 24)	"Ballots Returned not in the final Voted File"	430	0
5.6.4 (pg. 25)	"Mail-in Ballot Received Without Record of Being Sent"	397	0
5.6.1 (pg. 20)	"Voters Not Part of the Official Precinct Register"	618	0
5.6.9 (pg. 34)	"Date of Registration Changes to Earlier Date"	193	0
Total(s)		10,679	0
5.7.4 (pg. 51)	"Early Votes Not Accounted For in EV33"	N/A	False Claim
5.7.11 (pg. 59)	"Real-Time Provisional Ballots"	N/A	Misleading Claim

State & Federal Laws

Arizona Law governs the type of early ballot request and return reports that are required to be provided to registered political parties, laws around temporary early ballot requests, curing signatures, and special election boards. Applicable Arizona laws include:

- A.R.S. § 16-168 (C.11)(D)
- A.R.S. § 16-542(E)
- A.R.S. § 16-550 (A)
- A.R.S. § 16-549(A)(C)(D)

Maricopa County Findings

Arizona law and the Elections Procedure Manual outline the data files and voter record files that the law requires counties to produce for each election. The naming conventions for these various files (EV32, EV33, VM55, VM34 etc.) may differ from county to county, but the content and prescribed for use of these files is the same. To assist with understanding these reports, below is a summary description and Maricopa County's unique naming convention for each required file:

- Early Ballot Requests and Returns: Statute requires all counties to create a daily report of early ballot requests and returns from voters at the request of political parties. These daily reports must begin 33 days prior to the election and for returns, end the day before Election Day. They are not intended to be a reconciliation of all early ballot requests and returns, as they are required to end prior to Election Day. Historically political parties use this for "get-out-the-vote" efforts. This file also does not include any protected voters (A.R.S. § 16-153). Below is how Maricopa County and the political parties agreed to the file creation and sharing:

- EV32 File: This is a daily data file created for political parties of early ballot requests from voters. For the November 2020 General Election, these files were provided from October 1-23, 2020. October 23 was the eleventh day preceding the election and the last day to request a ballot to be mailed (A.R.S. § 16-542.E).
- EV33 File: This is a daily data file created for political parties of early ballots returned by voters. This is not a list of ballots that were counted. All early ballot envelopes must go through the exhaustive and comprehensive signature review process to have the signature verified before it can be counted. For the November 2020 General Election these files were provided from October 12 to November 2, 2020, the Monday before Election Day.

- VM55 Voted File: This file, prescribed for in state law, is the final accounting of voters who participated in the election broken out by early voting and Election Day. The file is run after all early ballot signatures have been verified and after all provisional ballots have been researched. This file does not include any protected voters (A.R.S. § 16-153).
- VM34 Monthly Voter Roll: This file is distributed to political parties and jurisdictions conducting elections upon request. The file contains the voter name, voter ID#, mailing and residential address, party affiliation, and voting history for all voters-both active and inactive (A.R.S. § 16-168).

Summary

5.4.1 (More Early Ballots Returned), 5.6.3 (Returned Ballots Not in Voted Filed), 5.6.4 (Ballot Received Without Sent Record) & 5.7.4 (Early Votes Not Accounted For)

Cyber Ninjas' apparent lack of understanding of the purpose of the EV32 and EV33 files resulted in inaccurate speculations about the legitimacy of 9,868 ballots.

Response and Analysis

Voters in Maricopa County may vote early by mail or in person prior to Election Day. Arizona law defines both of these cases as a voter casting an early ballot. Statute requires the County provide registered political parties with direct access to daily early ballot request and returns. As described in the findings section above, those files are called the EV32 and EV33 requested and received files. The political parties generally use the files for get-out-the-vote efforts. These files are not a comprehensive listing of all voters, as they have specific start and end dates outlined in statute, they then would not include voters that dropped off an early ballot on Election Day, nor do they include protected voters (A.R.S. § 16-153).

Any comparison using these files will likely lead to inaccurate conclusions, as was the case with Cyber Ninjas when they incorrectly claimed there were over 74,000 more early ballots returned than were requested for the November General Election.

Our review of Cyber Ninjas' data supporting this finding and Maricopa County voter registration data found no evidence of double voting. These EV33 return entries were related to voters legally curing questionable signatures or blank unsigned envelopes leading to those envelopes to be scanned in as "returned" once again upon receipt of the cured packet. All voters reviewed were eligible to cast a ballot. Below are further details about sections 5.4.1, 5.6.3, 5.6.4 and 5.7.4.

9,041 Ballots

5.4.1 – Cyber Ninjas Appendix C1 (More Early Ballots Returned than Voters Received)

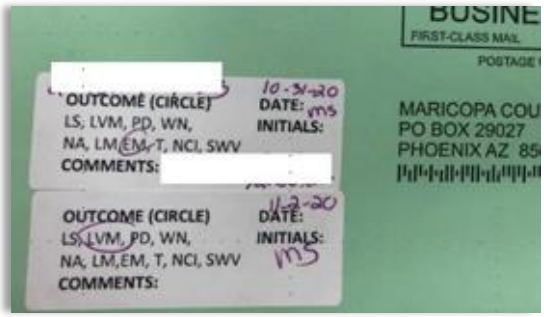
In Cyber Ninjas' report on page 8, they state that there were 9,041 duplicated entries in the EV33 file. Cyber Ninjas' report speculates and offers four potential explanations of why there may be duplicate entries. The second bullet

on that page, *"The same ballot could have been processed more than once on different days, resulting in two EV33s for one ballot*" is mostly correct.

There are some multiple entries on the EV33 report because an early ballot packet envelope can be reviewed more than once. When an early affidavit envelope is flagged as a questionable signature or blank signature, the packet is manually set aside and staff works to contact the voter to cure the signature. If the signature is cured, the packet is rescanned on a different date creating an additional EV33 entry, thereby creating a second entry, one for the initial time the packet was scanned for review (1st EV33 entry), then when it was scanned again for new review (2nd EV33 entry). There can be other additional scans and EV33 entries if a packet was set as a "questionable signature" or if a packet was cancelled. During this process, the early ballot affidavit envelope remains sealed until the signature is cured. After the signature is cured, the ballot packet is opened, and then the ballot is counted. If the signature remains "questionable" after the end of the statutory curing period, the ballot affidavit envelope remains sealed, is not opened, and would be marked as a "bad signature" in the canvass.

Most signatures on early ballot affidavit envelopes match the signature on record—the ballot affidavits do not require curing and are processed as normal. The Elections Department is required to contact voters when their signatures cannot be verified, or if the affidavit envelope was not signed. For those small percentages of affidavits that require further review and are subsequently cured by the voter, we include the stamp "Verified and Approved MCTEC" and physically log on the affidavit envelope all the individual contact attempts and verification methods used to reach the voter (see *EV Image #1*).

EV Image #1 - Example of "Cured" Affidavit Envelopes



(Left) An example of an Early Ballot Affidavit Envelope with Curing Contact Information. (Right) An example of the verified and approved stamp.

On October 20, 2021, Cyber Ninjas issued an 11-page public statement further clarifying its position. In it, Cyber Ninjas said that the explanation above was "a soundbite, not an explanation" and said that EchoMail found that only 2,138 of these voter IDs had more than one scanned envelope. That is not true. Maricopa County reviewed the data for scanned packets for all 9,041 voters and compared this to the affidavit images provided to the Senate (see *Exhibit – EARLY BALLOTS).* Below is a summary of our analysis:

- 8,850 (2 Envelope Images) – These voters were in the EV32 file once and the EV33 file twice. This shows that the initial signature issue was cured and the ballot packet was scanned in a second time. These could be questioned signatures, no signatures or household exchanges (ex. when a husband signs his wife's envelope, and the wife signs her husband's envelope). Once cured, the envelopes were then opened and only one ballot per voter was counted.

- 162 (3 Envelope Images) – These voters were in the EV32 file once and the EV33 file three times. This shows that there was an initial signature issue, but the envelope was scanned in on two other occasions as staff worked to verify signature. These could be questioned signatures or no signatures. Staff was able to contact the voters, use the "Verified and Approved MCTEC" stamp and cure the signature issue. The envelopes were then opened and only one ballot per voter was counted.
- 3 (4 Envelope Images)– While this doesn't happen often, these voters were in the EV32 file once and the EV33 file four times. This shows that there was an initial signature issue, but the envelope was scanned in on three other occasions as staff worked to verify the signature. Staff was able to contact the voters, use the "Verified and Approved MCTEC" stamp and cure the signature issue. The envelopes were then opened and only one ballot per voter was counted.
- 26 (Unique Voter Situations) – There were 26 unique instances where the number of images did not match the number of times the voter appeared in the EV33 file. Below are a few reasons.
    - Voter A's ballot was returned, but a household member signed his own name in place of Voter A. Staff called to cure the signature issue and found out Voter A was eligible to vote a UOCAVA ballot. The first ballot was cancelled, and Voter A was issued a UOCAVA ballot after the 10/23/2020 early ballot request deadline as is permitted under law for military and overseas voters. Voter A's signature was verified and the ballot was counted. In this instance, the voter was in the EV32 file once and the EV33 file once, but would not have any images because the initial packet was voided and we don't scan UOCAVA envelopes, as the verification process is manual.
    - Voter B returned the ballot packet without a signature. The ballot packet was mailed back to the voter. Voter B returned the ballot packet a second time without a signature. The ballot was mailed back to the voter a second time. Voter B returned the signed envelope on Election Day, it was cured and counted. In this instance, the voter would be in EV32 once and EV33 twice, but have three image scans.
    - Voter C had a questionable signature. Staff contacted the voter to cure the signature and added the "Verified and Approved MCTEC" stamp. The ballot packet was scanned again, but the envelope was upside down. The ballot packet was scanned a third time after Election Day and then the ballot was counted. In this instance, the voter would be in EV32 once and EV33 twice, but have three image scans.

