



Mesa County
Colorado
Voting System

Report #2

Forensic Examination and Analysis Report



February 28, 2022

Table of Contents

Executive Summary	1
Critical Discoveries	1
Most Significant Findings: The Voting System is Not Secure, Violates Security Standards Required By State and Federal Law	2
“Back-Door” found in Voting System; Uncertified Software Invalidates Voting System Certification ...	2
Capability to Easily “Flip” Election Results Demonstrated	3
Voting System Components Manufactured and Assembled in China and Mexico.....	3
Voting System Presents an Immediate threat and is Dangerous to use in the upcoming 2022 election	3
Key Findings	5
Analysis Summary: Compliance of Mesa County, Colorado, DVS D-Suite systems with the law	7
Examination Methodology	15
FORENSIC ANALYSIS.....	19
System identification	19
Authenticity	21
Chain of Custody.....	21
Tools Used.....	22
TEST PREPARATION	22
Finding 1:	25
EXAMINATION OBJECTIVE 1:	34
Finding 2:	51
Finding 3:	52
Finding 4:	52
EXAMINATION RESULT 1	52
EXAMINATION OBJECTIVE 2:	53
Finding 5:	68
Finding 6:	75
EXAMINATION RESULT 2:	75
EXAMINATION OBJECTIVE 3:	76
EXAMINATION RESULT 3:	89
Conclusion.....	92
Appendix A. Compliance Requirements	96
Federal Election Commission 2002 Voting Systems Standards (VSS)	96
APPLICABILITY	96
VSS V1, 1.6, page 1-13:	96
VSS V1, 2.1, page 2-19:	97
VSS V1, 2.2, page 2-20:	97

DATA RETENTION.....	98
Election Record Definition, Scope and Content	98
VSS V1, 4.4.3, page 4-84:.....	98
Security Requirements for Voting Systems	100
VSS V1, 6.1, page 6-93:	100
VSS V1, 6.2, page 6-96:	101
VSS V1, 6.2.2, page 6-97:	101
Appendix B. Database Fundamentals.....	104
Appendix C. IP ADDRESSING FUNDAMENTALS	107
Appendix D. Nation-State Cyber Attack Capabilities.....	109
Introduction.....	109
Moonlight Maze.....	110
Stuxnet.....	110
Operation Titan-Rain	111
Operation Aurora.....	111
2020 US Government Attack.....	112
Summary.....	112
Appendix E. Security Considerations for SQL Server Installations.....	113
Appendix F. C.R.S. 1-5-608.5.....	115
Appendix G. C.R.S. 1-5-615.....	117
Appendix H. Man in the middle attack.....	119
Appendix J. Forensic Imaging Technology.....	121
Appendix K. Accessing a Computer Without a Password.....	126
Finding a password	126
Cracking a password	126
Rainbow Tables.....	126
Bypassing a password.....	127
Exploitation of Services.....	127
Intel Active Management Technology (AMT) and Management Engine (ME)	128
Dell Integrated Remote Access Controller (iDRAC).....	128
Strengthening Access Security.....	129
APPENDIX L. Supply Chain Security Threat and Foreign Manufacturing.....	131
Appendix M. Colorado Secretary of State Press Release	133
Doug Gould Biography.....	137

