

EXHIBIT 75

**IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION**

**DONNA CURLING, ET AL.,
Plaintiffs,**

v.

**BRAD RAFFENSPERGER, ET AL.,
Defendants.**

**DECLARATION OF
J. ALEX HALDERMAN**

Civil Action No. 1:17-CV-2989-AT

Pursuant to 28 U.S.C. § 1746, I, J. ALEX HALDERMAN, declare under penalty of perjury that the following is true and correct:

1. I hereby incorporate my previous declarations as if fully stated herein. I have personal knowledge of the facts in this declaration and, if called to testify as a witness, I would testify under oath to these facts.

2. This declaration supplements the findings from my expert report dated July 1, 2021 (“July 2021 Report”) in light of the events that occurred in Coffee County, Georgia in January 2021.

3. On January 7, 2021, individuals accessed the Coffee County elections office and imaged the election system software and data, including the software used to operate Georgia’s election management systems (EMSs) and ballot marking

devices (BMDs). This software and data were distributed to a wider group of individuals and technical experts via the Internet¹ and via one or more hard drives that were physically shipped to recipients.² On multiple occasions later in January 2021, individuals again accessed the Coffee County elections office and had repeated physical access to Coffee County's EMS and other voting equipment and data over a multi-week period.

4. The Secretary of State's Office reportedly was unaware of these events for more than a year. It reportedly opened a formal investigation in or around March 2022 because of information that surfaced in this lawsuit. But the Secretary of State's Office also contacted Coffee County election officials in or around May 2021 about a possible compromise of the county's voting equipment after learning that a business card for Cyber Ninjas was found in the elections office. That investigation reportedly failed to uncover the access that occurred in January 2021 and any related conduct, including subsequent distribution and analyses of the software and data taken from the Coffee County elections office. The Georgia Bureau of Investigations reportedly has been investigating that access since August 2022. Very little

¹ SullivanStrickler production 08122022-000126.

² SullivanStrickler production 08122022-000097.

information has been provided about that investigation, and apparently no charges have been brought against anyone involved.

5. To assess how the events involving Coffee County bear on the security of elections in Georgia, I examined a series of forensic images from Coffee County's EMS server and other components of the county's election system, documents and deposition transcripts obtained during discovery, and other materials cited in this declaration. I have not examined any of the extensive voting equipment I understand the Secretary of State's Office took from Coffee County in September 2022, as that equipment has not been made available to me.

6. My principal findings and conclusions are as follows:

- a. The events in Coffee County confirm that outside technical experts could (and did) gain the degree of access to Georgia's election system that would enable discovery and exploitation of vulnerabilities such as those described in my July 2021 Report. The degree of access to election software and equipment that technical experts obtained in Coffee County was far more extensive than the access I had when preparing my July 2021 Report, as it included access to the county's live election system and to additional election system components that I did not have access to, such as the EMS server, ImageCast Central

(ICC) workstation, compact flash drives, thumb drives, and one or more laptops. This degree of access would be more than sufficient to discover and test methods for exploiting any of the vulnerabilities listed in my July 2021 Report, as well as additional vulnerabilities I may not have identified, and to implant malware to affect future elections.

- b. The risk that a future Georgia election will be attacked materially increased with the outside group(s)'s copying and distribution of the proprietary software that operates Georgia's election system and its specific system configurations. Technical experts who analyze this data can discover vulnerabilities and develop means to exploit them, such as malware for the ImageCast X (ICX) BMDs. The heightened risk of future attack applies not only to Coffee County but to all other Georgia counties too, since counties throughout the state use the same Dominion software and the same or similar system configurations. The outside group(s) copied the complete EMS server and ICC workstation, as well as important peripherals such as compact flash drives used with the voting system. They also copied the most critical software component of the ICX BMD. All this data was uploaded to the Internet and distributed to an unknown number of people who may have further

distributed it, including potentially by sharing login credentials for the Internet repository with as-yet-unidentified individuals and organizations. The risk of attack remains elevated despite Georgia eventually replacing some of Coffee County's election equipment, because the Dominion software that was copied and the configuration details used in counties across Georgia have not to my knowledge been changed to this day. I have seen no evidence that even some passwords to internal EMS server accounts exposed in the Coffee County breach and likely shared by other Georgia county EMSs have been changed.

- c. The Dominion EMS configuration used in Coffee County has serious weaknesses that increase the risk that it could be successfully attacked, and it is likely that the same or similar problems affect EMSs in other counties throughout Georgia. In Coffee County, all users of the EMS server shared a single Windows username and password, and this account had administrator privileges that allowed the user to bypass all Windows security controls and manipulate software, election data, and log files. As a result, any user could connect external USB sticks and install arbitrary software, including malware, or otherwise modify the software on the voting equipment. The EMS server's hard drive was

not encrypted, so anyone with physical access to the computer could bypass the password protections entirely and read or modify any of the data or software. The EMS server appears not to have had any operating system security patches applied since 2016, when the version of Windows it uses was produced. It lacks security patches that Microsoft labeled “critical”, including for problems that could likely be exploited to spread malware to the server via USB sticks in Stuxnet-style attacks.

- d. The Secretary of State has not, to my knowledge, inspected any of the Coffee County voting equipment for evidence of malware or other tampering or taken any effective measures to determine whether the Coffee County infiltration compromised the voting system. Also, to my knowledge, the Secretary has also not taken any effective technical steps to address the vulnerabilities discussed in my July 2021 Report and later confirmed and publicly disclosed by CISA, despite the events in Coffee County having added further urgency to mitigating these flaws. The Secretary of State’s apparent lack of response to the events in Coffee County demonstrates that the State, and the counties which rely on the Secretary of State for direction and resources, cannot be relied upon to prevent future infiltrations of elections offices or to

prevent potentially compromised election equipment from affecting voters.

- e. The Secretary of State took more than 18 months to replace all of the Coffee County election equipment accessed by the outside technical experts, and its piecemeal replacement of some of the Coffee County equipment was done in such a way that it leaves open the possibility that malware potentially introduced during the incident could continue to infect the equipment. The Secretary of State reportedly replaced the Coffee County EMS and ICC in June 2021³ and the Coffee County BMDs, printers used by the BMDs, ICPs, flashcards, and thumb drives in September 2022.⁴ During the 15-month period when the new EMS and ICC were used in elections along with the original BMDs, BMD printers, ICPs, flashcards, and thumb drives, the new EMS and ICC could have been infected by any malware on that original equipment. Despite the risk that the new EMS and ICC were infected, the Secretary of State did not replace them in September 2022, leaving the possibility that malware potentially inserted during the incident could continue to

³ Dkt. 1377 at 3-4, Ex. D.