In addition to the analysis above, the County performed a random sample of 325 of the 9,041 Voter ID numbers Cyber Ninjas provided to support its claim. Our detailed review of the affidavit envelope images and the voter records confirmed that all 325 instances were the result of the County's early voting team contacting a voter for a questionable signature and curing that signature in accordance with the Elections Procedure Manual (EPM) 2019 (pages 68-69) and A.R.S. §16-550.

430 Ballots

5.6.3 – Cyber Ninjas Appendix K1 (Ballots Returned Not in the Final Voted File)

In Cyber Ninjas report on page 24, they claim 2,472 voters returned an early ballot but are not accounted for in the final VM55 Voted file. They then calculated the 430 "ballots impacted" number by subtracting the total number of early ballots not counted because the envelope did not have a signature (1,455) and the total that did not match any signatures on file (587), as reported in the canvass. Below is a breakdown of the 430 ballots.

- 4 – These were duplicates of the same voters that Cyber Ninjas should have filtered out of the K1 Appendix.

- 51 – These voters received a new Voter ID number during the election. In this rare circumstance, the initial Voter ID number is accounted for in the EV33 file, and the new Voter ID number is accounted for in the post-election VM55 Voted File, which was prepared on November 24, 2020. Both Voter IDs are tracked and connected to the voter, but the new Voter ID number would be used for the voter moving forward.
- 375 – These records were voided early ballots. There are several reasons why a ballot would be returned, put in this category, and not counted. They can include a ballot returned by a household member noting a voter has moved, an unresolved household exchange packet signed by a household member, a packet damaged by USPS, etc.

397 Ballots

5.6.4 – Cyber Ninjas Appendix M1 (Mail-In Ballot Received Without Record of Being Sent)

The County's review of the 397 records found in Cyber Ninjas Appendix M1 show that all were associated with a legitimate and eligible voter with a verified signature and valid returned early ballot. These records do not appear in EV32 "Sent" file because they were requested or "flagged" after the last day the file was prepared (10/23/2020). We also found Cyber Ninjas mistakenly included four voter records twice. The County verified that each voter cast only one ballot, but had two scans due to signature curing. That leaves only 393 unique voter records for review. Below is a summary of our analysis:

- 200 – All of these ballots were requested by the voter prior to the 5 p.m. deadline on 10/23/2020, many just minutes prior to the deadline. These requests are valid, but our staff needs time to research, finalize and flag the ballots to prepare them for mailing. It can take through the weekend to clear that queue. Ballots requested just before the deadline but processed by staff over the weekend would not be included in the EV32 file.
- 131 – All of these ballots belong to military and overseas voter requests, which are covered under the Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA), which mandates these voters be allowed to request a ballot up to and including on Election Day. Ballots requested by UOCAVA voters after the 10/23/2020 deadline (applicable to all other voters) would not be included in the EV32 file.
- 54 – These voters updated their voter registration during the election and received a new Voter ID number. The initial Voter ID number is accounted for in the EV32 file, and the new Voter ID number is accounted for in the EV33 file. Both Voter IDs are tracked and connected to the voter, but the new ID number would be used for the voter moving forward, including in the post-election VM55 Voted File prepared on November 24, 2020.
- 8 – While a small number, these voters have an emergency request that occurred after the 10/23/2020 deadline. These voters are usually in the hospital or another setting that prevents them from voting in person or casting an early ballot from home. In these cases, the law allows these voters to request a ballot through Election Day. A bipartisan Special Election Board assists the voter at the hospital or other setting in accordance with A.R.S. §16-549.

Informational

Section 5.7.4 (Early Votes Not Accounted For in EV33)

Much like the error made initially by Cyber Ninjas in July 2021 — when they said that 74,243 records were missing versus this newly adjusted 397 total — this is still a misunderstanding as to the true purpose and actual use of the EV32 and EV33 files. State law is clear. These daily files are created for the "county or state chairman." The start and end dates of each file can be found in A.R.S. § 16-168(D) and in the Elections Procedure Manual (EPM) 2019 (pages 62-63). These files are not intended to capture all voters that participated in the election as the "returned"

file is required to end the Monday before the election. Instead, they have traditionally been used by the political parties for targeted "get-out-the-vote" efforts.

For the 2020 General Election, the EV33 file was last created on the Monday before Election Day (November 2, 2020). The Election Department tracks every sent and received ballot through a barcode on the ballot envelope that is unique to each voter, and even to each ballot request by the voter. The voters not included in the EV33 file, but are tracked in the VM55 Voted File include:

- 187,707 mail-in ballots that were dropped off on Election Day or the day prior
- 38,796 voters that voted in-person during the last few days of early voting
- The remaining 28,823 are a combination of two reasons:
    - 28,614 – These voters were in the 10/13/2020 EV33 File. We do not know why Cyber Ninjas did not include these 28,614 voters in their data file.
    - 137 — These voters updated their voter registration during the election and received a new Voter ID number. This is typically caused when a voter submits a voter registration form that has different information than what is already on file. Both Voter IDs are tracked and connected to the voter, but the new ID number would be used for the voter moving forward, including in the post-election VM55 Voted File prepared on November 24, 2020.

It is important to point out that protected voters are not included on any public file, including the EV33 or VM55 Voted files. Arizona law requires that the confidentiality of protected voters be maintained (A.R.S. § 16-153).

Summary

(5.7.11) Real Time Provisional Ballot, (5.6.1) Voter not Part of the Official Precinct Register and (5.6.9) Date of Registration Changes to Earlier Date

> **The County has implemented an award-winning, secure, real-time voter check-in station at voting locations that prevents double voting while also expanding voting access.**

Response and Analysis

Maricopa County's voter check-in system, the SiteBook, has a real-time, secure connection to the voter registration system. Developed in-house by our information technology experts, the SiteBook uses proprietary software and a virtual private network (VPN) connection for enhanced security. It is not connected to the tabulation equipment at the voting locations or the County's Ballot Tabulation Center.

When a voter checks in at the polls, the SiteBook conducts a live check of the voter registration database to ensure the voter is eligible and that the voter has not already cast a ballot. If an early ballot has already been issued, the SiteBook does a "real-time" check of the voter's record. If that ballot was not returned, the SiteBook cancels the early ballot and issues the voter the standard ballot for voting at the polls, referred to here as a "real-time provisional ballot." The provisional ballot check is done behind the scenes and provides voters a much more streamlined voting experience, allowing the voter to receive a ballot that could be counted at the polls if an early ballot has not already been recorded as returned. If an early ballot was already returned by the voter, the SiteBook informs the voter that a ballot was already cast. State and federal law require that the voter still has the option to vote a provisional ballot, which is a fail-safe for voters whose eligibility to

vote is uncertain. The voter's record would be researched by staff separate from the voting location, and the provisional ballot would not be counted if the voter's early ballot was already counted.

The County has been using this real-time provisional ballot approach since 2016. The advancement in e-pollbook technology has allowed jurisdictions nationally to utilize a systematic process to verify a voter's eligibility through a real-time connection, including if a voter has already cast a ballot in person or by mail. This process has been utilized under three separate County Recorder administrations and was initially reviewed and approved for use as an alternative process and procedure by the Secretary of State's Office in 2015 under Arizona Secretary of State Michele Reagan. There are several statutory requirements for provisional ballots. Below is a summary of the statute and the action taken in Maricopa County to comply:

- The generation of a new ballot for the voter complies with the requirement that such electors vote provisional ballots, A.R.S. §§ 16-579(B) and 16-584, as a provisional ballot requires additional review to determine whether the one casting the ballot is eligible to do so.
- The check of the database in real-time to determine whether another ballot has been counted complies with the required check for provisional ballot voters described in A.R.S. § 16-584(D).
- The voter signing the affidavit on the e-pollbook or SiteBook, as it is called in Maricopa County, complies with the affidavit requirement described in A.R.S. § 16-584(B).
- The counting of the ballot complies with the requirement of A.R.S. § 16-584(D) that, if the elector has not already had her vote counted, then their provisional ballot shall be counted.

In the November 2020 General Election, the real-time provisional ballot casting process and system worked as intended. In Cyber Ninjas' own report on page 59, it states that they "identified no instances of these voters casting more than one ballot, however."

Cyber Ninjas includes a claim on page 20 of its report that there are 618 voters that participated in the November 2020 General Election who were not listed in the November 7, 2020 VM34 Monthly Voter Roll. We did not receive a data set that supported Cyber Ninjas analysis and conclusion. This analysis is another instance of Cyber Ninjas' attempting to compare unrelated data sets that are not intended to match. Cyber Ninjas incorrectly assumed that all voters that were eligible to participate in the November 2020 General Election would show in the November 7 version of the VM34 Monthly Voter Rolls. This is not the case because the VM34 Monthly voter roll file is a snapshot of the voter rolls at that specific point and time. In a County with over 2.6 million voters, there are thousands of changes made to the voter registration database on a daily basis.

There are variety of reasons why a voter that was eligible to participate in the November 2020 General would not show on the 11/7/2020 VM34 Voter Rolls. Below are a few examples of why a voter may appear on the VM55 Voted File and not on the VM34 Voter Rolls file.

- The voter was eligible to vote and then moved after the October 15, 2020 court-ruled cut-off period and before November 7, 2020. Upon the County receiving notification of the move, the County would update the voter registration system and the voter would not appear on the VM34 November 7, 2020 voter roll file. However, the voter would appear in the VM55 Voted File because they were eligible to vote in the November 2020 General Election.
- The voter submitted one or more voter registration forms with incomplete or inaccurate information. The voter would be assigned a temporary voter registration number while the County's Voter Registration staff performed required citizen and residency checks. In some of these instances, the voter already has an assigned voter

registration number. In these cases, the voter registration team would confirm all paperwork was properly provided. After which they would identify the voter as having two assigned voter registration numbers and merge the files. Depending on the timing of when the voter submits the voter registration form and when the voter registration team completes their research, the voter may have one or more records included or not included in the monthly VM34 Voter File.