Table of Figures

Figure 1 - SSMS Installation Date on Mesa County EMS server	12
Figure 2 - Mesa County, Colorado EMS server (5.11-CO) Forensic Image Attributes.....	20
Figure 3 - Test Workstation and Dominion EMS server	23
Figure 4 - Installed Microsoft Software	25
Figure 5 - SQL Server 2016 Configuration Manager	26
Figure 6 - SQL Server 2016 Configuration Manager – Network Protocols enabled.....	27
Figure 7 - TCP/IP Properties.....	30
Figure 8 - TCP/IP Properties of SQL Server, attached to port 1433 the standard (default) port.	31
Figure 9 - SQL Server Properties	32
Figure 10 - Encryption is enabled but No Encryption Certificate is configured	33
Figure 11 - SQL Server Management Studio (SSMS) software showing in the EMS server Start Menu	34
Figure 12 - SSMS is installed and starting on the EMS server system.....	35
Figure 13 - Logging in to the SQL Server using SQL Server Management Studio.....	36
Figure 14 - SSMS enables direct access to the internal databases to anyone logged in to the EMS server.	37
Figure 15 - Databases from many prior elections are fully accessible	38
Figure 16 - Additional databases used in previous elections	39
Figure 17 - Internal database tables, including ones with counted votes are accessible	40
Figure 18 - Menu Option to Select the Top 1000 rows	41
Figure 19 - Accessing the Ballot Choice database table	42
Figure 20 - Test to determine if the Ballot Choice Table can be edited to easily flip the votes	43
Figure 21 - Candidate settings for Trump.....	44
Figure 22 - Candidate settings for Biden	45
Figure 23 - Pulling up the results report prior to attempting the alteration	46
Figure 24 - Run Stored Procedure to pull up a report of Presidential Electors.....	47
Figure 25 - Retrieved Vote Totals	48
Figure 26 - Candidate number for Trump modified	49
Figure 27 - Candidate number for Biden modified.....	50
Figure 28 - Vote totals retrieved again after modification.....	51
Figure 29 - Accessing port 1433 with Telnet	53
Figure 30 - The EMS server network interface appears to answer a connection to port 1433.....	54
Figure 31 - EMS server has the 'Windows Firewall' enabled	55
Figure 32 - Windows Firewall Custom SQL entry is enabled	57
Figure 33 - SQL port 1433 is allowed.....	58
Figure 34 - Access to the SQL database standard port is allowed from ANY IP ADDRESS worldwide.....	59
Figure 35 - No additional IP address restrictions or permissions.....	60

Figure 36 - Test Workstation, 192.168.100.150, and EMS, 192.168.100.10, are on the same subnet	61
Figure 37 - Mesa EMS server is responding to network ping test.....	62
Figure 38 - Telnet connectivity test from separate computer not part of the Dominion system	63
Figure 39 - Telnet to EMS server port 1433 (SQL) succeeds	64
Figure 40 - SSMS access test from separate computer not part of the DVS D-Suite system.....	65
Figure 41 - Log In to the server.....	66
Figure 42 - From a separate Windows 10 computer EMS server database access has been obtained.....	67
Figure 43 - From a separate Windows computer, the databases can be accessed and reports run.....	68
Figure 44 - SSMS permits database Edit.....	69
Figure 45 - EMS server Database view from a separate computer not part of the DVS D-Suite system	70
Figure 46 - SSMS permits us to edit the databases	71
Figure 47 - “internalMachineld” for Trump is now changed back to a 2.	72
Figure 48 - Candidate data for Biden from previous change	73
Figure 49 - Candidate data for Biden changed back to original	74
Figure 50 - The vote choice was remotely changed back to its original state	75
Figure 51 - Network scanner installed on cellphone.....	76
Figure 52 - IP address for the EMS server found via wireless connection and iPhone app.....	77
Figure 53 - Scanner Results.....	78
Figure 54 - SQL Access Functionality	79
Figure 55 - SQL Pro Capabilities.....	80
Figure 56 - Making an SQL Connection.....	81
Figure 57 - iPhone Connection to Dominion EMS Database.....	82
Figure 58 - Databases listing, Continued	83
Figure 59 - Database Table Listing.....	84
Figure 60 - Database Access	85
Figure 61 - Executing a Database Query.....	86
Figure 62 - Table Data.....	87
Figure 63 - A script to change the vote data	88
Figure 64 - Script Results	89
Figure 65 - Small Wireless Device Surreptitiously Installed (internally) on a Computer Motherboard	90
Figure 66 - DVS Compliance Statement.....	102
Figure 67 - Man In The Middle Attack	119
Figure 68 - Illustrative Hard Disk Components.....	121
Figure 69 - Disk Track and Sector illustration	122

EXECUTIVE SUMMARY

This report documents findings in an ongoing forensic examination of images of the hard drives¹ of the Dominion Voting System (DVS) Democracy Suite (D-Suite) version 5.11-CO Election Management System (EMS) server of Mesa County, Colorado. The DVS D-Suite EMS server in that configuration was used for all elections held in 2020 and through May 2021, including the November, 2020 General Election, and the April, 2021 Grand Junction Municipal Election. This voting system represents a portion of the overall election system infrastructure in Mesa County and the State of Colorado. This report is limited to a subset of the findings of an ongoing investigation. Report #1 is incorporated by reference.² The findings in this report were prepared by me as a consultant to the legal team representing Tina Peters, the Mesa County Clerk and Recorder, pursuant to her statutory duties as Mesa County's Chief Election Official.