⁴ Dkt. 1492 at 1-2, Ex. A.

infect the Coffee County election system today. And there is no indication that the Secretary of State's Office, or anyone else, examined the EMS server or ICC workstation currently used in Coffee County for malware or other compromise since installing them last year, even after the January 2021 access to Coffee County's voting equipment surfaced in this litigation.

- f. Even if no malware was inserted into Coffee County's election system during the January 2021 incident, the fact that outside individuals who are technical experts now have exact copies of Georgia's election software and system configurations means these outsiders—and others who gain access to that software and data, such as via the Internet repository where they resided for many months—can develop malware that could be inserted into Coffee County's new election equipment or the election equipment of other Georgia counties, either through subterfuge or with brief cooperation from an insider (even a well-intended insider who might genuinely believe that access for third parties is appropriate and lawful). Since the state could not prevent the original, extensive breach in Coffee County, it cannot credibly assure

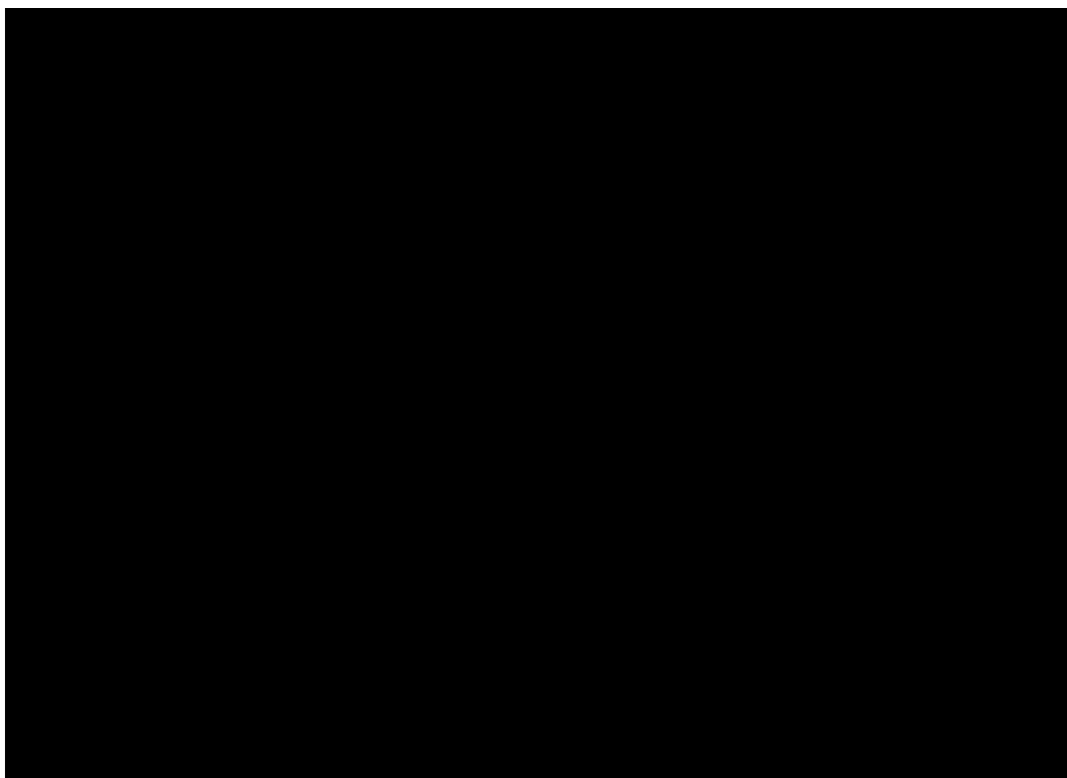
the public that the election system is safe and reliable. Any such claims unfortunately would be speculation.

Data Copied by SullivanStrickler in Coffee County

7. Emails produced by the forensics firm SullivanStrickler establish that a team from the firm visited the Coffee County elections office on January 7, 2021, to “.”⁵

8. Photographs produced by SullivanStrickler show the company’s team carrying out parts of the data collection process. In one photograph (shown below), they are shown creating a forensic image of the Coffee County EMS server. It appears that they have attached two external USB devices to the server—a thumb drive and an external hard drive. They appear to have booted the server from the thumb drive and to be using a Linux-based forensic imaging tool contained on the thumb drive to copy the EMS server hard drive to the external hard drive.

⁵ Email from Paul Maggio to Sidney Powell, “Re: SSA1722: Jim Penrose - Coffee County GA Forensics Engagement Agreement” (Jan. 7, 2021). SullivanStrickler production 08122022-000034 at -035.



*SullivanStrickler employees imaging the Coffee County EMS server.*⁶

9. This data collection process was itself a security risk. If SullivanStrickler's bootable USB stick was infected with malware, it could have infected the Coffee County EMS server during the imaging process.

10. SullivanStrickler Director of Data Risk & Remediation Dean Felicetti testified that, in addition to the EMS server, the firm's team imaged or attempted to image the ICC workstation, ICP scanners, ICP memory cards, Poll Pads, ICX

⁶ SullivanStrickler production 08122022-000236-265 at -240.

BMDs, and other equipment at the elections office.⁷ In the process, the team would have connected USB sticks or specialty forensic devices to each piece of equipment.

11. SullivanStrickler produced a hard drive containing what it says is a complete copy of the data the team collected in Coffee County.⁸ A directory listing of that hard drive is attached as Exhibit A.

12. I examined the data using standard forensics tools and determined its contents. The items copied by SullivanStrickler included the following:

- a. A complete copy of the Coffee County EMS server hard drive, including the Windows installation and configuration, the Dominion Democracy Suite EMS software, and all election data that was present on the server as of January 7, 2021.
- b. A complete copy of the Coffee County ICC workstation hard drive, including the Windows installation and configuration and the Dominion ImageCast Central software.⁹

⁷ SullivanStrickler 30(b)(6) Dep. Tr. at p. 189.

⁸ SullivanStrickler hard drive produced on Aug. 12, 2022.