- The voter submitted a paper registration form prior to 10/15/2020 (the court-ruled voter registration deadline for the November 2020 General Election). The voter would have likely voted provisionally, while the County finished processing the paper registration forms. In addition, the statutory deadline for curing a provisional ballot was 5:00pm on 11/10/2020. This is three days after the VM34 November 7, 2020 file was created. In these instances, the voter may legitimately not appear on the Monthly VM34 file created in November and then be listed on the December file.

Cyber Ninjas also incorrectly concludes that the County creates an official precinct register report that is distributed to voting locations for check-in purposes. Since the County uses an electronic check-in system (SiteBook described above), the County does not create a paper precinct register. Rather, the precinct register is maintained in real-time and updated through Election Day.

Item #13: Early Ballot Envelope Images

(EchoMail Report)

EchoMail made many false, inaccurate, and misleading claims about Maricopa County's early ballots due to a flawed understanding of the County's signature verification process. Addressed in this report are 10 claims made by EchoMail. All were found to be based in a misunderstanding of Arizona laws and County early ballot processes.

EchoMail Report			County Analysis
Page Number	Claim Topic	Envelopes	
Pg. 14	Canvass Requirements	n/a	False Claim
	17,126 "Duplicate" Early Ballot Images	17,126	Misleading Claim
	More Envelopes Processed & Submitted than Identified by EchoMail	6,545	Misleading Claim
Pg. 14-15	No Signatures, Scribbles & Bad Signature Rates	2,580	Inaccurate Claim
		9,589	Inaccurate Claim
Pg. 15	Increase in Envelopes but Decrease in Signature Rejections	n/a	Inaccurate Claim
Pg. 74-75	Daily Duplicate Numbers	7,797	Misleading Claim
Pg. 79	Stamped in Signature Region	n/a	Misleading Claim
Pg. 84	Stamp Behind the Envelope Triangle	n/a	Misleading Claim
Pg. 85-86	Two-Different Voter IDs	n/a	Misleading Claim

State & Federal Laws

Arizona law governs the type of early ballot request and return reports that are required to be provided to registered political parties, laws around temporary early ballot requests, curing signatures, and special election boards. Applicable Arizona laws include:

- A.R.S. § 16-168 (C.11)(D)
- A.R.S. § 16-542(E)
- A.R.S. § 16-550 (A)
- A.R.S. § 16-549(A)(C)(D)

Maricopa County Findings

Maricopa County has had "no excuse" early voting since 1992. In the 2020 General Election, over 91% of voters participating in the election cast an early ballot. Maricopa County has a rigorous signature verification process. All ballot affidavit envelopes require a signature that is checked against a known signature on the official voter registration file. The Elections Department has strong internal controls and tracking methods for ballot security. Only verified ballots with signatures on their affidavit envelopes are counted, but we report all uncounted, rejected ballots as well.

The accuracy and completeness of Maricopa County's signature verification process was confirmed in court (*Ward v. Jackson*). The Arizona Supreme Court affirmed the lower court ruling, "conclud[ing], unanimously, that...the challenge fails to present any evidence of 'misconduct,' 'illegal votes' or that the Biden Electors 'did not in fact receive the highest number of votes for office,' let alone establish any degree of fraud or a sufficient error rate that would undermine the certainty of the election results." (Ariz. S. Ct., December 9, 2020)

Summary
(EchoMail Report Pgs. 14-16, 74-75, 79 & 84-86)

The "anomalies" EchoMail uncovered are due to a flawed understanding of signature verification laws and practices. The EchoMail analysis did not consider the signature curing process, which accounts for multiple scanned images on an envelope, but only one ballot that was counted.

Canvass Requirements
EchoMail Report (pg. 14): "It is unknown, per the CANVASS report, how many EVB return envelopes were originally received by Maricopa election officials."

The purpose of the canvass is to report final results for each precinct and to officially certify the election. What is required to be reported in the canvass is clearly outlined in state law A.R.S. §§ 16-642-16-651 and the Arizona Elections Procedures Manual (Section II, Pgs. 239-244) 2019. It is not meant to report how many return envelopes were received or how many envelope images were captured, because those envelope images have no bearing on how many valid ballots were tabulated. Return envelopes can be scanned multiple times if there are questions about the voter's signature or if there is not a signature on the envelope. If a return packet is ultimately rejected (bad signatures, no signatures, etc.), that number is required to be reported in the canvass. During a general election, the canvass must be done no later than 20 days after Election Day.

The canvass must contain:

1. A Statement of Votes Cast, which includes:
    a. The number of ballots cast in each precinct and in the county;
    b. The number of ballots rejected in each precinct and in the county;
    c. The titles of the offices up for election and the names of the persons (along with the party designation, if any, of each person) running to fill those offices;
    d. The number of votes for each candidate by precinct and in the county;
    e. The number and a brief title of each ballot measure; and
    f. The number of votes for and against each ballot measure by precinct and in the county. A.R.S. § 16-646.
2. A cumulative Official Final Report, which includes:
    a. The total number of precincts;
    b. The total number of ballots cast;
    c. The total number of registered voters eligible for the election;
    d. The number of votes for each candidate by district or division, including a designation showing which candidate received the highest number of votes;
    e. The number of votes for and against each ballot measure by district, including a designation of which choice received the highest number of votes;
    f. The total number of votes in each district or division.
3. A Write-Ins Vote Report, which includes the name and number of votes for each authorized write-in candidate by precinct

- In addition, four other reports are required to be created and publicly reported in a general election, which include:
    1. Provisional Ballot Report
    2. Accessibility Report
    3. Voter Education Report
    4. Poll Worker Training Report

As required by the law, Maricopa County reported in the canvass that 1,915,487 early ballots were counted in the November 2020 General Election. An additional 2,976 early ballots were returned but not counted: 587 bad signatures, 1,455 no signatures and 934 late returns. In order to report these figures, the County maintains a full accounting of all ballot returns and keeps a record of each time an envelope is scanned. Federal and state laws do not have a reporting requirement for listing the number of early ballot envelopes received. It is not uncommon for the County to receive a small number of late early ballot affidavits after the canvass is complete and certified.

17,126 "Duplicate" Early Ballot Images

EchoMail Report (pg. 14): "EchoMail identified 34,448 EVB return envelope images being 2-copy, 3-copy, and 4-copy Duplicates originating from 17,126 unique voters, while no Duplicates were reported in Maricopa's CANVASS report."

Maricopa County only counts one ballot per eligible voter. The canvass is designed to report ballots, not envelopes. EchoMail did not understand that Maricopa County may scan an envelope multiple times as a voter "cures" a signature issue or signs a blank envelope. Early ballot envelopes are NOT opened until a signature is verified.

As commanded by the January 12, 2021 subpoena, the County provided the Senate every envelope scan for early ballot envelopes. The Elections Department may scan an envelope multiple times if the signature is questioned or left blank. As required by law, staff work to contact these voters to offer them the opportunity to "cure" the signature issue. During the 2020 General Election, Maricopa County contacted upwards of 25,000 such voters.

EchoMail reported that 17,126 duplicate envelope images were provided to the Senate. It's absolutely true that an envelope may be scanned in multiple times. When an early ballot is returned, the envelope is scanned in and sent to signature verification. 100% of mail-in ballot signatures are verified by trained staff. If a signature is questioned, the voter is contacted to verify the signature. After the signature is cured, the envelope would be scanned a second time, then sent to processing to be opened. There are several reasons why an affidavit envelope may be scanned three or even four times. No matter how many times an envelope is scanned, the envelope is not opened unless the signature is verified.

Some have asked why there is a difference between EchoMail's 17,129 early ballot envelope number and Cyber Ninjas' 9,041 early ballot return number. The reason is straight forward. While EchoMail looked all ballot envelope scans through the "questionable signature" cure period (ending November 10, 2020), Cyber Ninjas looked at the EV33 Returned File, which is a daily file of early ballots returned until the day before Election Day (November 2, 2020). Every voter that cured their signature from November 3-10, 2020 and all voters that did not, would not be included in Cyber Ninjas' total. Envelopes can be scanned multiple times during this process, but as stated above, it is not opened without a good or cured signature.

More Envelopes Processed & Submitted than Identified by EchoMail

EchoMail Report (pg. 14): "6,545 more *unique EVB return envelopes were processed by Maricopa than identified by EchoMail."*

As commanded by the Senate's subpoena in January, Maricopa County provided the Senate with more than 1.9 million early ballot envelope images for ballots that were counted. That file included all scans of the envelopes throughout the election cycle. The Senate's August 2021 subpoena commanded the production of all "envelope" images. Below in *ENVELOPES Table #1* outlines the total number of envelope images provided to the Senate compared to the total number of early ballots counted.

ENVELOPES Table #1 - Ballot Envelope Images Provided to the Senate				
Category	Scans	Date Provided	Unique Voters	Total Unique Voters
Envelope Images	1,919,598	August 18, 2021	1,902,276	1,911,919
	9,643	September 16, 2021	9,643	
Early Ballots Counted (Reported in the Official Canvass)				1,915,487
Difference (Empty Affidavit Envelopes, Protected Voters, and Other Situations)				3,568

The difference between the total number of unique envelope images and the number of early ballots counted is due to protected voters and cancelled voters. The County is required under A.R.S. § 16-153 to protect the confidentiality of protected voters (judges, law enforcement, domestic violence victim, etc.). These envelope images were not provided. The County had more than 3,000 protected voters participate in the November 2020 General Election.

No Signatures, Scribbles & Bad Signature Rates

EchoMail Report (pg. 14-15): "464 more 'No Signature' EVB return envelopes were reported by EchoMail… 2,580 scribbles identified…9,589 more EVB return envelopes were submitted for Signature Verification by Maricopa than the EVB return envelope images identified by EchoMail as having signatures."