Critical Discoveries

This report details the following critical discoveries regarding Mesa County's voting system:

- **Uncertified software installed, rendering the voting system unlawful for use in elections.**
- **Does not meet statutorily mandated Voting System Standards (VSS) and could not have been lawfully certified for purchase or use.**
- **Suffered systematic deletion of election records (audit log files required by Federal and State law to be generated and maintained), which, in combination with other issues revealed in this report, creates an unauditible "back door" into the election system.**
- **Violates Voting Systems Standards ("VSS") which expressly mandate prevention of the ability to "change calculated vote totals." This report documents this non-compliance from the logged-in EMS server, from a non-DVS computer with network access, and from a cell phone (which may be possible if any of the 36 internal wireless devices in voting system components are deliberately or accidentally enabled and a password is obtained).**
- **Mandatory VSS "System Auditability" required features are disabled.**
- **Is configured with 36 wireless devices, which represent an extreme and unnecessary vulnerability, and which may be exploited to obtain unauthorized access from external devices, networks, and the Internet.**
- **Is configured through firewall settings to allow any computer in the world to connect to the Election Management System (EMS) server.**
- **Uses only a Windows password with generic userIDs to restrict and control access.**
- **Contains user accounts with administrative access that share passwords, subverting VSS-required user accountability and action traceability controls.**
- **Uses a self-signed encryption certificate which exposes the system to the risk of undetected compromise or alteration.**

¹ A forensic image of a hard drive is a bit-for-bit copy of the user accessible data storage area residing on the data storage mechanism used by the computer system; it is every byte of data accessible to the computer or user. For a complete discussion of this definition, see Appendix J.

² Report No.1 was issued on September 15, 2021 and can be downloaded at <https://standwithtina.org/>.

Most Significant Findings: The Voting System is Not Secure, Violates Security Standards Required By State and Federal Law

The most significant findings include the conclusive determination, based on testing, that the voting system is not secure and protections have not been implemented in accordance with the requirements of the Federal Election Commission's 2002 Voting System Standards (VSS) (see Appendix A). Those Standards constitute a mandatory minimum requirement for a voting system to be certified and used under Colorado law. Given the fundamental flaws in the security design and configuration of this system, there is no conceivable interpretation under which this voting system could be considered secure.³ The fact that it was tested and certified for use vitiates claims of competency and trustworthiness of the entire regime of testing and certification being used, of truthfulness of testing and certification statements, of competency of the Colorado Secretary of State's office, and of the validity of any election results obtained from the voting system as used in any jurisdiction.

"Back-Door" found in Voting System; Uncertified Software Invalidates Voting System Certification

The combination of unauthorized software installed in the EMS server in 2017 (still present in violation of law in 2021), the failure to employ security mechanisms already built into the system and required by VSS, and the obliteration of mandatory audit logs (destruction of both election records and evidence of access to the EMS server) that Federal and State law require be preserved, create a "back-door" to the EMS server that is only partially protected by a simple password, with no preserved audit records. The existence of uncertified software violates the certification of the voting system and makes the use of the voting system in an election illegal. Indeed, University of Michigan Professor J. Alex Halderman,⁴ a recognized computer science expert on electronic voting systems, testified under oath⁵ that components of this Dominion Voting System ("DVS") are highly vulnerable to attack and that the system he examined is used in 16 other states, including Colorado. In his declaration he states under oath that this vulnerability in the Dominion voting system can be used to "steal votes", and requests the federal court allow him to give the Critical Infrastructure Security Agency (CISA) immediate access to his report detailing his findings.⁶ The findings in this report agree with Professor Halderman's finding that the system can be used to steal elections.

³ Even the Center for Internet Security (CIS) recognizes the need for these controls in their Handbook for Election Infrastructure Security: <https://www.cisecurity.org/wp-content/uploads/2018/02/CIS-Elections-eBook-15-Feb.pdf>. The National Institute of Standards and Technology (NIST), which chaired the development of the Voting Systems Standards extensively recommends the fundamental security principle of "Least Privilege" that has been ignored in the configuration of the EMS.

⁴ Professor of Computer Science & Engineering, University of Michigan, Director, University of Michigan Center for Computer Science and Society, Director, Michigan CSE Systems Lab, <https://jhalderm.com/>.

⁵ Declaration of J. Alex Halderman, *Curling et al. v. Raffensperger et al.*, 1:17-cv-02989-AT, Docket No. 1177-1, (ND Ga.).