⁹ SullivanStrickler employees labeled this image “██████████” during collection, but this is a mistake. The image matches the software found on a typical ICC workstation. An ICP scanner uses an entirely different operating system, file layout, and set of software components. This mislabeling was confirmed by Dean Felicetti. SullivanStrickler 30(b)(6) Dep. Tr. at p. 297.

- f. Complete copies of eighteen compact flash memory cards used in Coffee County's ICP scanners during the January 2021 runoff election. Each ICP uses a pair of memory cards to store data files, including the election results.
 - g. Copies of six other USB sticks containing election projects or backups of election projects, and a copy of a USB stick that appears to have been used to install election definition files on Coffee County's ICX BMDs.
 - h. Partial backups from 20 KNOWiNK Poll Pad devices. Metadata associated with the Poll Pad images indicates that they were collected using a Cellebrite Universal Forensic Extraction Device (UFED), which is a device designed to extract data from a wide variety of mobile devices, including Apple iPad hardware like that used by the Poll Pads. These backups appear to be incomplete and do not contain the Poll Pad application software or voter registration data.
13. After collecting the Coffee County data, SullivanStrickler uploaded it to an Internet service named ShareFile. In discovery, SullivanStrickler produced an activity log from the ShareFile service that indicates that five individuals downloaded Coffee County data during January and February 2021: Doug Logan, James Penrose, Todd Sanders (listed as "██████████"), Conan Hayes, and Michal

Pospieszalski.¹⁰ At least some of these individuals shared their ShareFile credentials with others, including Ben Cotton,¹¹ and it is likely impossible to determine how many people now have copies of the data.

14. All of these individuals apparently would have had unfettered access to analyze the Georgia election software and data taken from Coffee County. This access would be sufficient to discover any of the vulnerabilities in the EMS server and ICC workstation that I describe later in this declaration—indeed, I found or confirmed them using the forensic images that SullivanStrickler collected. Using only the forensic images, an attacker could discover vulnerabilities, craft malware to exploit them, and test the malware against copies of the EMS server and ICC workstation running in virtual machines. Malware that worked in such a virtual machine would be highly likely to work identically if used with a real EMS system built with the same software.

15. The ICX application installation files (ICX.apk files) that SullivanStrickler copied contain the most important information that someone would need to develop attacks against the ICX. As I described in my July 2021 Report,

¹⁰ “SSA1722 Useage Report Dec20-Mar21.xlsx”; SullivanStrickler production 08122022-000137.

¹¹ Cotton Dep. Tr. at p. 89.

16.

Felicetti testified that SullivanStrickler attempted to create a complete forensic image of an ICX in Coffee County, but no such image was included in the data that the firm produced in this case. However, James Penrose, one of the outsiders involved in the Coffee County incident, later authored a report in which he credibly claims to have studied a forensic image of an ICX.¹² His report is silent about the provenance of this image.

17. Following the data collection activities by the SullivanStrickler team, on January 7, 2021, two individuals working as part of the same group, Jeffrey Lenberg and Doug Logan, visited the Coffee County elections office several times. Surveillance camera footage from the elections office obtained in discovery shows that Logan and Lenberg both visited the office on January 18 and 19. Lenberg then returned without Logan on January 25, 26, 27, 28, and 29. Logan and Lenberg

¹² James Penrose, “Preliminary Wireless Communications Technology for Michigan Voting Systems” (Apr. 8, 2021). Lenberg production, file 11c.pdf at p. 2.

testified that they worked with Coffee County Election Director Misty Hampton to conduct a series of experiments on the EMS and election equipment.

18. I examined a separate set of forensic images of the Coffee County EMS server and ICC workstation that were collected for Plaintiffs in September 2022. This second set of images shows traces from the experiments that Logan and Lenberg performed. The Windows event logs and EMS user logs from the two systems show that their experiments involved programming compact flash memory cards for the ICP scanner and USB sticks and smartcards for the ICX BMDs. They also involved accessing the System Settings on the EMS server and ICC workstation computers and setting back the internal clocks on both computers to around the time of the November 2020 General Election, scanning at least 6,400 ballots for that election, and uploading results to the EMS.

19. The evidence suggests that Logan and Lenberg may have had access to the EMS, ICX, and other election equipment for seven days. This access began more than 10 days after SullivanStrickler collected the Coffee County data and software, which would have given technical experts ample time to analyze that data and software and discover vulnerabilities. The degree of access that Logan and Lenberg appear to have had would have been more than sufficient to discover any remaining vulnerabilities described in my July 2021 Report, to test malicious software designed

to exploit vulnerabilities in the election equipment, or to infect the EMS or other equipment with malicious software programmed to attack future elections.

20. To further understand the vulnerabilities that the outside technical experts could have discovered or exploited, Curling Plaintiffs asked me to examine the forensic images of the EMS server and ICC workstation hard drives that were collected by SullivanStrickler.

21. Due to time and resource constraints, I focused on finding weaknesses in the Windows installation and its configuration, rather than in the Dominion EMS software.

22. I examined the hard drive images using the Autopsy forensics toolkit, which is a widely used forensics software package. I also examined the behavior of the EMS components by creating virtual machines from the hard drive images. A virtual machine simulates a running computer system and allows an analyst to interactively operate a copy of the computer—logging into Windows, running applications, etc.—without modifying the forensic image or the original computer. I used VMWare Workstation Pro to create virtual machines of the EMS server and the ICC workstation. I also created an isolated virtual network to connect the two virtual machines, just as the EMS server and ICC workstation would be connected by an isolated network in a county EMS deployment. My findings follow.

Security Posture of Georgia Election Management Systems

23. The EMS server and ICC workstation appear to have been set up using a process called “imaging” or “cloning”. In such a process, Windows and the Dominion application software would be installed and configured once, on a single “master” computer, then the contents of that computer’s hard drive would be replicated onto many different computers. This is a common practice in enterprise IT environments, where many desktop or laptop computers use the same software and configuration. The advantage to such a process, in addition to saving time, is that it ensures that all the systems are at least initially in a consistent configuration.

