IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ARIZONA

Kari Lake, *et al*, Plaintiffs, v. Katie Hobbs, Arizona Secretary of State, *et al.*, Defendants.	No. 2:22-cv-00677-JJT

DECLARATION OF BENJAMIN R. COTTON

I, Ben Cotton, being duly sworn, hereby depose and state as follows:

1) I am over the age of 18, and I understand and believe in the obligations of an oath. I make this affidavit of my own free will and based on first-hand information and my own personal observations.

2) I am the founder of CyFIR, LLC (CyFIR).

3) I have a master's degree in Information Technology Management from the University of Maryland University College. I have numerous technical certifications, including the Certified Information Systems Security Professional (CISSP), Microsoft Certified Professional (MCP), Network+, and Certified CyFIR Forensics and Incident Response Examiner.

4) I have over twenty-six (26) years of experience performing computer forensics and other digital systems analysis.

5) I have over nineteen (19) years of experience as an instructor of computer

forensics and incident response. This experience includes thirteen (13) years of experience teaching students on the Guidance Software (now OpenText) EnCase Investigator and EnCase Enterprise software.

6) I have testified as an expert witness in state courts, federal courts and before the United States Congress.

7) I have testified before the Arizona State Senate in public hearings on 15 July 2021 and 24 September 2021 concerning the digital forensics findings connected to the Arizona State Senate Maricopa County audit of the 2020 general elections. I fully stand behind those forensic findings. I have included my presentation to the State Senate, file name Senate Final Presentation.pdf, as Exhibit A to this affidavit.

8) I regularly lead engagements involving digital forensics for law firms, corporations, and government agencies and am experienced with the digital acquisition of evidence under the Federal Rules of Evidence.

9) In the course of my duties I have forensically examined Dominion Democracy Suite voting systems in Maricopa County Arizona, Antrim County Michigan, Mesa County Colorado, and Coffee County Georgia, hereinafter referred to as the "Analyzed Elections Systems".

10) In the course of my duties I have reviewed the administrative manuals and documentation for the Dominion Democracy Suite software and hardware components.

11) In the course of my duties I have reviewed the public information from the Election Assistance Commission and its certification process for election software.

12) I have reviewed and considered applicable Arizona law[1] concerning the certification and operation of electronic voting systems[2].

13) I have reviewed and considered the Pro V&V report dated 3/2/2022 concerning the programmatic errors of the Dominion tabulator titled "ICP Modification to Reset Provisional Flag on each Ballot Scan".

14) I have reviewed and considered Exhibits A through J in forming my opinion.

15) I have reviewed and considered the Maricopa Board of Supervisors' Response to the Arizona Senate dated 5-17-21 and named "2021.05.17 Response Letter to Senate President Fann - FINAL_202105171430291332.pdf".

16) I have reviewed and considered the published Department of Homeland Security, Cyber Security & Infrastructure Security Agency (CISA) Best Practices for Securing Election Systems dated 1 February 2021 and last revised on 25 August 2021. Publicly available, this document can be located at https://www.cisa.gov/tips/st19-002. This document provides recommendations for securing election systems in the following areas:

a) Software and Patch Management – Note: The Analyzed Election Systems do not Comply with CISA Recommendations

b) Log Management - Note: The Analyzed Election Systems do not Comply with CISA Recommendations

[1] Arizona Revised Statutes Title 16. Elections and Electors

[2] https://azsos.gov/sites/default/files/2019_ELECTIONS_PROCEDURES_MANUAL_APPROVED.pdf

c) Network Segmentation - Note: The Analyzed Election Systems Partially Comply with CISA Recommendations

d) Block Suspicious Activity - Note: The Analyzed Election Systems do not Comply with CISA Recommendations

e) Credential Management - Note: The Analyzed Election Systems do not Comply with CISA Recommendations

f) Baseline Establishment for Host and Network Activity - Note: The Analyzed Election Systems do not Comply with CISA Recommendations

g) Organization-Wide IT Guidance and Policies – Note: The Analyzed Election Systems Comply with CISA Recommendations

h) Notice and Consent Banners for Computer Systems – Note: The Analyzed Election Systems Comply with CISA Recommendations

17) In addition, in forming my opinions, I reviewed and considered Exhibits B, C, D, E, F, G, H, I, and J, of which true and accurate copies are also attached hereto.