⁶ *Id.*

A password was not necessary to access this EMS server.⁷ There are many mechanisms by which a server can be exploited and administrative access obtained without a password; the National Institute of Standards and Technology (NIST) National Vulnerability Database (NVD) has identified over eight hundred of these admin-access vulnerabilities⁸ (among hundreds of thousands of other vulnerabilities) since its inception in 2005, and the Common Vulnerabilities and Exposures (CVE) program operated by MITRE Corp. lists nearly 170,000 computer vulnerabilities⁹ that are *publicly known* since its inception in 1999.

Capability to Easily “Flip” Election Results Demonstrated

Tests demonstrate the vote totals can be easily changed, commonly known as “flipping the election,”¹⁰ in this critical Election Management System server. The VSS directs voting systems vendors, like DVS, to address this specific risk¹¹ but based on the software contained on the EMS that was analyzed, the vendor has not done so here. Further, the obliteration of audit trails (logs) on the EMS server makes it extraordinarily difficult (and maybe impossible) to forensically determine whether any external connection allowing unauthorized access to the voting system, wireless or wired, occurred before, during or after the elections.

This report describes the absence of legally required security features on the voting system and then demonstrates only a few examples of the many possible methods by which it is possible to change calculated vote totals and alter the results of an election as consequence of those security failures.

Voting System Components Manufactured and Assembled in China and Mexico

The Mesa County EMS server used through May 2021 (serial number 4NV1V52) was assembled in Mexico, and its motherboard was manufactured in China. It is well understood that foreign manufacture or assembly exposes the components to the risk of compromise through the installation of foreign-controlled access devices during manufacture in the reported supply-chain attack.¹²

Voting System Presents an Immediate threat and is Dangerous to use in the upcoming 2022 election

The tests conducted in this report demonstrate and document three test intrusions into the DVS Election Management System server using popular, commercially available software that allows easy access to vulnerable election records. Given even momentary access, a person with only moderate computer skills can perform such an intrusion. It is not possible to reconcile these massive security failures with the obvious

⁷ The Mesa County Co. DVS D-Suite 5.11-CO server was forensically restored in a virtual environment, and a common password reset/bypass technique was used. See Appendix K. Also see www.gaverifiedvoting.org/pdf-litigation/20200819-785_2-Declaration-Alex-Halderman.pdf

⁸https://nvd.nist.gov/vuln/search/results?form_type=Basic&results_type=overview&query=administrative+access&search_type=all&isCpeNameSearch=false

⁹ <https://www.cve.org/>

¹⁰ The switching of calculated vote totals in an election has been identified in 2 other jurisdictions: Fulton County, Pennsylvania, and Antrim County, Michigan. See <https://rumble.com/embed/vjr2u6/?pub=dw7pn> which documents testimony of the Fulton County finding.

¹¹ “Changing the calculated vote totals,” VSS, Volume 1, section 6.1, page 6-93. See Appendix A.

¹² <https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies>; See Appendix L for discussion.

requirements for such an important piece of critical infrastructure. In combination with mandatory audit records being deleted in violation of state and federal laws that require their preservation, and in violation of evidence preservation orders for active legal cases ¹³, this EMS server presents an immediate threat to election integrity, with potential grave consequence to Colorado and the Nation by allowing the unauthorized alteration of election results.

The threat is immediate because 2022 election processes are already underway with primary elections imminent, and many jurisdictions will use these systems, and citizens' electoral franchise will be at risk, if citizens and public officials are not warned.

The initial installation and continued presence of uncertified software (Microsoft SQL Server Management Studio) in the Mesa County EMS Server is a violation of law. However, the tests conducted for this report clearly demonstrate that it is not the SSMS software alone that enabled illegal access to and modification of election databases and scanned ballot images. The state certifying this software on a chronically insecure system does not remedy the system's chronic insecurity – it only obfuscates one problem (insecurity) with another (improper testing and certification).

In contrast to the testing and certification of DVS D-Suite 5.11-CO, the current certification in Colorado of DVS D-Suite 5.13 includes SSMS, but tests conducted in this examination demonstrate conclusively that the EMS system is insecure both with, and without, SSMS.

¹³ Log files and other auditable records of normal and abnormal activity on computer-based voting systems are not only election records which must be preserved for 22 months according to Federal law, and 25 months according to Colorado law, they also represent evidence that is subject to document preservation requirements in existing civil litigation and, foreseeable, for future civil and criminal cases.