24. One indicator that the Coffee County systems were provisioned through a cloning process is that the Windows installation date on each system appears to predate construction of the computer. The Coffee County EMS “server” is a Dell Precision 3431 desktop computer with service tag [REDACTED].¹³ (A service tag is essentially a serial number used by Dell that is unique to each computer the company sells.) Dell’s website shows that the computer with that service tag was shipped to the customer on December 3, 2019.¹⁴ However, Windows shows that it and the

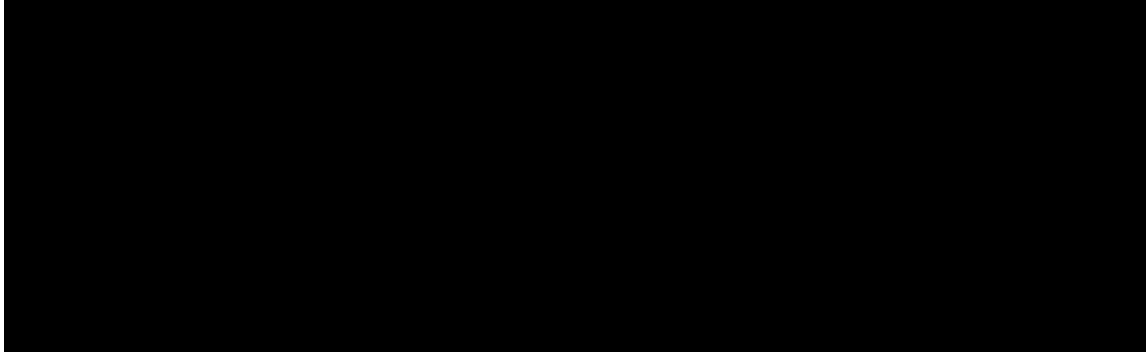
¹³ SullivanStrickler production 08122022-000236-265 at -254.

¹⁴ Dell US, “Support for Precision 3431”. Available at <https://www.dell.com/support/home/en-us/product-support/servicetag/0-UnNYYXRjckNITU1WanA0UXJNdUImdz090/overview>.

Dominion application software were installed on September 12, 2019. Similarly, the Coffee County ICC workstation is a Dell OptiPlex 3050 all-in-one computer with service tag [REDACTED].¹⁵ Dell's website shows that the computer was shipped to the customer on November 27, 2019, but Windows reports that it and the Dominion ICC software were installed on November 25, 2019, and November 26, 2019, respectively. Since the Dominion software would not have been installed by Dell before shipping the computers, the most likely explanation is that the hard drives were cloned from another computer where the software was installed on the earlier date.

25. Further evidence that the systems were set up through a cloning process comes from the ICC workstation. The forensic image of the ICC contains a web browser history file that indicates the system was at least briefly connected to the Internet on November 25, 2019, the same day Windows was installed. Entries in the history file indicate that someone logged in under the "[REDACTED]" user account visited the Dell website, entered the service tag of the running system, and downloaded device driver software for the computer's specific hardware to complete the Windows setup process.



¹⁵ SullivanStrickler production 08122022-000236-265 at -250.



Excerpt from ICC web browser history showing visit to Dell website.

26. It is a security risk to connect an old and unpatched version of Windows to the Internet. (As I explain below, the version of Windows running on the ICC dates from 2015 and even now lacks numerous critical software updates.) Attackers continuously scan the Internet for unpatched systems, and in some cases can exploit vulnerabilities soon after a system is connected to the Internet for the first time. Taking this risk was unnecessary, since the drivers could have been downloaded on a separate, up-to-date system and then copied to the ICC on removable media.

27. Normally, to find the appropriate drivers for a system, the operator enters the service tag for that machine into the Dell website. Visiting the Dell support URL in the browser history shows that the device driver software request was instead for a machine of the same model but with a different service tag than the Coffee County ICC: [REDACTED].

	OptiPlex 3050 All-In-One	Service Tag	Express Service Code	Ship Date	Location
		[REDACTED]	[REDACTED]	11 NOV 2019	United States
	OptiPlex 3050 All-In-One	Service Tag	Express Service Code	Ship Date	Location
		[REDACTED]	[REDACTED]	27 NOV 2019	United States

Screenshots from Dell website showing ship dates for the two service tags.

28. The most likely explanation is that the Windows installation on the Coffee County ICC workstation was set up on another computer, with the [REDACTED] service tag, and then later cloned to the Coffee County ICC. It is likely that counties across Georgia use EMS servers and ICC workstations that were configured using the same process, by cloning pre-made system images to their hard drives. If so, this means that vulnerabilities found in the Coffee County systems are likely to also affect EMS servers and ICC workstations in other Georgia counties that were created from the same master images.

29. For example, both the EMS server and the ICC workstation lack critical Windows security updates. The EMS server runs Windows 10 Pro version 1607 (build 14393.0), which was released in August 2016. The instance of Windows running on the EMS server was installed on September 12, 2019. Microsoft has released approximately 380 software patches or updates that apply to this Windows

version, approximately 165 of which the company has rated as “critical”.¹⁶ On the EMS server, Windows reports that *zero* operating system security patches are installed.

30. The ICC workstation runs an even older version of Windows, Windows 10 Pro version 1507 (build 10240). This was the first version of Windows 10 and was released in July 2015. Microsoft has released approximately 184 software patches or updates that apply to this version of Windows, approximately 101 of which the company has rated as “critical.”¹⁷ On the ICC workstation, Windows reports that only 4 patches have been installed, the most recent of which was released in 2016 and installed on November 25, 2019—the same day that the instance of Windows running on the ICC system was installed.

31. Keeping the operating system and other security-critical software updated is universally recognized as a security best practice. Updates that are rated “critical” frequently fix vulnerabilities that are readily exploitable—or that are actively being exploited by attackers in the wild—and so it is important to install

¹⁶ ManageEngine Patch Repository, “Windows 10 Version 1607 Patches”. Available at <https://www.manageengine.com/products/desktop-central/patch-management/Windows-10-Version-1607-updates.html>.

¹⁷ ManageEngine Patch Repository, “Windows 10 Version 1507 Patches”. Available at <https://www.manageengine.com/products/desktop-central/patch-management/Windows-10-Version-1507-updates.html>.

these patches promptly. When critical security patches are missing, attackers may be able to exploit security problems by running publicly available attack tools.