EchoMail's conclusion that Maricopa County had too few invalid signatures (eg. Reporting only 587 "bad signatures" out of the 1,918,463 counted), or that the County approved scribbles and envelopes without signatures demonstrates a misunderstanding of Arizona election laws. Counties are required to contact voters when their signatures cannot be verified, or when they did not sign the affidavit envelope and offer those voters an opportunity to "cure" their signatures (A.R.S. § 16-550). This "cure" period for the General Election, which is outlined further below, allows voters five business days to verify and validate their signatures. This additional time reduces the number of ballot packets ultimately designated "bad signature."

Maricopa County has a multi-level signature verification process to review 100% of the signatures on mail-in ballots. Trained staff first look at the broad and local characteristics of the signature and compare it to one signature on file. In this first review, staff can only select one of two options: approve the signature (if it matches the one signature used for this initial review) or move it to an "exception" status (if it does not). If an envelope is moved to an "exception status," the manager is able to review every signature sample we have on file for that particular voter. Additionally, in every batch of approximately 10,000 signatures, the managers perform a statistically significant 2% audit of the signatures within that batch.

Questioned Signatures

If the signature doesn't match any of the voter's signatures on file, the manager would mark it as a questionable signature and the voter is notified by mail, email, text and phone (if available in the voter record and/or signed up for text alerts). If the voter returns our messages and confirms the ballot and signature is valid, staff stamp the envelope with "Verified and Approved MCTEC" stamp and it would be rescanned and sent to ballot processing and

tabulation. Pursuant to law, voters had until 5 p.m. on Tuesday, November 10 to cure their signature for the November 2020 General Election. An envelope is not opened unless there is a verified signature.

ENVELOPES Image #1 - Scribble Verified by Voter

(Above) Blurred Image from Figure 49 of the EchoMail report on page 65.

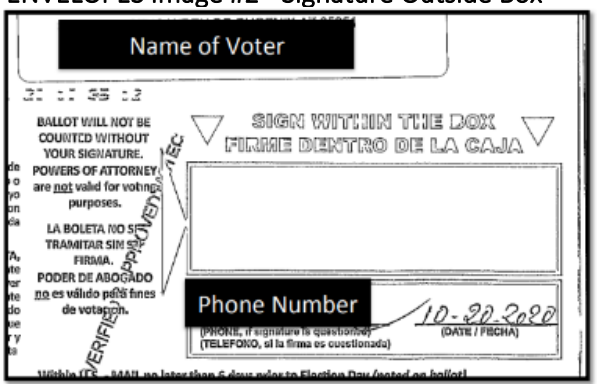
EchoMail provided a great example of this process on in Figure 49 on page 65 of its report. The image on the left is the first scan. If it was questioned, a manager would have reviewed other signature samples or the voter would have been contacted directly to offer him or her the opportunity to cure the signature issue. Once cured, staff would add the "Verified and Approved MCTEC" stamp to the envelope and it would be rescanned and sent to ballot processing and tabulation. To determine the exact path this envelope packet took, the County would need the Voter ID number.The conclusion that a "scribble" could not be viable as a valid signature, is incorrect. In addition to the fact that some people intentionally use a scribble as their signature, other people's signatures degrade or mature over time, even to a point of being a scribble. Below are the most common reasons that a signature could be inconsistent with the other signatures in the voter's registration record:

- Natural shifts and changes overtime
- Maturing (18-years-old versus 40-years-old)
- Deterioration with age
- Professional versus personal signature (i.e. physicians)
- Writing surface
- Writing instrument used to sign the envelope
- Medical conditions or illness impacting handwriting (i.e. stroke)

Blank Signatures

While voters are instructed to sign in the signature box, that doesn't always happen. If the scanned image of the signature area on the affidavit envelope is blank, the manager requests the actual physical packet to see if there is a signature somewhere else on the affidavit envelope. If there is a signature elsewhere that matches the signature on file, the manager would stamp the envelope "Verified and Approved MCTEC" and it would be rescanned for retention of that updated second-scan image and consequently sent to ballot processing and tabulation as valid to count. If there is no signature, the voter is notified by mail, email, text and phone (if available in the voter record and/or signed up for text alerts). Voters had until 7 p.m. on Election Day to sign the envelope or vote a new ballot in-person. If the voter signs the envelope prior to the deadline, staff would add the "Verified

ENVELOPES Image #2 - Signature Outside Box



(Above) Image from EchoMail's September 24, 2021 presentation to the Senate (Page 96).

and Approved MCTEC" stamp and send it to be rescanned. An envelope is not opened unless there is an approved and verified signature.

EchoMail stated they "analyzed, solely [the] signature region" inside the scanned image of the signature box. Without this additional inspection of the full, physical affidavit envelope packet, there can be no conclusions on whether the envelope had a signature. Further proof of this within EchoMail's September 24 presentation (see *ENVELOPES Image #2)*. EchoMail indicated the image was a "blank signature." But it looks to have a signature in the phone number region. If this were the case and the signature matched the voter registration records, that ballot would be counted.

Increase in Envelopes but Decrease in Signature Rejections

EchoMail Report (pg. 15): "While the number of EVB return envelopes in Maricopa for the 2016 general election increased…for the 2020 general election… the number of rejections from Signature Mismatches…decreased. This inverse relationship requires an explanation."

The explanation is simple. The law changed. The increase in the number of cured signatures as compared to 2016 is a result of a law passed in 2019, that allows voters five business days after Election Day to cure a questioned signature. The law also requires that blank envelopes must be signed by the voter no later than 7 p.m. on Election Day. As Maricopa County planned for a large number of early ballots dropped off on Election Day, combined with the new curing law, the Elections Department hired 40 additional staff to work October 30 to November 6, 2020. These employees were specifically assigned to contact voters with questioned signatures to offer them the opportunity to cure their signatures, as the law requires.

Daily Duplicate Numbers

EchoMail Report (pg. 74-75): "The graph reveals a significant surge of 7,797 Duplicates during the six days from 11/04/2020 to 11/09/2020."

There are several reasons why more envelope image scans are completed following the election. Arizona law does not require voters to mail their early ballots to the Elections Department. In addition to returning their ballot by mail, a voter is legally allowed to return their voted early ballots to ballot drop boxes at officially designated locations, including voting locations. More than 170,000 early ballots were dropped off on Election Day. On page 85, EchoMail states that "over 85% of the daily" early ballot return envelopes are duplicates. This is consistent with the fact that if a signature is questioned, staff has only a week following the election to contact the voter and offer the voter the opportunity to cure the signature issue. Staff work quickly to identify a signature issue and contact the voter.

Stamped in Signature Region

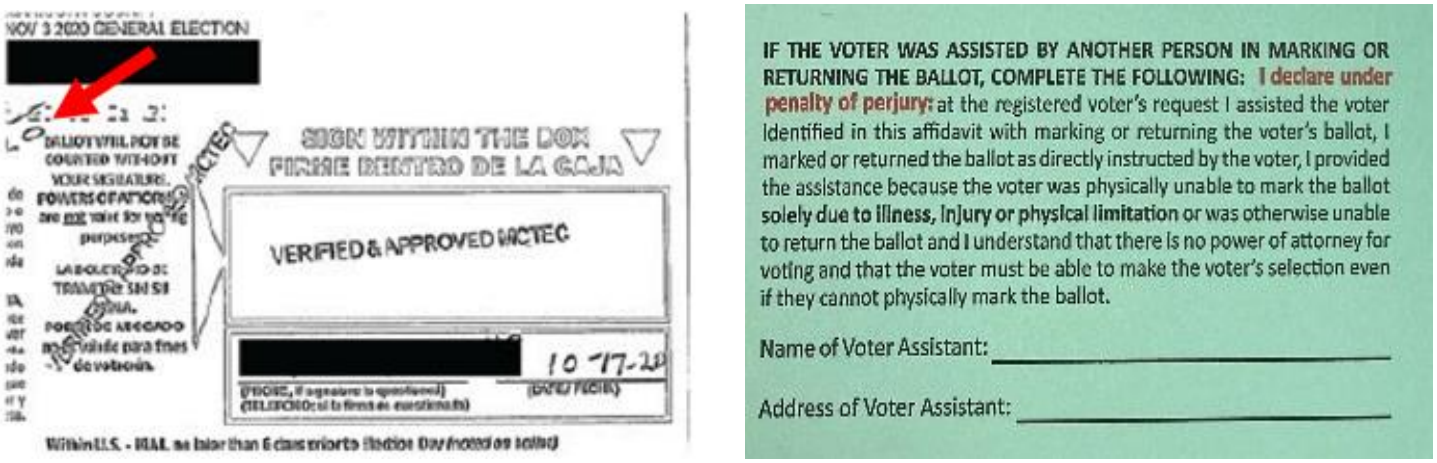
EchoMail Report (pg. 79): Two verified and approved stamps on a single image scan.

There are viable reasons why two "Verified and Approved MCTEC" stamps would appear on a single image scan (see *ENVELOPES Image #3)*. Upon review of the full packet, the staff is adding clarity when a signature is found outside of the clipped signature window. See the image to the left where the red arrow is pointed to what appears to be the voter's signature outside of the "Signature Region" that EchoMail inspected for its analysis.

Alternatively, this can occur when a voter is assisted by a Special Election Board (SEB), such as a disabled voter who does not have use of his/her hands. These boards are made up of two members from differing political parties as outlined in

A.R.S. § 16-549. If a voter is unable to make a mark, the Board can indicate this and sign to the left of the affidavit's signature block in the assistance attestation section also shown above (i.e. Name of Voter Assistant). The Board then uses the "Verified

ENVELOPES Image #3 - Two Verified & Approved Stamps on Envelope



(Left) Image from the EchoMail Report on page 96 of an envelope with two "Verified and Approved MCTEC" stamps. The red arrow was added by the County for clarify. (Right) Image of the early ballot assistance attestation section on the outside of the early ballot affidavit envelope.