Key Findings

Six Key Findings in this report are:

1. The Mesa County EMS server used in the 2020 General Election had Microsoft SQL Server Management Studio 17 installed in May 2017. This software is not listed on the official test and certification report nor on the vendor’s application to the Colorado Secretary of State for certification of DVS D-Suite version 5.11-CO signed by “Nick Ikonomakis,” VP, Engineering [Dominion Voting Systems], dated 6/6/2019. As it was not listed, tested, or certified, the unauthorized installation of this software violates and renders illegal the certification of the election system, and its use in an election.

2. The inclusion of unauthorized and uncertified Microsoft SQL Server Management Studio software, as configured, allows the bypassing of Dominion Voting Systems’ software and enables any data in the vote databases to be changed. For example, using the uncertified Microsoft SQL Server Management Studio software, it is a quick and simple task to “flip” the vote (change calculated vote totals, demonstrated herein by changing only two values in the database to flip tens of thousands of votes).

3. With the addition of a wireless access device (added to the test to emulate the presence of multiple wireless devices that exist on Mesa County’s DVS hardware), the insecure configuration of the Mesa County EMS server allowed the editing and changing of the calculated vote totals using a standard iPhone. Wireless access, whether enabled accidentally or enabled/added deliberately (even in secret) to a voting system network, enables intrusion, attack, and compromise of any electronic voting system. The security configuration of the EMS server was wholly inadequate to prevent such intrusions. Thirty-six wireless access devices were identified built-in to the Mesa County DVS D-Suite system components, as documented by Dell and the Secretary of State’s equipment inventory.

But, due to the DVS-specified configuration of the EMS, and the Secretary of State-approved procedures that overwrite audit records¹⁴ – by mandating that the EMS server “overwrite” log files “as needed,” and further, during the Secretary of State’s so-called “Trusted Build” update which overwrote the EMS server, both in violation of federal and state laws - it is at best, extremely difficult to determine from EMS server audit log data how or even whether the wireless connections were used during or affecting Mesa County’s elections.

4. The exceptionally poor security configuration of the EMS server’s operating system, firewall, and the improper and inadequate configuration of the SQL Server database management system (DBMS) enabled access to the election databases and the alteration of vote totals using freely available, non-DVS and non-Microsoft database app downloaded and installed onto on a cell phone.

¹⁴ Approved, by certifying vendor supplied information. CRS-1-5-620 states that the vendor provides documentation including manuals to the Secretary of State, and any information not on file with and approved by the Secretary of State shall not be used in an election.

5. The Colorado Secretary of State's certification of DVS D-Suite version 5.11-CO for use throughout the state of Colorado was illegal,¹⁵ given the overwhelming number of VSS compliance violations found within the EMS server, which undermine the credibility of the claimed testing, technical competency of the testing lab, and the Secretary of State's certification.

6. The Mesa County, Colorado EMS server as used in elections including the 2020 General Election, and the April 2021 Grand Junction Municipal Election, has been shown to be insecure and grossly misconfigured such that it could not prevent unauthorized access to the election database or, as explicitly required by the VSS, prevent "changing the calculated vote totals" (demonstrated using an exact forensic replica of the system). This constitutes a material violation of the VSS requirements. It was possible to access the EMS server and change only 2 numbers in the database to completely reverse the Mesa County election 2020 Presidential election results stored on the EMS server. If this was done during the election, the EMS server would have then reported the changed vote totals as its authentic result.

¹⁵ The Colorado Secretary of State's certification of both DVS D-Suite 5.11-CO and 5.13 were also apparently illegal under state law, given that testing by a federally accredited testing lab is prerequisite for certification under Colorado law, and the Secretary's certifications both relied upon testing by an unaccredited voting system testing lab.

Analysis Summary: Compliance of Mesa County, Colorado, DVS D-Suite systems with the law

Four Key Objectives for this assessment are:

1. To determine whether implemented security capabilities comply with the 2002 Voting System Standards (VSS), mandatory under Colorado law;
2. To determine whether the results of an election stored on the EMS server can be altered by any person with physical access to the logged-in EMS server,
3. To determine whether the results of an election stored on the EMS server can be altered by any person using even a non-Dominion computer directly or indirectly connected to the EMS server network, and
4. To determine whether the results of an election stored on the EMS server can be altered by any person using a device such as a cell phone wirelessly connected to the EMS server network.