32. One example of a vulnerability that is unpatched on the EMS server and ICC workstation is [REDACTED], which has a severity score of 9, or “critical”.¹⁸ This vulnerability allows an attacker to create malware that, if placed on a USB stick that is later inserted into a vulnerable computer, will infect the vulnerable computer without any interaction with or indication to the user. Although the [REDACTED] vulnerability was discovered in 2017, before the EMS server and ICC workstation were purchased, the outdated, unpatched Windows installations on these computers continued to be vulnerable to it in January 2021.

33. That the Windows software patches are so out-of-date makes attacking the EMS server and ICC workstation within reach for relatively unsophisticated attackers, in addition to better-resourced attackers such as nation states. Whereas sophisticated attackers can discover entirely new vulnerabilities and develop the means to exploit them, less sophisticated attackers frequently rely on attack toolkits

¹⁸ Rapid7 Vulnerability and Exploit Database, “Microsoft [REDACTED]: LNK Remote Code Execution Vulnerability”. Available at [https://www.rapid7.com/db/vulnerabilities/msft-cve-2017-\[REDACTED\]](https://www.rapid7.com/db/vulnerabilities/msft-cve-2017-[REDACTED])

such as the Metasploit framework,¹⁹ which make exploitation of known vulnerabilities a relatively simple, step-by-step process.

34. An additional risk of using older, unpatched versions of the Windows operating system is that more recent versions of Windows have added important defensive features that strengthen the overall system's security. Since the EMS server and ICC workstation run versions of Windows that are six and seven years out of date, they do not benefit from these protections.

35. Other software present on the EMS server and ICC workstation also appears to lack important software updates and patches, including the Microsoft SQL Server database system.

36. Both the EMS server and the ICC workstation have the Windows Defender antivirus software installed. Windows Defender is part of Microsoft Windows and is typically installed automatically as part of the operating system. Like other antivirus products, Windows Defender must receive regular updates to its malware definition database to be able to reliably identify recently created malware. In a typical computing environment, these updates are delivered automatically over the Internet every few days. However, on systems that are not connected to the

¹⁹ Rapid7, "Metasploit: Penetration Testing Software". Available at <https://www.metasploit.com>.

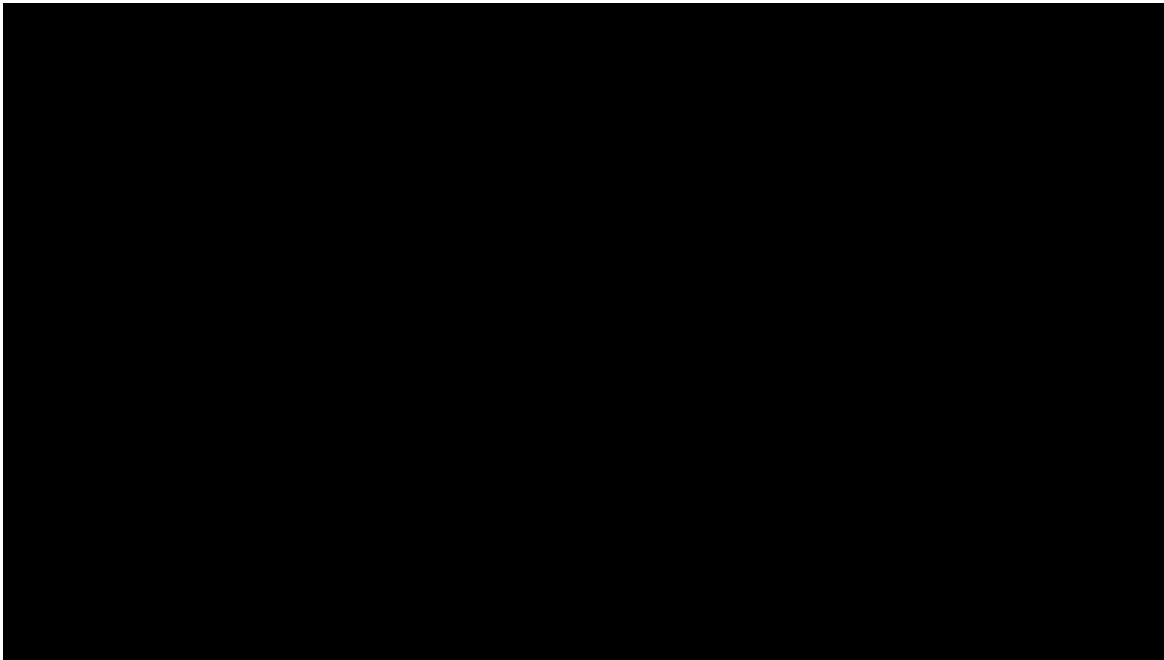
Internet, such as the EMS server and ICC workstation, Windows Defender updates need to be installed manually from removable media.

37. On the EMS server, Windows Defender shows that the malware definition database was last updated on the day that Windows was installed, September 12, 2019. On the ICC workstation, Windows Defender shows that the malware definition database was last updated in July 2015, when the version of Windows running on the workstation was released.

38. Antivirus products such as Windows Defender offer only limited protection against malware that is specifically created to target a particular system. However, the use of such outdated malware definitions renders the antivirus software on the EMS server and ICC workstation *even less* effective and exposes the election system to an elevated risk of compromise through run-of-the-mill untargeted malware.

39. In the EMS server's "Recycle Bin" folder are two files named "[REDACTED]", both with metadata indicating that they were created on December 23, 2019. The files have similar content, and they appear to be the output of a hash verification tool used during acceptance testing of EMS systems in Georgia. This tool would likely have been run on the EMS server after it was

received by Coffee County to check the integrity of the software. The content of one of these files is shown below.



Content of “[REDACTED]” found in the EMS server’s Recycle Bin.

40. This output indicates that the hash verification tool only verified the hash values of four files. This is inadequate to confirm the integrity of the EMS server. The Dominion software applications on the EMS server consist of approximately 700 files. The EMS server as a whole contains approximately 240,000 files, of which more than 27,000 are .exe or .dll files, two kinds of files that contain executable code. This means that the server contains numerous files that could be modified to introduce malicious functionality but that were apparently not inspected in the hash verification process.