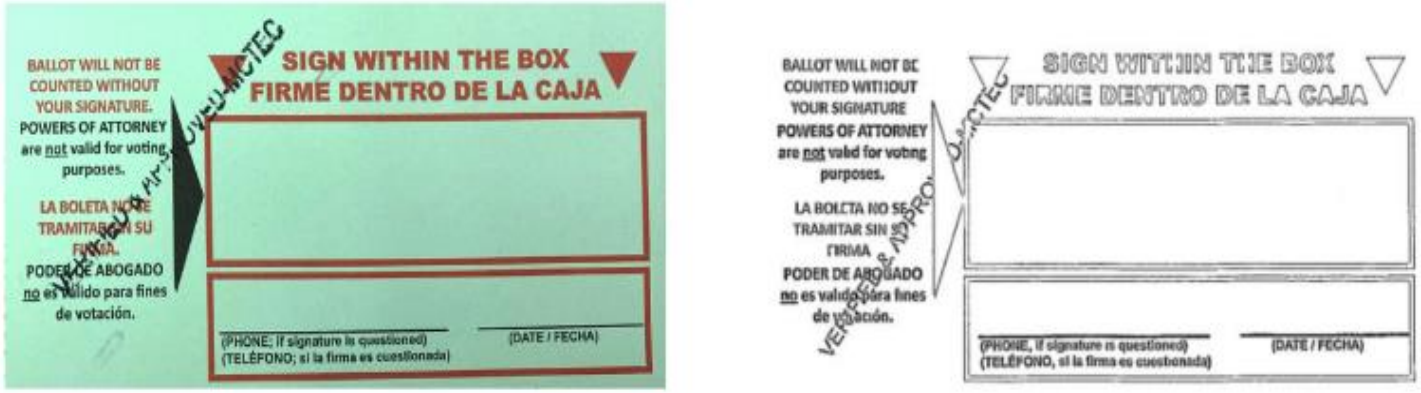
and Approved MCTEC" stamp so signature verification staff know the voter's identity was verified.

Stamp Behind the Envelope Triangle

EchoMail Report (pg. 84): Verified and approved behind the envelope triangle.

The reason the scanned stamp looks like it's behind the triangle is due to a common practice on high-speed scanners called "binary image format," which means the scanner takes a black pixel or a white pixel only capture. When an early ballot affidavit envelope is returned, it is scanned using this process. The binary image process looks to enhance edges.

ENVELOPES Image #4 - Verified & Approved Stamp Behind the Triangle



(Left) Image of the "Verified and Approved MCTEC" stamp on an early ballot affidavit envelope not using a high-speed scanner. (Right) Image of the "Verified and Approved MCTEC" stamp on an early ballot affidavit envelope after it was scanned using a binary image format.

Once the edges are determined, any filled area on that binary scan is "hollowed out" and only shows the outline of the shape or words (left image). This process improves speed and readability while reducing file size. While the "Verified and Approved MCTEC" stamp is used after the rigorous verification process described above, it appears to be behind the "hollowed out" arrow because it is stamped over the black and red arrows. Images captured in a binary format are standard within the industry and used by most mail sorters to:

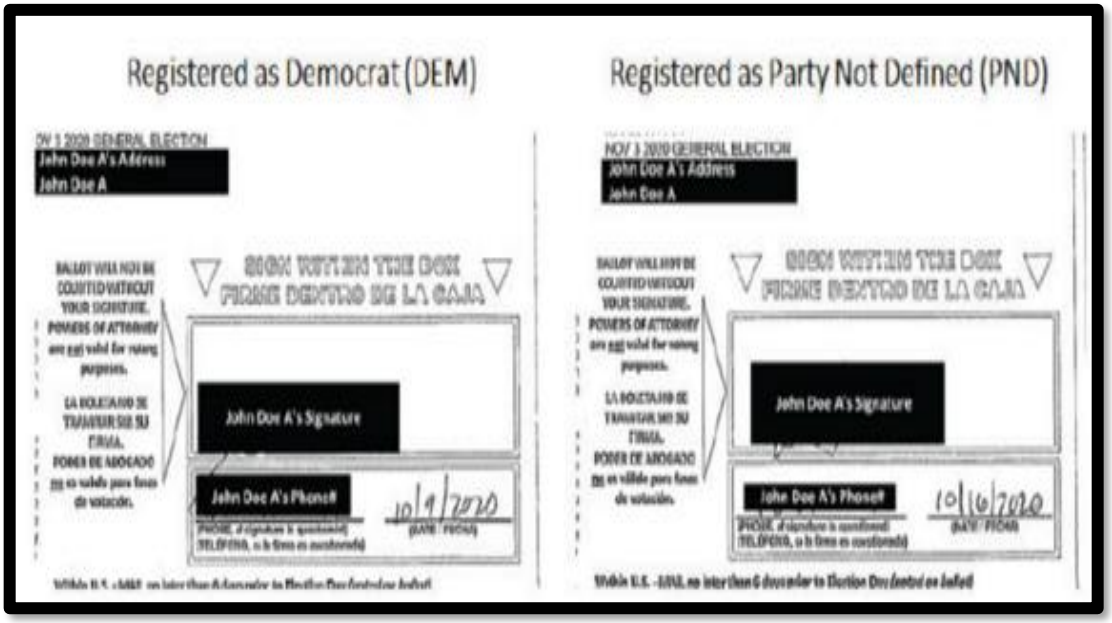
- enhance the barcodes for readability
- reduce image size
- increase rate of transmission across the network for saving the image — the high-speed scanners used to scan in early ballot envelope returns read and take images of 12-15 envelopes per second
- improve resolution — the high-speed scanners used to scan in early ballot envelope returns captures images at approximately 250 dpi. A color scanner would reduce resolution to 100 dpi at these speeds.

Two-Different Voter IDs

EchoMail Report (pg. 85-86): Same Name, Same Signature, Same Phone, Two Different Voter-IDs

Maricopa County has instances of voters with the same name in the same household (e.g., Sr. and Jr.). The example provided on page 85 of the Echo Mail Report and shown in *ENVELOPES Image #5* below shows that in fact the signatures are different. On the left image, the first name downstroke at the beginning of the signature goes into the phone number. The visible markings on the packet on the right stay closer to the bottom of the signature area. Additionally, the dates signed on the affidavits are different. To verify the actual circumstance with certainty, the County would need the Voter IDs associated with these sample records shown in the EchoMail report.

ENVELOPES Image #5 - Two Envelopes, Same Name



(Left) Image from EchoMail Report on page 85 of show two separate envelopes

Item #14: Damaged and Duplicated Ballots

(Cyber Ninjas Volume III Report Sections – 5.5.2, 5.6.2, 5.6.14, 5.7.3)

Cyber Ninjas made four claims about Maricopa County's ballot duplication process. These claims demonstrate a lack of understanding of state law and elections procedures. Additionally, the Senate's machine count also found a variance from Cyber Ninjas' hand count, which reviewed the duplicated numbers below. Those discrepancies cast doubt on the reliability of Cyber Ninjas' methodology and results. All of Cyber Ninjas' claims described below are inaccurate and cannot be substantiated.

Cyber Ninja Volume III			County Analysis	
Reference	Claim	Ballots		
5.5.2 (pg. 13)	"More Duplicates than Original Ballots"	2,592	0	No ballots were found counter to A.R.S. § 16-621(A) or the Elections Procedures Manual (Pg. 201-202)
5.6.2 (pg. 22)	"Duplicated Ballots Incorrect & Missing Serial Numbers"	~500	0	
5.6.14 (pg. 47)	"Duplicate Ballots Reuse Serial Numbers"	6	0	
Total(s)		4,981	0	
5.7.3 (pg. 50)	"Commingled Damaged and Original Ballots"	N/A	Inaccurate Claim	

State & Federal Laws

A.R.S. § 16-621(A) governs how "damaged or defective" ballots that can't be run through the tabulation equipment should be duplicated.

Maricopa County Findings

Summary

5.5.2 (More Duplicates than Originals), 5.6.2 (Duplicated Ballots Incorrect or Missing Serial Numbers), 5.6.14 (Duplicated Ballots Reuse Serial Numbers) & 5.7.3 (Comingled Damaged and Original Ballots)

> **The courts that examined the County's duplication process found that the process was reliable. There was no evidence of fraud and only a very minimal number of human duplication errors, which the courts conclude had no bearing on the election outcome. At no point were illegitimate ballots duplicated and the County has a thorough accounting of all duplicated ballots.**

Response and Analysis

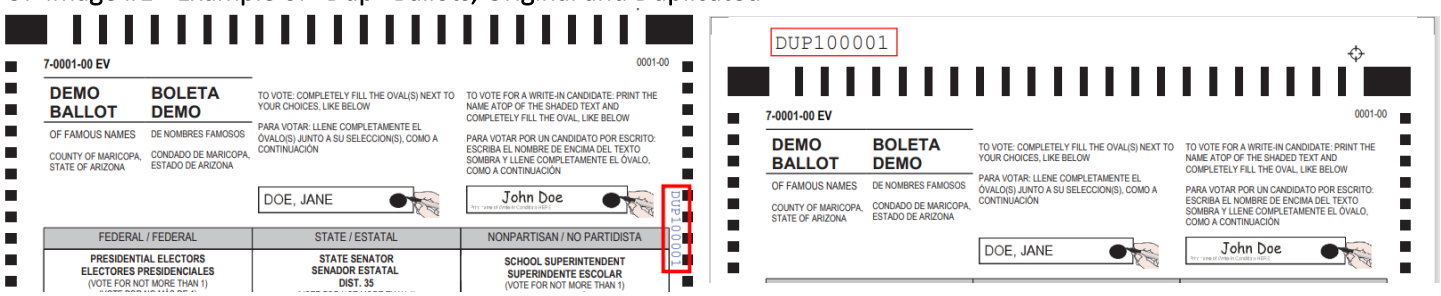
The accuracy and completeness of Maricopa County's duplication process was confirmed in court (*Ward v. Jackson*) where the court ordered a random sampling of 1,626 of the more than 27,000 duplicated ballots that, because of damage or for other reasons, had to be duplicated by bipartisan duplication teams. The court found that the duplication process was reliable, with only a very small number of duplication errors, none of which affected the election outcome and are not evidence of fraud. The Arizona Supreme Court affirmed the lower court ruling, "conclude[ing], unanimously, that . . the

challenge fails to present any evidence of 'misconduct,' 'illegal votes' or that the Biden Electors 'did not in fact receive the highest number of votes for office,' let alone establish any degree of fraud or a sufficient error rate that would undermine the certainty of the election results." (Ariz. S. Ct., December 9, 2020)

At no point were illegitimate ballots duplicated or inserted into the duplication process. Because the different sizes and formats of ballots cast by voters who are in the military, temporarily overseas, vote using large print or braille ballots, Maricopa County duplicates these ballots as prescribed for in A.R.S. § 16-621(A) and the Elections Procedures Manual (EPM) 2019 (Pg. 201-202). As required by these same laws, the County does the same for ballots that are returned too damaged to be read by the tabulator. During the duplication process, the Elections Department assigns a matching serial number to both the original and duplicated ballot.