It is recommended that this report be viewed on a computer. Some of the screen images may be difficult to read when printed on paper, but viewed on a computer they can be expanded (zoomed in) and are easily read.

Documented in this report is a series of tests conducted as part of the examination to evaluate a few aspects of the security compliance¹⁶ of the Mesa County, Colorado DVS D-Suite version 5.11-CO EMS server, and the findings from that examination. These tests were limited to the EMS server. The EMS server receives and stores ballots in the form of electronic ballot images and cast vote records (CVR) from each ballot optically scanned into ImageCast Central (ICC) scanning/tabulation machines, and tabulates the results of the election. The images, CVRs, tabulated results and all system log files that document every aspect of system state, access, and operation are critical election records. The EMS server is one of the most critical components of the voting system and the security of its election records is of paramount importance.

The examination began with no pre-conceived assumptions about vulnerabilities and security. An identical copy of the Mesa County EMS server hard drive image¹⁷ was mounted and tested to exactly replicate the conditions of use during elections conducted between the installation of version 5.11-CO in 2019 and its replacement on May 25, 2021. The identified uncertified SSMS software component was installed earlier and very likely presented this same security weakness since its installation in 2017, but the scope of the tests in this report only addresses the 2019-2021 period. The computer-based voting system is extraordinarily complex and requires skill, knowledge, and diligence to configure securely. Despite being custom-ordered and then configured by the vendor, the critical nature of voting systems and the extreme importance of securely configuring these computer-based systems requires that voting systems be tested by competent cybersecurity professionals to determine their vulnerability. Colorado law requires only that

¹⁶ The evaluation identified critical weaknesses in the system and this report documents those findings. A comprehensive evaluation of every possible defect is beyond the scope of this report; the investigation is ongoing.

¹⁷ An identical copy of the Logical drive image, mounted within an Oracle VirtualBox virtual environment.

they be tested by a laboratory accredited by the U.S. Election Assistance Commission (EAC) and the results certified by the Colorado Secretary of State.

The DVS application to the Colorado Secretary of State for certification of DVS D-Suite 5.11-CO represents that this system “meets the requirements of the Colorado Secretary of State Election Rules (8 CCR 1505-1)” (which specify that all voting systems in Colorado must meet the requirements of the 2002 VSS).¹⁸ This includes documentation of the “minimum services needed for the successful, secure and hardened operation of the voting system” and “contains security measures for all systems, software, devices (upload, download, and other programming devices) that act as connectors and any additional recommended security measures.” While this provision of law addresses documentation to be provided, it is also necessarily required that the documentation be truthful and accurate. A forensic examination of this system, and tests performed in this examination, clearly show that these requirements are not met; the system is not secure and certainly not hardened against unauthorized access.

Testing confirmed that an outside party could use a separate computer as well as a cell phone, with publicly available and widely used free software (none of which were part of the DVS D-Suite), to easily change election results. The obliteration of audit trails on the EMS server by DVS and the Secretary of State personnel during the “trusted build” process diminished the ability to forensically determine whether any network connections (including wireless connections or intrusions) were made to the EMS server. Thirty-five wireless devices were identified on the DVS D-Suite system, including the ImageCast Voter Activation (ICVA) computer, serial number 2DX0Z52, ordered on August 16, 2015 by DVS for use in Mesa County. It was ordered by DVS configured with a Dell Wireless 1560 internal wireless adapter, providing both 2.4GHz and 5GHz (dual band) Wi-Fi and Bluetooth connectivity to and through that ICVA computer. In total, Mesa County was provided thirty-five D-Suite components with wireless capability installed: Dell Latitude 7450 computers providing ICVA functionality, serial nos. 8GX0Z52, 8JX0Z52, BCX0Z52 with Dell Wireless 1560 modules, and Dell Optiplex 9030 ImageCast Central (ICC) systems, serial nos. H4B4T52, H4G0T52, H4JBT52, and H4L9T52 with Dell Wireless modules. A Dell E310DW wireless printer was configured as the EMS server’s default printer, with IP address 192.168.100.11, bringing the total number of wireless devices to thirty-six. Wireless device encryption can be easily broken,¹⁹ and the vulnerabilities are online and in the Computer Vulnerabilities and Exposures (CVE) database.²⁰ A demonstration video of this intrusion is also available.²¹ Twenty-eight (28) tablets, provided by DVS as ICX devices in the D-Suite system, include