18) Based on my reviews of these documents, my cyber security experience, and my forensic analysis and review of the Dominion voting systems experience I find the following specific to the Cyber Security protections observed in the examinations of the Dominion Democracy Suite:

a) **Failure to Update Antivirus Protections** - Based on my personal knowledge and experience, over one million (1,000,000) new malicious code samples are identified on a daily basis. It is imperative to the security of any computing system or enterprise that the antivirus definitions be updated as they become available, typically on a weekly basis. There is a systemic issue with all of the Analyzed Elections Systems. There was an antivirus program installed on each of the systems. None of the system's antivirus definitions had EVER been updated following the installation of the Dominion Democracy Suite Software. In terms of the Maricopa County election system, the antivirus software had not been updated for over 19 months. In practical terms, this means that the virus protection was so out of date that the system would not have prevented over five hundred seventy million (570,000,000) pieces of malicious code from compromising the voting system.

b) **Failure to Patch and Maintain Operating System (OS) Security** – The operating systems within the Analyzed Election Systems, including Windows, Linux and MacOS, contained vulnerabilities. These vulnerabilities could be exploited to gain unauthorized access to the targeted systems. Microsoft, the developer of the Windows software that was present on the Dominion PC-based Voting systems during my examination, releases operating system patches on a weekly basis to correct previously unknown operating system vulnerabilities and to prevent the possibility of unauthorized access to these systems. Based on my analysis of the Analyzed Election Systems in Maricopa County Arizona, Maricopa County Arizona, Fulton County Georgia, Antrim County Michigan, Mesa County Colorado, and Coffee County Georgia, there is no evidence of a procedure or process to patch or fix the operating system vulnerabilities on the voting systems. None of these organizations had patched the operating systems since the date that the Dominion Democracy Suite had been installed. In Maricopa County, the Windows operating systems had not been patched for over 19 months and contained fixes (patches) for three thousand five hundred twelve (3,512) known vulnerabilities directly applicable to the Maricopa County Dominion voting system. A list of these vulnerabilities is included as a file included with this report named, "Microsoft Patched Vulnerabilities between August 2019 and April 2021.xlsx (md5 hash value: D1E09A7C762E21653B1A28C3D9EE4E5E).

c) **Failure to Properly Establish and Control Assess to Voting Systems** - Based on my review and consideration of the Analyzed Election Systems from different jurisdictions it is apparent that there is a systemic problem with access controls to the voting systems. In each case the usernames and passwords were established concurrently with the installation of the voting software by the Dominion employees. There are two major issues with the password management of these systems. First, in all examinations of the Analyzed Election Systems, the passwords were identical for all user accounts on that unique system. For each unique jurisdiction, all passwords within that election system were the same for all user accounts. Second, these passwords were never changed by the local officials following the installation of the software. These two deficiencies result in long-term shared password exposure for multiple elections. Furthermore, there does not appear to be any accountability or assignment of the accounts to a specific individual for specific time periods. This makes individual accountability for actions performed by the account during an election impossible. CISA and industry best practices recommend that all username and password combinations be unique to each individual user. When that individual no longer requires access to the system, the username should be disabled to prevent unauthorized access to the system. When a new user arrives or is assigned, a new username and password are created for that user. Furthermore, CISA best practices dictate that each individual password should be changed every ninety (90) days. In the case of the Maricopa County devices, the passwords had not been changed for over nineteen (19) months, and no user accounts had ever been created following the installation of the Dominion software.