If the original ballot is of standard size and can be scanned by our duplication scanners, we scan the ballot using a commercial scanner. We call these duplicated ballots "Dups." The scanner automatically assigns a sequential serial number and prints this number on the left side of the (original) ballot near the timing marks. Our duplication system then affixes a matching serial number to the top of the (duplicated) ballot. For an example see *DUP Image #1* below.

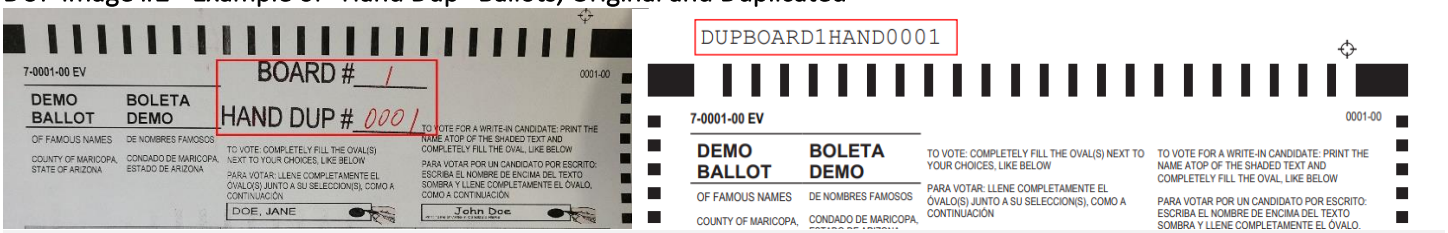
DUP Image #1 - Example of "Dup" Ballots, Original and Duplicated



(Left) An example of an original ballot with a scanned serial number near the timing marks. (Right) An example of a duplicated ballot with a marrying number at the top of the ballot.

If the original ballot is a large print, braille, UOCAVA, or damaged ballot that cannot be scanned, we use a physical stamp that includes the board number and the system generated hand duplication number. We call these duplicated ballots "Hand Dups." When the bipartisan citizen boards duplicate these Hand Dup ballots, the system automatically assigns a sequential marrying number. The duplicated ballot will have this number affixed to the top of the ballot. The citizen boards are instructed to write this system generated serial number on the original ballot. For an example see DUP Image #2 below.

DUP Image #2 - Example of "Hand Dup" Ballots, Original and Duplicated

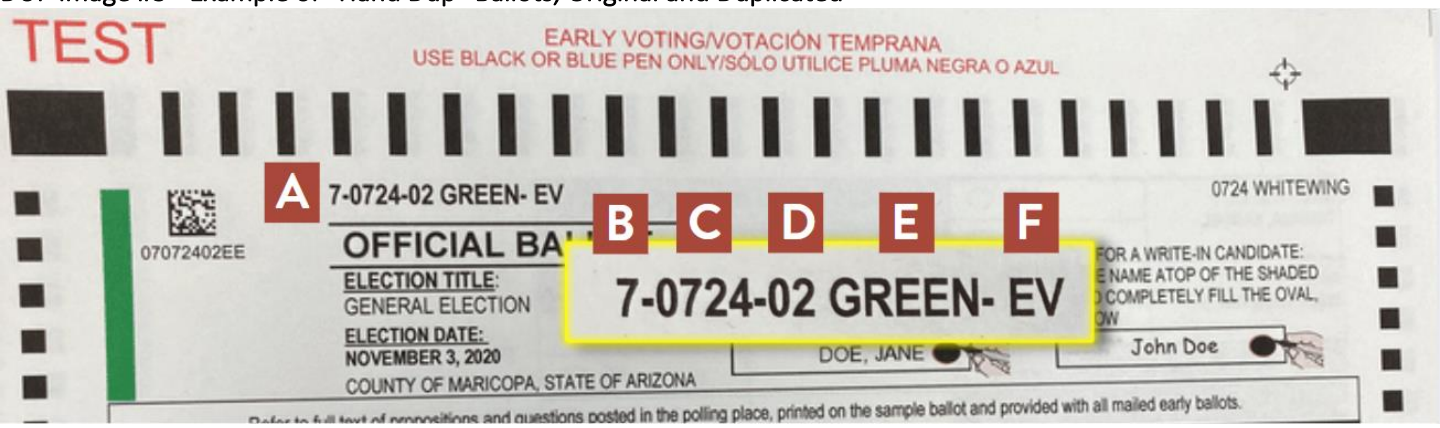


(Left) An example of an original ballot with a hand dupped serial number near the timing marks. (Right) An example of a hand duplicated ballot with a marrying number at the top of the ballot.

There are several indicators that are used to match the original ballot with the duplicated ballot. The system generated numbers, the ballot type and the ballot style. Each ballot has a *type* (EV – Early, ED – Election Day, PV – Provisional) that is identified on the top left of the ballot (see *DUP Image #3*). In the November 2020 General Election there were also 10,920 unique ballot *styles* depending on the voter's precinct, precinct split, language preference, or federal only registration status. This information is found on the top of the ballot as well and can also be used to match the original ballot with the duplicated ballot. Below is an example of a ballot style, each letter corresponds to its purpose.

- A – the entire letter and number sequence is the ballot style
- B – this is only customized in a primary election when voters choose a party ballot
- C – this is the precinct number
- D – this indicates the number of boundary splits within a precinct, meaning there are multiple ballot styles within the precinct
- E – a color is assigned for each precinct split (green, gold, purple etc.)
- F – this is the ballot type. It could be EV (early ballot), ED (Election Day ballot) or PV (provisional ballot)

DUP Image #3 - Example of "Hand Dup" Ballots, Original and Duplicated



(Above) An image of the letters and numbers within the ballot style code. See bulleted list above for descriptions.

2,592 Ballots

5.5.2 – Appendix F1 and F2 (More Duplicates Than Original Ballots)

On page 13, Cyber Ninjas claim that their comparison of original, damaged ballots to duplicate ballots found a discrepancy of 2,592 ballots. The County has a detailed record of all original ballots that were sent to duplication and subsequently duplicated (see *Exhibit - DUPLICATED BALLOTS*). This listing shows that there were 1,748 Election Day ballots and 26,131 early ballots. This totals 27,879, the amount that the County reported during the *Ward v. Jackson* court case. We cannot determine why Cyber Ninjas obtained a different count, but it has been reported that during Cyber Ninjas' hand count, observers noted contractors spilled a box of UOCAVA ballots "across the Coliseum floor." The Senate's machine count also found variance from the hand count, which is an indication that Cyber Ninjas' hand count process was unreliable.

~500 & 6

5.6.2 (Duplicated Ballots Incorrect & Missing Serial Numbers) and Section 5.6.14 (Duplicate Ballots Reuse Serial Numbers)

The County is not aware of any instances in which an original or duplicated ballot was missing a serial number. Cyber Ninjas did not provide a data set that included any information by which to compare. The County acknowledges that there may be some instances where the serial number was printed over a timing mark on the original damaged ballot. This may make it difficult to read the serial number on the original ballot. Since the duplicated ballot and not the original is tabulated, the added serial number overlapping a timing mark does not impact tabulation.

The County has also identified 27 instances where a similar serial number was used for both "Dup" and "Hand Dup" ballots. Due to the three indicators that are used to match the original ballot with the duplicated ballot (dup number, ballot style and ballot type), the original and duplicate ballot could be matched in all instances, which means that there is no confusion concerning which original corresponds to which duplicated ballot (see *DUP BALLOTS Table #1*).