41. The version of Windows installed on the EMS server and ICC workstation supports full-disk encryption through a feature that Microsoft calls BitLocker. Full-disk encryption is essential to protect computers against attackers with physical access. For this reason, it is enabled by default on most modern smartphones and many corporate laptops. However, I could find no evidence that BitLocker or any other full-disk encryption method was used on the hard drives in the EMS server or ICC workstation. Felicetti testified at his deposition that the EMS server and ICC workstation hard drives were not encrypted when SullivanStrickler imaged them.²⁰ He also testified that no passwords were necessary for the imaging process SullivanStrickler followed, which implies that neither system required a password to change its BIOS settings. The BIOS settings determine, among other things, whether the computer will start up by running software from its internal hard drive or from an external USB device, which could potentially contain malicious code. In these respects, the Coffee County EMS computers were less well secured against attackers with physical access than a typical modern smartphone or enterprise laptop.

²⁰ SullivanStrickler 30(b)(6) Dep. Tr. at p. 172-174.

42. Since the hard drives were not encrypted and there apparently were no BIOS passwords, an attacker with physical access to the EMS server or ICC workstation could entirely bypass the Windows account passwords and other software security mechanisms by changing the BIOS settings to boot from an external USB device. SullivanStrickler used this method to make a complete forensic image of the EMS server without making use of any passwords.²¹ This demonstrates that an attacker with physical access could read any of the data on the EMS server or ICC workstation. The same method could also be used to *change* any data on these computers, including modifying the software to insert malware.

43. Moreover, on Windows systems that do not use full-disk encryption, anyone with physical access can use simple, widely documented techniques to bypass or change the Windows login password. State Defendants' forensics specialist Jim Persinger used a similar technique in July 2022 to change the Windows login password on the Coffee County EMS server.²²

44. To confirm that the Windows login password for the EMS server could be easily reset, I carried out a password reset procedure on a copy of the server

²¹ SullivanStrickler 30(b)(6) Dep. Tr. at p. 148-153.

²² Declaration of James Persinger (Nov. 10, 2022) at ¶¶ 23, 26.

running in a virtual machine by following instructions that are easily found online.²³

Without making use of the original password, I changed the Windows password to a new password I selected, after which I was able to log in to Windows using the new password. The process took less than an hour and did not require the use of any third-party software or any security expertise. Using such methods, anyone with physical access to the EMS server could change or bypass the Windows password.

45. The authentication and access control mechanisms on the EMS server and ICC workstation have serious weaknesses beyond the ability to bypass or reset the Windows passwords. On the EMS server, all users shared a single Windows account with the username “██████████”. This is the only account that is available to log into after booting the server. Similarly, on the ICC workstation, all users shared a single Windows user account with the username “██████████”.²⁴

46. Sharing a single account among multiple people is widely considered to be a poor security practice, for several reasons. First, it makes it difficult to later attribute actions or misbehavior to a specific responsible party. This complicates

²³ Sergey Tkachenko, “Reset Windows 10 password without using third party tools”, WINAERO (June 8, 2016). Available at <https://winaero.com/reset-windows-10-password-without-using-third-party-tools/>.

²⁴ The ICC also contains accounts named “██████████”, “██████████”, “██████████” and “██████████” which may indicate that there was once an intention to provide different accounts for different users. However, Windows indicates that those accounts have never been logged into.

post-incident forensics and hinders accountability. In addition, it means the password for the shared account must be provided to everyone who uses the computer. If a person leaves their job position (or otherwise needs to have their access revoked), the password must be changed and the new password provided to all the remaining authorized users (it is unclear whether this important practice is followed in Georgia with respect to voting equipment). In practice, this often means the password will be written down somewhere, which increases the risk that it may be discovered by unauthorized people (as apparently occurred with Coffee County when passwords written on Post-it notes were inadvertently released publicly in a video recorded inside the county's EMS server room that was later published on YouTube in late 2020, which I address below).

47. Using a shared account makes it impossible to follow the “principle of least privilege” with respect to EMS users. The principle of least privilege is a security best practice that holds that users’ access rights should be limited to only what is required to do their jobs. For example, in Georgia, a county election worker might need access to run the Dominion EMS software but typically would not need access to *alter* the Dominion EMS software, so that level of access could be reserved for a separate login account used by Dominion technicians. Tailoring account privileges to job functions in this way would reduce the potential for deliberate

misbehavior or accidental introduction of malware. However, since the EMS server and ICC workstation each effectively had only one user account, that account had to have complete access to the system.

48. Indeed, the “██████████” and “██████████” accounts both are “administrator” accounts. On Windows systems, an “administrator” account effectively has complete access to a computer, including the ability to install or modify software, change or bypass security controls (such as disabling the Windows Defender antivirus software), and modify arbitrary files, such as election databases and security logs. As administrative users, these accounts can also change both their own Windows passwords and the Windows passwords of other user accounts.

49. Conducting routine election tasks from accounts with administrator privileges raises serious (and wholly unnecessary) security risks. For instance, if an election worker unknowingly inserted a USB stick containing malware, that malware would run on the EMS server with the same access privileges as the logged-in user. Since the “██████████” account has administrator privileges, the malware would effectively have complete control over the EMS server.

50. The EMS server and ICC workstation do not appear to be configured to restrict what USB devices can be attached. One might expect that the systems would be locked down to allow the use of only “trusted” USB sticks, such as those from a

particular manufacturer or ones with write-blocking capabilities, but this is not the case. The systems also do not appear to have any kind of software “allowlisting” configured that would limit the software that can run to a set of authorized applications. I confirmed that anyone logged into the “██████████” and “██████████” accounts could run arbitrary software from an external USB device. To test this, I attached USB sticks from various manufacturers to virtual machines running copies of the EMS server and ICC workstation. I was able to read and write to the USB sticks normally. I was also able to run programs that I wrote on both systems after copying the programs from USB sticks.

51. EMS users would not have to install any external software to manipulate election data on the EMS server. An application called Microsoft SQL Server Management Studio application is installed on the EMS server and accessible to anyone logged in with the “██████████” account. I found that I could use it to view and edit any of the election databases on the server with no additional passwords.

52. By editing the databases through SQL Server Management Studio, any EMS server user could bypass security mechanisms present in the Dominion EMS applications. For example, within the EMS application software, each election project is individually password-protected. However, I was able to circumvent these passwords by creating a new project with a known password, extracting the

password hash from the project's database, and copying it into the databases for the other projects. In addition, an EMS server user could use SQL Server Management Studio to manipulate election projects or election result data without being subject to any of the technical controls imposed by the Dominion EMS application software. SQL Server Management Studio would also allow such a user to delete or modify log entries from the EMS applications.