d) **No Process Monitoring, Network Monitoring or Baseline Monitoring** – Based on my review of the electronic voting systems from different jurisdictions, none of the jurisdictions had the capability to actively monitor programs that were running on the computers, monitor network activity, or had a process to alert election officials if a deviation from an approved baseline occurred.

e) **Log Management** – Retaining and adequately securing logs from both network devices and local hosts is a critical component of cyber security. Not only does a robust log management program support the detection and monitoring of real-time security postures, but in the event of an audit or a cyber security event, these logs support triage and remediation of the historical cybersecurity events. None of the election systems that I have examined have an independent log management program. An effective log management program should include the following capabilities:

i) **Centralized Log Management**: It is common for threat actors to delete, modify and/or otherwise manipulate logs and other artifacts as an integrated element of an unauthorized attack. An effective log management program would establish a centralized log repository that is not located on the device that generates the logged event. This method allows for potentially unlimited log retention time periods, assurance of log preservation, ensures the integrity of the logs, and establishes a data repository to aid in the detection of malicious behavior. None of the election systems that I have analyzed forwarded logs to a centralized log management server.

ii) Security Information and Event Management – A security information and event management tool is commonly referred to as a SIEM. I have personal experience with and have observed threat actors attempting to delete local logs to remove on-site evidence of their activities, including log deletion, log modification and changing logging settings. By sending logged events to a SIEM tool, an organization can reduce the likelihood of malicious log spoilation and maximize the ability to detect malicious activity. None of the election systems that I have analyzed utilized a SIEM.

iii) Effective log correlation from both network and host security devices is critical to protecting election networks and computing devices. By reviewing logs from multiple sources, an organization can better triage an individual event and determine its impact to the entire organization. Modern log analysis and correlation systems provide the analysis, detection of an anomaly, and alerting within 15 seconds from event to eyes on glass by an analyst. None of the election systems that I have analyzed were capable of log correlation.

iv) Review both centralized and local log management policies to maximize efficiency and retain historical data. CISA recommends that organizations retain critical logs for a minimum of one year, if possible. Federal law[3] requires that all election system- related logs be retained for at least 22 months. In the case of the Maricopa County election system analysis, the Election Management Server (EMS) contained two hundred thirty-seven (237) distinct Windows-specific log files and three hundred fifty-two (352) archived Dominion Democracy Suite logs. The Dominion Democracy Suite logs appear to have been preserved in accordance with the Federal retention statute, but of the two hundred thirty-seven (237) distinct Windows-specific log files only three were produced in response to the subpoena. Among the missing were the critical Windows security.evtx log. It is critical that all

[3] US Code 52 Section 20701 - Retention and Preservation of Records and Papers by Officers of Elections; Deposit with Custodian; Penalty for Violation.

system and application-specific logs be independently retained in accordance with the federal, state, and local statutes. Centralized logging also addresses potential logging and log retention issues discovered during the analysis of the Maricopa County election system. In all examined systems, the Windows operating system event logs were set to the default Windows log size of 20 megabytes. When the maximum file size is reached, for every new logged event that is created, the oldest log entry is deleted. This ensures that the actual log file never exceeds 20 megabytes. The issue arises over time if the logs are not forwarded to a centralized log server, then logged events are lost over time. In the event of the Maricopa County analysis, the oldest logged event in the security.evtx log file was dated 5 February 2021. Thus, the log did not encompass the 2020 General Election time frame.

v) PowerShell and Advanced Logging Should be Enabled

(1) PowerShell is a cross-platform command-line shell and scripting language that has quickly become a central exploitation capability by malicious actors. I have personally observed threat actors, including advanced persistent threat (APT) actors, using PowerShell to exploit systems and hide their malicious activities.