DUP BALLOTS Table #1 - Maricopa County's Analysis of Duplicated Ballots with Similar Serial Numbers			
Duplication Number	1st Ballot Type/Style	2nd Ballot Type/Style	Can Ballots Be Matched?
DUPBOARD4HAND0005	Early Ballot-07066501EE	Election Day Ballot-07044100PE	Yes
DUPBOARD4HAND0003	Early Ballot-07023101EE	Election Day Ballot-07025301PE	Yes
DUPBOARD4HAND0007	Early Ballot-07040100EE	Election Day Ballot-07069001PE	Yes
DUPBOARD4HAND0008	Early Ballot-07041099EE	Election Day Ballot-07028201PE	Yes
DUPBOARD4HAND0004	Early Ballot-07034801EE	Election Day Ballot-07067101PE	Yes
DUPBOARD9HAND0165	Early Ballot-07008500EE	Early Ballot-07034100EE	Yes
DUPBOARD4HAND0006	Early Ballot-07066501EE	Election Day Ballot-07011100PE	Yes
DUPBOARD4HAND0001	Early Ballot-07018900EE	Election Day Ballot-07025200PE	Yes
DUPBOARD4HAND0002	Early Ballot-07039400EE	Election Day Ballot-07067700PE	Yes
DUPBOARD4HAND0009	Early Ballot-07044100EE	Election Day Ballot-07069700PE	Yes
DUPBOARD2HAND0001	Early Ballot-07073999EE	Election Day Ballot-07018201DE	Yes
DUPBOARD13HAND0005	Early Ballot-07074300EE	Election Day Ballot-07029000DE	Yes
DUPBOARD13HAND0003	Early Ballot-07009501EE	Election Day Ballot-07040801DE	Yes
DUPBOARD11HAND0001	Early Ballot-07012099EE	Election Day Ballot-07025601DE	Yes
DUPBOARD15HAND0002	Early Ballot-07059000EE	Election Day Ballot-07051199PE	Yes
DUPBOARD11HAND0002	Early Ballot-07009499EE	Election Day Ballot-07030700DE	Yes
DUPBOARD13HAND0002	Early Ballot-07044100EE	Election Day Ballot-07029802DE	Yes
DUPBOARD11HAND0003	Early Ballot-07022400EE	Election Day Ballot-07064200DE	Yes
DUPBOARD13HAND0004	Early Ballot-07071300EE	Election Day Ballot-07023500DE	Yes
DUPBOARD11HAND0004	Early Ballot-07023799EE	Election Day Ballot-07050000DE	Yes
DUPBOARD15HAND0001	Early Ballot-07026099EE	Election Day Ballot-07020599PE	Yes
DUPBOARD11HAND0005	Early Ballot-07003000EE	Election Day Ballot-07045600DE	Yes
DUPBOARD15HAND0003	Early Ballot-07026099EE	Election Day Ballot-07044700PE	Yes
DUPBOARD11HAND0006	Early Ballot-07033700EE	Election Day Ballot-07034100DE	Yes
DUPBOARD2HAND0002	Early Ballot-07051599EE	Election Day Ballot-07027801DE	Yes
DUPBOARD13HAND0001	Early Ballot-07005602EE	Election Day Ballot-07015801DE	Yes
DUPBOARD2HAND0003	Early Ballot-07063200EE	Election Day Ballot-07008900DE	Yes

The County incorporates a continuous improvement philosophy in all of our processes and decision making. When evaluating our duplication process, we had already begin making changes prior to Cyber Ninjas' review. During the 2021 election cycle, we took steps to prevent the duplication number from being printed over the timing marks and are incorporating additional indicators to streamline the serial numbers.

Informational

Section 5.7.3 (Commingled, Damaged, and Original Ballots)

On page 50 of its report, Cyber Ninjas incorrectly state that the County commingled original ballots with duplicated ballots. This is not accurate. All 14 batches listed in Cyber Ninjas report were tabulated ballots and did not contain any original ballots that were sent to duplication.

Cyber Ninjas further claim that both the original ballot and the duplicated ballots must be stored separately. This is also not accurate. There is no statutory requirement to store tabulated ballots in separate boxes – whether that ballot was duplicated or not.

DUP Image #4 – Ballot Custody Transfer Manifest

Pallet #	Box # (Ballot Type, Machine, Date, First Batch)		Batches
41		1	Original Ballots/Damaged/Sent to Duplication
41		2	Original Ballots/Damaged/Sent to Duplication
41		3	Original Ballots/Damaged/Sent to Duplication
41		4	Original Ballots/Damaged/Sent to Duplication
41		5	Original Ballots/Damaged/Sent to Duplication
41		6	Original Ballots/Damaged/Sent to Duplication
41		7	Original Ballots/Damaged/Sent to Duplication
41		8	Original Ballots/Damaged/Sent to Duplication
41		9	Original Ballots/Damaged/Sent to Duplication
41		10	Original Ballots/Damaged/Sent to Duplication
41		11	Original Ballots/Damaged/Sent to Duplication
41		12	Original Ballots/Damaged/Sent to Duplication
41		13	Original Ballots/Damaged/Sent to Duplication
41		14	Original Ballots/Damaged/Sent to Duplication
41		15	Original Ballots/Damaged/Sent to Duplication
41		16	Original Ballots/Damaged/Sent to Duplication
41		1	Braille Original to Duplication
41		2	Braille Original to Duplication
41		3	Braille Original to Duplication
41		1	Large Print Original to Duplication
41		2	Large Print Original to Duplication
41		3	Large Print Original to Duplication
41		1	Election Day Damaged Original to Duplication
41		1	Provisional Damaged Original to Duplication

(Above) Screenshot from page 4 of the Ballot Custody Transfer Manifest

There is, however, a requirement in the Elections Procedures Manual (pg. 202) that states the original ballot that needed to be duplicated must be contained in its own box and clearly marked. All of these ballots from the November 2020 General Election were segregated and the boxes were marked as Original Ballots/Damaged Ballots/Sent to Duplication, Braille Original to Duplication, Large Print Original to Duplication, etc. These original ballots were all included on pallet #41 when delivered to the Senate on March 3, 2021 as commanded by the January 2021 subpoena (*see DUP Image #4*). The County prepared the Ballot Custody Transfer Manifest to track the items provided to the Senate. That manifest included a summary the pallets and what was inside the sealed boxes (see *Exhibit - MANIFEST*).

Item #15: Ballots and Batch Discrepancies

(Cyber Ninjas Volume III Report Sections – 5.6.12, 5.7.2)

Cyber Ninjas' report included two claims about the County's counting and handling of ballots. Our analysis and findings are summarized below.

Cyber Ninja Volume III			County Analysis
Reference	Claim	Ballots	
5.6.12 (pg. 45)	Double Scanned & Counted Ballots	50	50
5.7.2 (pg. 48)	Batch Discrepancies	N/A	False Claim

Maricopa County Findings

Summary

5.6.12 (Double Scanned Ballots) & 5.7.2 (Batch Discrepancies)

> **After Maricopa County's post-election review of all 2,089,563 ballot IDs, it appears that 50 ballots in one batch were scanned twice. This had no impact on the outcome of any contest.**

Response and Analysis

As part of the County's post-election review, we performed an analysis of the Cast Vote Record and all 2,089,563 unique ballot IDs. The Cast Vote Record is a complete log of how every contest was tabulated for every ballot. It also captures other information about the ballot including the ballot precinct, whether the ballot was adjudicated, and what percent of each oval was completed. By using the information listed below, we can create enough unique pieces of information to determine if there are any instances where a ballot's unique characteristics, matches another ballot's unique characteristics. If so, this could be an indication of a ballot being scanned twice.

- Ballot Style – In the November 2020 General Election there were 10,920 unique ballot styles, which have a unique letter and number sequence. Ballots are customized to ensure voters only vote for the contests and candidates in their area.
- Contests Voted – In the November 2020 General Election the majority of ballots had over 60 contests, with some ballots exceeding 70 contests.
- Percent of Oval Completed within 2% – Voters frequently only complete a portion of each oval. Given 60-70 contests, it is not likely for a voter to complete every oval the same as another voter.

After performing this analysis, we found 137 ballots that had the same combination of unique characteristics to another ballot. We then compared the images for these 137 and found that 87 were unique ballots and not a double counted ballot. After further review, it appears that a tabulator operator inadvertently included an already tabulated stack of 50 ballots from a previous batch in a subsequent batch. The two batches are listed below.

- Tabulator ID# 6004, Batch 287, Ballots 1 – 50 (50 ballots correctly scanned)

- Tabulator ID# 6004, Batch 288, Ballots 150-199 (50 ballots from the previous batch appear have been scanned again)

During the election, tabulation staff and political party observers perform a reconciliation of total ballots tabulated before and after each shift by comparing and confirming the totals on the tabulator screens to the totals collected in the previous shift. The 50-ballot-discrepancy was not identified because the totals from each central count tabulator matched the totals from the tabulation operator logs and early voting ballot reports (created by the bipartisan ballot processing board).

The County performed a review of the votes that were cast on these ballots for every contest and found that the double scanning of 50 ballots did not have an impact on the outcome of any contest. The *BALLOTS Table #1* below provides the vote counts from the 50 double scanned ballots for the Presidential Electors and U.S. Senate Contests.

BALLOTS Table #1 – Results of Presidential and Senate Contests from Batch 287 & 288			
Contest / Candidate	Batch 287 & 288	Impacted Votes	Net Impact on Contest
Presidential Electors (Trump)	188	17	14 - votes more for Biden
Presidential Electors (Biden)	195	31	
Presidential Electors (Jorgensen)	7	1	
Write-in	4	0	
Presidential Electors (Undervotes)	4	1	
Presidential Electors (Overvotes)	1	0	
U.S. Senate (McSally)	182	17	15 - votes more for Kelly
U.S. Senate (Kelly)	207	32	
U.S. Senate (Undervotes)	10	1	
U.S. Senate (Overvotes)	0	0	

No Batch Discrepancies

On Page 48 of Cyber Ninjas' report, they incorrectly conclude that the number of ballots in batch numbers listed in the Cast Vote Record do not match the total number of ballots listed on the blue tabulator operator logs. To support their claim, Cyber Ninjas' show an example of a blue operator log dated 10/31/2020, that logs activity from that day for Central Count Tabulator - Cannon 1. Cyber Ninjas compare these batch totals to the Cast Vote Record for Tabulator ID# 6001, batches 40 and 41.

However, to better organize ballots and to maintain efficient use of storage space, we limit the total number of batches for each tabulator to no more than 1,000 batches. Once we approach 1,000 batches on a single central count tabulator, we renumber the tabulators and restart batches at number 1. On October 28, we were approaching 1,000 batches counted on several of our central count tabulators. We renumbered each of the tabulators to the next sequential number and restarted batch numbers at #1 for all tabulators. For Cannon Central Count #1, the new assigned sequential number was 6021 instead of 6001. According to the Cast Vote records, the blue tabulator logs match with the Cast Vote Record for Tabulator ID# 6021, batches 40 and 41.