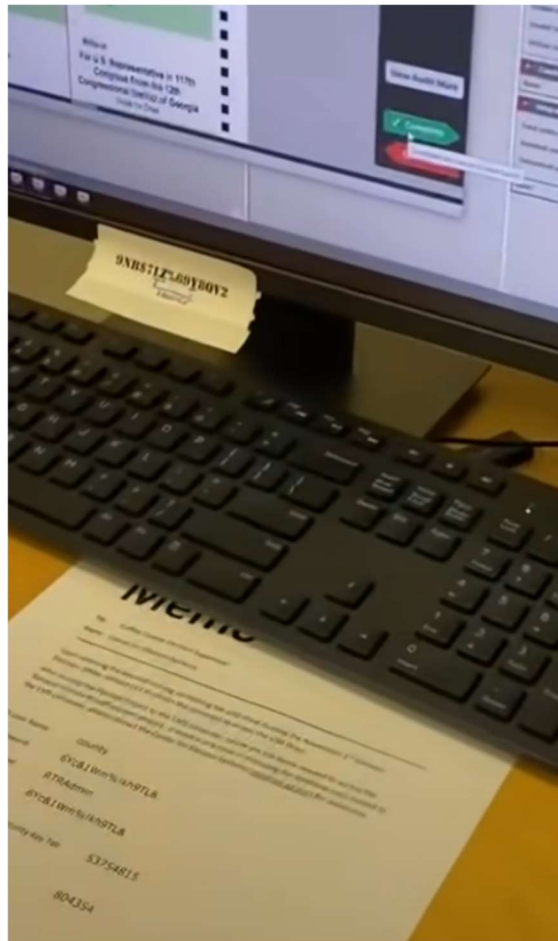
Passwords Exposed through Events in Coffee County

53. In a pair of cellphone videos recorded on November 12, 2020, and first posted publicly on or before December 9, 2020, then Coffee County election director Misty Hampton demonstrated the electronic ballot adjudication process and expressed concerns about its security.²⁵ The videos show Hampton operating the Coffee County EMS server and ICC workstation. What appears to be a sticker or a Post-it note attached to the bottom of the EMS monitor shows the password “9NB\$7lz%69y8QV2”, which is clearly readable in the public videos.

54. Below the keyboard is a memo addressed to the Coffee Election Supervisor from the Center for Election Systems. The memo contains the credentials

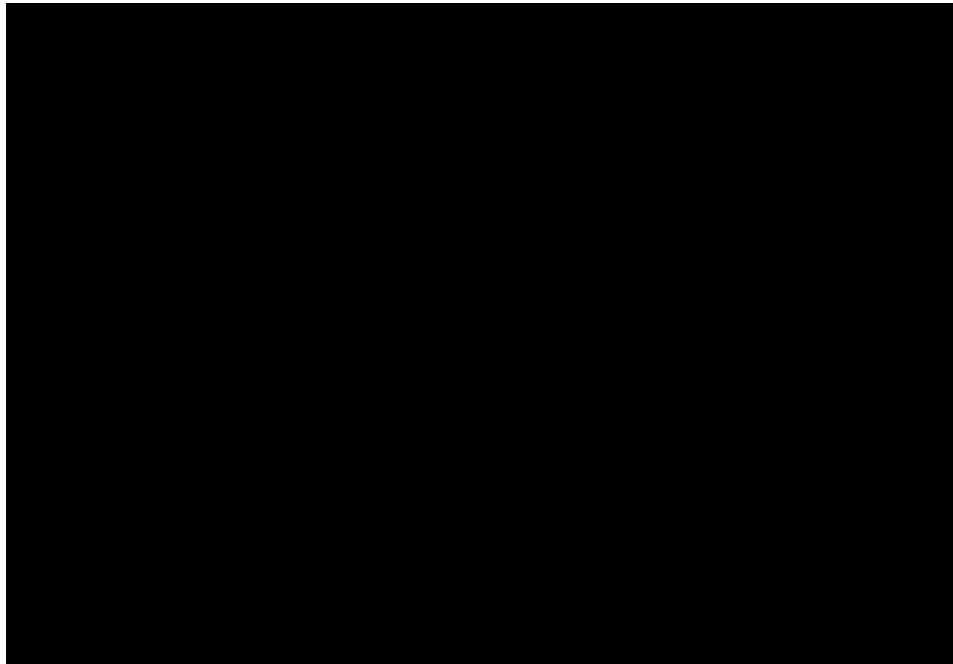
²⁵ DouglasNow, “Dominion Voting Machine Flaws—2020 Election Coffee County, Georgia Video 1,” YouTube (Dec. 9, 2020). Available at <https://www.youtube.com/watch?v=46CAKyyObls>; DouglasNow, “... Video 2” YouTube (Dec. 9, 2020). Available at <https://www.youtube.com/watch?v=ijjwS6h-PyU>.

for accessing the election project for the 2020 general election, including the username (“county”) and password (“6Yc&1Wm%!kh9TL&”) for the EMS Election Event Designer (EED) application; the username (“RTRAdmin”) and password (“6Yc&1Wm%!kh9TL&”) for the EMS Results Tally and Reporting (RTR) application; the PIN (“53754815”) and supervisor code (“804354”) used for the county’s ballot scanners; and the menu code for the Poll Pads (“mcge2020”). All are clearly visible in portions of the public videos.



Cropped still from YouTube video showing Coffee County passwords.

55. At the time the video was posted, the password on the Post-it attached to the EMS monitor may have been the then-current Windows login password for the EMS server's "[REDACTED]" user account, which had full administrative access to the computer. That account has a *different* password in the forensic image of the EMS server that SullivanStrickler created on January 7, but Windows records that the password was changed on December 14, 2020, a few days after the Secretary of State's office criticized Hampton for revealing her password in the video.²⁶ The password was changed to "[REDACTED]".



Windows output showing when the "emsadmin" password was changed.

²⁶ Ross Williams, "Georgia Election Officials Launch Inquiry into Coffee County Recount," Georgia Public Broadcasting (Dec. 11, 2020). Available at <https://www.gpb.org/news/2020/12/11/georgia-election-officials-launch-inquiry-coffee-county-recount>.