¹⁸ [https://web.archive.org/web/20201018013640/https://www.sos.state.co.us/pubs/rule_making/CurrentRules/8C CR1505-1/Rule21.pdf](https://web.archive.org/web/20201018013640/https://www.sos.state.co.us/pubs/rule_making/CurrentRules/8C%20CR1505-1/Rule21.pdf)

¹⁹ Vulnerability: <http://www.dell.com/support/kbdoc/en-us/000125799/wi-fi-security-protocol-key-re-installation-attack-krack-impact-status-on-dell-products>; Published and freely available code to implement the attack: <https://www.joe0.com/2017/11/11/kali-linux-virtualbox-instructions-for-testing-wi-fi-devices-against-wpa2-key-reinstallation-attack-krack-attack/>

²⁰ <http://cve.mitre.org/> : CVE-2017-13077, CVE-2017-13078, CVE-2017-13079, CVE-2017-13080, CVE-2017-13081, CVE-2017-13082, CVE-2017-13084, CVE-2017-13086, CVE-2017-13087, CVE-2017-13088. This attack is against the WPA2 encryption protocol and all wireless devices, regardless of manufacturer, are impacted.

²¹ <http://www.krackattacks.com/>, [Key Reinstallation Attacks: Forcing Nonce Reuse in WPA2](https://papers.mathyvanhoef.com/ccs2017.pdf), Vanhoef and Piessens, <https://papers.mathyvanhoef.com/ccs2017.pdf>

wireless capability. The prior expert analysis and testimony of Professor Halderman further confirms the vulnerability of these Dominion ICX components to malicious attack and compromise by an outside party.²²

Because of the extraordinary nature of the “back-door” identified and because internal wireless devices were included as part of the DVS D-Suite system used in Mesa County, I added a wireless access device to the server network during testing to properly replicate the actual hardware used in Mesa County. This enabled determination of whether the system vulnerabilities could be exploited with the more limited capabilities of a mobile device. This report describes testing that demonstrates how easily the design and configuration of this voting system allows this type of exploitation.²³

The tests in this report first demonstrate that any person with physical access to the logged-in EMS system can change the election database results (calculated vote totals), with²⁴ or without²⁵ a userID and password, on the Mesa County EMS before, during, or after the election by using a few mouse clicks. By itself, the ability of any user to modify election database totals illustrates the voting system’s non-compliance with VSS and Colorado law. The tests also demonstrate that if the voting system has any external connection for even a moment, a person anywhere in the world can change the election database results on the EMS server with a few mouse clicks. This is an extraordinary danger to election integrity.

The protection offered by use of passwords is further weakened by the fact that different userIDs created on the EMS server share the same password.²⁶ Shared passwords were also reported in the Maricopa, Arizona forensic audit.²⁷ Rudimentary security protocol demands that each userID must have its own unique password. The sharing of password across accounts renders ineffective individual accountability for actions by a user (each assigned a specific userID, required for access control mandated by VSS and the ability of audit trails to identify fraudulent activity). This renders the system noncompliant with VSS requirements. VSS mandates, among other things, that the system: (1) “establish and maintain controls that can ensure that accidents, inadvertent mistakes, and errors are minimized; (2) protect the system from intentional manipulation and fraud, and from malicious mischief”; and (3) identify fraudulent or erroneous changes to the system.”²⁸ Other jurisdictions have learned that they do not have control of their voting systems but the vendor, Dominion Voting Systems, has the administrative passwords and, therefore,

²² www.gaverifiedvoting.org/pdf-litigation/20200819-785_2-Declaration-Alex-Halderman.pdf

²³ The VSS expressly identifies the prevention of this type of manipulation in its security objectives for voting systems, VSS Volume 1, section 6.1, page 6-93, excerpted in Appendix A.

²⁴ I accessed the EMS server with and without a password. I was able to guess the password, and separately used a well-known password bypass technique, both methods were successful and I gained access to a copy of the EMS server in an Oracle VirtualBox environment.

²⁵ Passwords are easily bypassed, and knowledge of a specific password is not required, since access can be obtained without a password. See Appendix K.

²⁶ Thirty different userIDs on the Mesa County EMS server were found to share an identical password. Two of those accounts were enabled and active.

²⁷ Maricopa County Forensic Election Audit, Volume III, section 6.5.2.1.3

²⁸ (VSS V1, 6.1, page 6-93, see Appendix A).

control.²⁹ Mesa County’s DVS EMS server has an administrator account installed specifically for Dominion Voting Systems’ use.³⁰ In light of the legal and security responsibilities in the administration of elections, allowing a vendor (in this case DVS) to maintain administrator access to the voting system is inexplicable, as is the exclusion of local election officials from control over their own elections.