(2) Given the extensive usage of PowerShell to exploit systems by malicious actors, it is imperative that the PowerShell instances have module, script

block, and transcription logging enabled.

f) **Network Segmentation** – In all the election systems that I have examined I identified an attempt to segment the systems that record the votes from the systems that administratively support the voting process, (e.g. poll worker laptops, voter registration data base, etc.). Segmentation was attempted by using an "air gap" to isolate the Dominion Democracy Suite systems. This partially complies with the CISA Best Practices for Securing Election Systems. The issue is the overreliance on the air gap to provide segmentation and security to a network. It is a false assumption that, because there is no connection to the internet by an internal router the network is fully segmented and secure. History has proven that air-gapped systems are easily bypassed by connecting cell phones, wireless "hockey pucks", other wireless networks to an endpoint internal to the air gapped systems. It is important to note that all the computers used within the Dominion Democracy Suite are commercial off-the-shelf (COTS) hardware from Dell computers. A search of a subset of these systems indicates that these systems do contain wireless 802.11 modems that can connect to unauthorized networks if the user has administrative access. As all of the accounts, including the administrative accounts, had the exact same password, any user of the system could have thwarted the air gap security in a matter of seconds. As previously mentioned, in the systems that I have examined there would not have been any mechanism to detect or prevent such a violation of the system security.

g) **Block Suspicious Activity** – In every election system that I have analyzed there has been no mechanism for blocking malicious activity or programs other than the outdated antivirus program. Given the lack of operating system patching, lack of antivirus definition updating, and the lack of password controls, the Analyzed Election Systems, as examined, simply do not have the ability to detect or block suspicious activity.

19) Updating election systems, subsequent system configuration, and subsequent system validation of election systems is an inherent government function of the local voting jurisdiction. Government officials must provide competent and continuous oversight of vendors supporting the updating and certification of those systems to comply with the appropriate jurisdictional requirements and regulations. In order to perform these oversight functions, the government must have full control and the same levels of administrative access as the vendors in order to access detailed information concerning the full scope/impacts of the vendor activities. This level of access and control is required to be able to independently validate that those contractors do not violate the law. I have discovered in the course of my work on the Analyzed Election Systems that the vendors of election software did not allow the counties to control or possess the authentication mechanisms that would permit independent validation of the system's configuration prior to certification. Simply put, there currently is no mechanism for county clerks to independently validate the installation of firmware, system configurations, determine the

status and configuration of wireless devices, or other program installations without relying solely on the vendor-provided data or data provided by a company closely associated with the software vendor as the basis for certification. This was the case in Maricopa County. In order to validate the configuration of the Dominion ICP ballot tabulators, including the ability to determine if a wireless modem was enabled or disabled, a technician password was required. In response to the Senate request for the technician password, the Board of Supervisors replied in paragraph 3 of the Maricopa County Board of Supervisor's Response to Arizona Senate questions dated 5-17-21 and named "2021.05.17 Response Letter to Senate President Fann - FINAL_202105171430291332.pdf" that the county did not possess that password, nor could the county compel production of that password from the Dominion employees. Therefore, it would have been impossible for the County Board of Supervisors to independently validate the ICP configuration for local certification of the voting system or to ensure that the configuration of the systems was changed after the system was certified.

20) Based on my experience if the Cyber Security failures and lapses exhibited by the election systems networks and computers that I have examined were present in an enterprise that was subject to PCI or HIPAA industry certifications, that network would not be certifiable.

SIGNED UNDER THE PAINS AND PENALTIES OF PERJURY THIS 8th DAY OF JUNE 2022.

Benjamin R. Cotton

Exhibit A - Senate Final Presentation
Exhibit B - CyTech Taiwan Germany
Exhibit C - 2021.05.17 Response Letter to Senate President Fann - FINAL_202105171430291332
Exhibit D - 033122 EAC Dominion Anomoly
Exhibit E - Antrim Lawsuit Exhibit 8 Benjamin Cotton Affidavit
Exhibit F - 081920 Halderman Declaration
Exhibit G - 080221 Halderman Decl.
Exhibit H - Special Master Final Report
Exhibit I - EMS Windows Log Files
Exhibit J - Microsoft Patched Vulnerabilities between August 2019 and April 2021