Item #16: UOCAVA Ballots

(Cyber Ninjas Volume III Report Sections – 5.6.7, 5.6.13, and 5.7.7)

Cyber Ninjas' report included three claims that made faulty or inaccurate statements about the County's processing or reporting of Uniformed and Overseas Citizens Absentee Voting Act (UOCAVA) ballots. Their claims were based on faulty data sets and a lack of understanding of elections administration.

Cyber Ninja Volume III			County Analysis
Reference	Claim	Ballots	
5.6.7 (pg. 30)	"Audit UOCAVA Count Does Not Match the EAC Count"	226	0
5.6.13 (pg.46)	"UOCAVA Electronic Ballots Double Counted"	6	0
Total(s)		232	0
5.7.7 (pg. 55)	"Inaccurate Identification of UOCAVA ballots"	N/A	False Claim

State & Federal Laws

There are both state and federal and laws that provide additional protections for active military and overseas voters. The Uniformed and Overseas Citizens Absentee Voting Act is commonly referred to as UOCAVA. UOCAVA citizens are U.S. citizens who are active members of the Uniformed Services, the Merchant Marine, and the commissioned corps of the Public Health Service and the National Oceanic and Atmospheric Administration, their eligible family members, and U.S. citizens residing outside the United States. This Act provides the legal basis for these citizens' absentee voting requirements for federal offices. The Military and Overseas Voter Empowerment Act (MOVE) amended UOCAVA and other statutes by providing greater protections for Service Members, their eligible family members and other overseas citizens. Among other provisions, the MOVE Act requires states to send absentee ballots to UOCAVA voters at least 45 days before federal elections. Applicable Arizona laws include:

- A.R.S. § 16-542(B)
- A.R.S. § 16-543
- A.R.S. § 16-543.02

Maricopa County Findings

Summary

5.6.7 (Audit UOCAVA Count Does Not Match the EAC Count)

> **Cyber Ninjas incorrectly identified the number of UOCAVA ballots reported by the County to the U.S. Election Assistance Commission for the EAVS Report.**

Response and Analysis

When performing this review, Cyber Ninjas used the incorrect data set from the Election Administration and Voting Survey (EAVS) Report, a state-by-state report that covers data on various topics related to the administration of federal elections published by the U.S. Elections Assistance Commission. On page 30 of Cyber Ninjas report they state that there were 10,408 UOCAVA ballots cast in Maricopa County during the 2020 General Election as reported by the EAVS report. It appears Cyber Ninjas pulled data from the wrong section.

The EAVS report actually shows there are 10,396 UOCAVA ballots that were successfully counted for the November 2020 General Election and not 10,408. See *UOCAVA Image #1* below, which is from sections B14 through B17 of the Arizona specific EAVS Report that shows "Ballots Counted" as 10,396 (8,986 Electronic Voters + 1,410 Mail Voters). "Postal mail" are UOCAVA ballots returned by mail and "other mode" are ballots returned by fax or a secure electronic portal. This misstep in reading the EAVS report points to the lack of expertise by Cyber Ninjas on conducting research or interpreting election related data.

UOCAVA Image #1 - 2020 EAVS Report- Section B14-B17

UOCAVA Ballots Counted: Questions B14-B17

B14–B17. UOCAVA Ballots Counted: Postal Mail, Email, Other

For these questions, we are interested in how many UOCAVA absentee ballots were counted for the November 2020 general election. For question B14, please report, out of all UOCAVA ballots returned by voters (as reported in B9a), the total number of ballots that were counted by your office for the 2020 general election. *Please EXCLUDE Federal Write-In Absentee Ballots (FWAB) from your totals. You will report data on FWABs starting with question B23.*

We are interested in knowing how many of the absentee ballots were returned and counted by postal mail (B15), email (B16), or other (B17). For questions B15–B17, divide the total number of UOCAVA absentee ballots counted (as reported in B14a) into the following categories of types of voters and modes of transmission.

	a. TOTAL[?]	a. Data not available	b. Uniformed Services voters Members of the Uniformed Services and their eligible dependents—domestic or foreign[?]	b. Data not available	c. Non-military/civilian overseas voters	c. Data not available	Does not apply
B14. TOTAL: Of all UOCAVA ballots returned by voters as reported in B9a, report the total number of ballots that were counted by your office for the 2020 general election. Do not include FWABs in this number. [?]	10396		3380		7016		
B15. Postal mail: Report the total number of UOCAVA ballots returned by postal mail that were counted by your office for the 2020 general election. This includes all ballots that your office received via the USPS or private courier shipping services (e.g., FedEx, UPS, DHL).[?]	1410		1116		294		
B17. Other mode: Report the total number of UOCAVA ballots returned through other methods that were counted by your office for the 2020 general election. This includes ballots received through all other modes, such as, fax, online systems, etc.[?] [?]	8986		2264		6722		

(Above) Screenshot of the 2020 EAVS Report, Section B14-B17, which shows Arizona's UOCAVA ballots returned by mail, fax or a secure electronic portal.

Cyber Ninjas' analysis further claims that there were 226 more electronically submitted UOCAVA ballots than the EAC reported total, which because of the misstep noted above, the corrected sum would now be 228. On page 30 of its report, Cyber Ninjas indicate that they had 9,214 electronically returned ballots "observed during the audit," which was "226 more electronically submitted UOCAVA ballots than the County reported to the EAC" when compared to the 8,988 they incorrectly found to be reported in that EAVS report – which is actually 8,986 reported to EAC for electronically counted UOCAVA ballots.

Regardless of their reported total, the County has a detailed record of voter-by-voter UOCAVA data records (see *Exhibit - UOCAVA*). This listing shows that there were 10,396 UOCAVA ballots returned and counted, 1,410 returned by mail and 8,986 returned electronically, which matches the EAVS report. We cannot determine why Cyber Ninjas obtained a different count. However, it has been reported that during Cyber Ninjas' hand count, observers noted contractors spilled a box of UOCAVA ballots "across the Coliseum floor." The Senate's machine count also found a variance from the hand count, which is an indication that Cyber Ninjas' hand count process was unreliable.

Summary

5.6.13 (UOCAVA Electronic Ballots Double Counted)

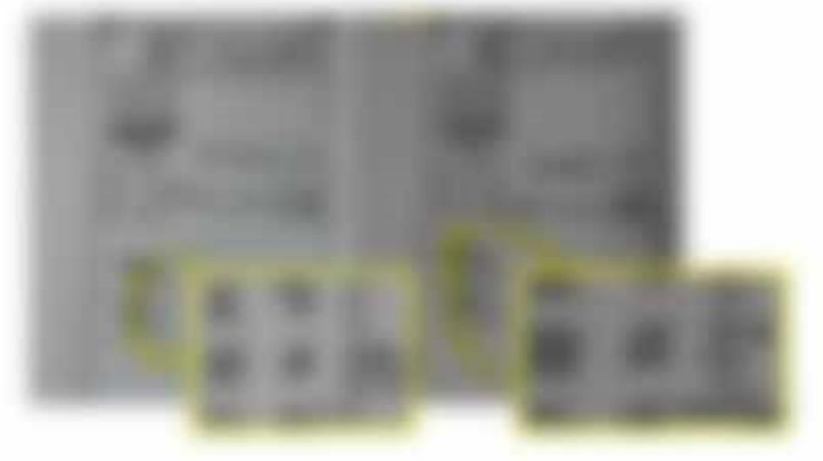
Cyber Ninjas' misunderstanding of the UOCAVA process resulted in an incorrect assumption that the County double counted UOCAVA voters' ballots. These ballots were voted by separate UOCAVA voters and returned in the same fax transmittal.

Response and Analysis

State and federal law provide military and overseas voters additional protections and time to participate in elections. The law allows UOCAVA voters to return ballots by mail, fax or through a secure electronic portal. While Cyber Ninjas did not provide the County with examples to support the six instances where they claim that a UOCAVA voter had their ballot counted twice, EchoMail included images for two of the six instances on Slide 21 of its presentation provided to the Arizona Senate. Upon inspection of the two separate ballots in the presentation images, it is clear that the ovals for the three voted contests (Presidential, U.S. Senate, and U.S. Representative) on the ballot are not filled-in using a similar fill pattern (see *UOCAVA Image #1. Note: To comply with the Arizona Constitution's guarantee of secrecy of the ballot, as well as A.R.S. § 16-1018(4), which prohibits showing voted ballots in a way that reveals the contents, we have blurred the images taken from the Echo Mail presentation*). This should have been the first indicator to Cyber Ninjas that these ballots were not completed by the same voter.

Since Cyber Ninjas had never previously examined the results of an election and are decidedly not election experts, they may not understand that there are instances where multiple UOCAVA voters (e.g., spouses, parents, adult children) may live together. In such instances, these UOCAVA household voters can and mostly likely would use the same fax to return their ballots to the Elections Department. In the photos, Cyber Ninjas highlight that the fax date and the "*from*" fax number are the same. Based on this information alone, they incorrectly conclude that this indicates that the ballots were the same ballot and counted twice. This is an inaccurate assumption. These ballots were from two separate voters within the same household who returned their voted ballots using the same fax machine and same fax transmission, hence the fax date header would show the same transmission date and the same "*from*" transmission fax number. We have verified in tracking back to the actual fax transmission from these voters that they are indeed accompanied with two faxed back signed affidavits from two different voters noted and shown on file to be in the same UOCAVA household.

UOCAVA Image #2 – UOCAVA Ballot Images from Cyber Ninjas' Presentation



(Above) Blurred Images of UOCAVA ballot images from Cyber Ninjas' September 25, 2021 presentation to the Senate (Slide 21).

Response and Analysis

5.7.7 (Inaccurate Identification of UOCAVA Ballots)

Cyber Ninjas include a finding where they state that the manifest the County used to transfer the ballots to the Senate does not identify which boxes contain UOCAVA ballots. The County had no operational need or statutory requirement to identify this information when the ballots were boxed and labeled, which occurred prior to the creation of the manifests.