56. Although the Windows login password for the EMS server was changed after the video was posted, the same password from the Post-it note was then and *is still* the primary Windows login password for the ICC workstation. That password works to log in to the ICC workstation image created by Plaintiffs' forensic specialist in September 2022. In other words, it is likely that the same password was used for the primary Windows user accounts on both computers, and that, despite changing the password on the EMS server after it was revealed in the video, nobody ever changed the same password on the ICC workstation.

57. Likewise, the EMS server image collected for Plaintiffs in September 2022 shows that the EED and RTR credentials that were revealed in the video were also never changed. They continue to provide access to open the election project for the 2020 general election using the Dominion applications on the EMS server.

58. SullivanStrickler produced a photograph that its employees took while imaging the Coffee County EMS server. It shows another Post-it note taped to the top of the EMS server. That Post-it note has what appears to be a password written on it: "██████████".



Cropped photograph of the EMS server taken by SullivanStrickler team.²⁷

59. It is possible that this was the initial Windows login password for the EMS server when it was delivered to Coffee County. An initial password would be set in the master image that was used to clone the EMS server for each county. In any event, the “ [REDACTED] Windows password for Coffee County’s EMS server was subsequently changed, likely multiple times. However, the EMS server also contains a variety of other Windows accounts that are not intended for normal users but are instead used internally by various components of the EMS software.

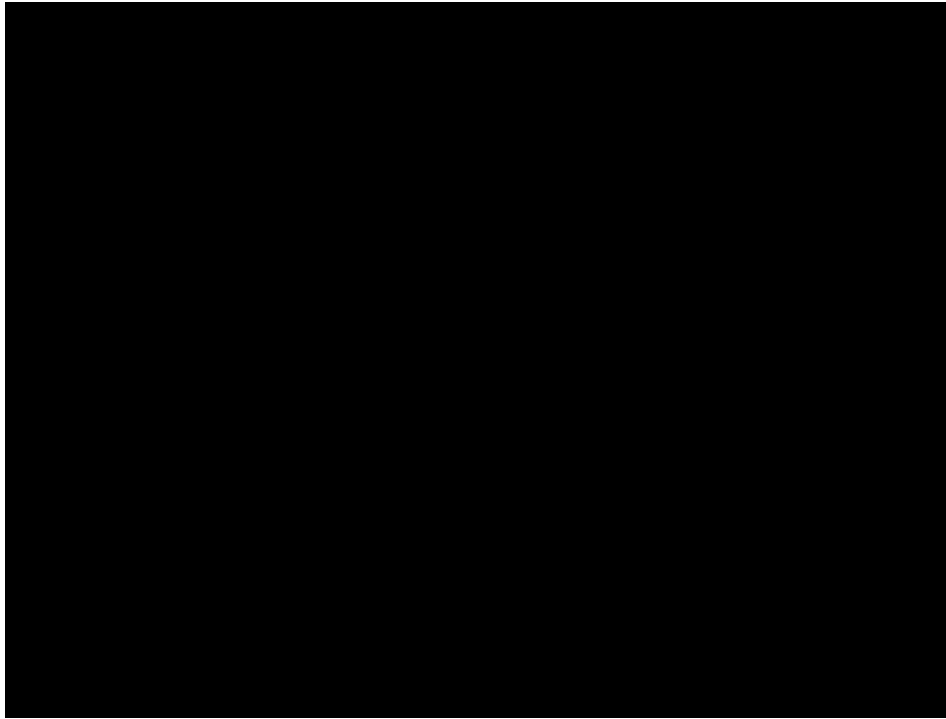
60. One of these accounts is named “ [REDACTED] which is likely a shortened form of “Adjudication System”. Windows reports that the “ [REDACTED] account

²⁷ SullivanStrickler production 08122022-000236-265 at -254.

password was set on September 12, 2019—the date that Windows was installed. This implies that the password for this account is part of the master image, and so it would be the same on all other county EMS systems created from that image. The password is “[REDACTED]”, the same as is written on the Post-it note. Three other internal accounts (“[REDACTED]”, “[REDACTED]” and “[REDACTED]” also had this same password set on that same date and never later changed.

61. Another internal account on the EMS server is named “[REDACTED]”. This account uses a different password, “[REDACTED]”, but that password was also set on September 12, 2019, indicating that it too was likely set in the EMS server master image and not later changed, which suggests that other Georgia county EMSs likely share this password too.

62. The Coffee County incident exposed both of these passwords to anyone with access to the SullivanStrickler data. Among the files that Doug Logan produced in discovery is a file named “[REDACTED]”, which shows that he or others working with him were able to recover both of these passwords.



Contents of “██████████” file produced by Doug Logan.²⁸

63. It is likely that the “██████████” and “██████████” passwords were the same in county EMS servers across Georgia at the time of the Coffee County incident, and I am not aware of any evidence that the Secretary of State’s Office changed these passwords in response to the Coffee County breach. It is likely that the same passwords are still used today for these accounts in counties across Georgia.

64. If so, the exposure of these passwords in Coffee County puts other Georgia counties at risk. The “██████████” password, for instance, can be used to access the EMS server’s network-attached storage (“██████████” folder over the local network.

²⁸ Doug Logan hard drive produced on Nov. 9, 2022.

the EMS server, ICX application software, and software and configuration for other components of Georgia's election system, reverse engineer them to find exploitable vulnerabilities, and develop malicious software to exploit those vulnerabilities.

67. Section 9 of my July 2021 Report explains

68. Such an attack could be developed using, for example, the EMS server image that SullivanStrickler copied and distributed. Technical experts can use the data in the image to discover any of the vulnerabilities in the EMS that I describe above. By running a copy of the EMS server in a virtual machine, as I did, technical experts can develop and test malware that exploits those vulnerabilities in an automated way.

69. Such malware could be injected into a Georgia county EMS intentionally by a malicious insider—or inadvertently by an unknowing and well-intended insider—with physical access to the EMS. As I discuss above, anyone with

physical access would have numerous ways to install malicious software, including by simply running it from a USB stick. Alternatively, malicious software could be installed on a Georgia county EMS without the knowing participation of an insider, by spreading the malware via infected USB sticks and taking advantage of the unpatched Windows vulnerabilities on the EMS server.

I declare under penalty of the perjury laws of the State of Georgia and the United States that the foregoing is true and correct and that this declaration was executed this 22nd day of November, 2022 at Ann Arbor, Michigan.



J. ALEX HALDERMAN

EXHIBIT A