The names of account userIDs on Mesa County’s EMS server, created during the installation of DVS D-Suite 5.11-CO, are generic. Generic account userIDs were also found in the Maricopa, Arizona audit.³¹ This finding in Arizona strongly suggests that it is a DVS practice to use generic userIDs and the same userIDs are likely used on *every* DVS election system in the USA. As one of the two components of required authentication (userID and password), this is an extraordinary compromise of security, as it is likely that once a userID from one state is known, it may be known for *all* states.

The examination found that the EMS server network was active and in use; the Ethernet network interface was found to be enabled, an IP address was found to be assigned, and election databases and ballot images were found to be stored on the EMS ‘NAS’ disk drive. The drive was shared to the connected network.³² Any representation that the EMS server was not connected to a network is false. The transmission control protocol / internet protocol (TCP/IP) port that supports direct back-end database access on the EMS server was found to be unprotected by anything other than Windows authentication (a common userID and a shared password) and any person who gains unauthorized access will have full access to ballot images and the tabulated vote databases, in violation of the 2002 VSS.

The tests conducted in this examination found the system to be insecure and also ensured that no protections that might otherwise have secured the system were overlooked by the examination process. No advanced security penetration techniques were needed; the initial access to the operating system (i.e., “login”) was performed both by guessing the password as well as by using well-known and easy to find password bypass techniques. The unauthorized and uncertified Microsoft SQL Server Management Studio software³³ (“SSMS”) on the EMS server was run and access to the SQL server databases on the EMS server, which should be highly restricted, was granted without restriction or challenge. This same access has been found in other forensic examinations of virtually identical DVS D-Suite voting systems used in at least two other states.³⁴ A non-Microsoft, non-DVS software application that supports SQL database access was also used (from an iPhone) and access to Mesa County EMS server election databases was obtained, allowing

²⁹ Maricopa County Forensic Election Audit, Volume III, section 6.5.3.1.3. See also <https://www.westernjournal.com/az-audit-exclusive-election-systems-password-hasnt-changed-2-years-shared-time/>.

³⁰ Account names are withheld in this report to protect the security of the system, since an account name and a password are literally the only things protecting this system.

³¹ Maricopa County Forensic Election Audit, Volume III, section 6.5.2.1.3

³² Dominion misleadingly refers to this as “NAS.” It is not. NAS stands for Network-Attached Storage. This storage was found not to be network-attached, but instead, “direct-attached,” and is thus a DAS instead of a NAS.

³³ D:\Program Files (x86)\Microsoft SQL Server\140\Tools\Binn\ManagementStudio\Ssms.exe.

³⁴ Analysis of the Antrim County, Michigan November 2020 Election Incident, J. Alex Halderman, March 26, 2021, p.10; September 24, 2021, Presentation of Ben Cotton entitled *Arizona Senate Audit, Digital Findings*, slide 13.

changes to the calculated vote totals. Testing shows conclusively that the voting system was not secure and that protections required by law were not enabled.

Report #1 documented the destruction of system log files that voting systems are required to generate and preserve in order to comply with federal and Colorado law.³⁵) Those critical election records would be necessary to allow a forensic examiner to identify whether any changes to the election databases were made, and when and how they occurred. This system did not preserve those election records,³⁶ in violation of federal and Colorado law. This failure was a direct result of the system configurations and technical guidance as directed by Dominion and mandated by the Colorado Secretary of State for all counties using D-Suite version 5.11-CO EMS servers. The installation of the voting system software update (called the “Trusted Build”) by the Secretary of State, assisted by DVS personnel, in all DVS-equipped Colorado counties further overwrote and eradicated most records necessary to perform a forensic audit of the affected elections.

As a direct result of the destruction of those election records (in the form of log files that provide an audit trail required by law to be preserved), any examiner, much less a non-expert public official, will find it difficult if not impossible to determine conclusively that the voting systems have not been tampered with or operated in an unauthorized manner. Destruction of those election records prevents detection and/or confirmation that the vulnerabilities identified in this report were not exploited to alter election results.

A full, independent forensic audit should be conducted in any jurisdiction that used this system, given the extraordinary insecurity and non-compliance of this voting system with both legal standards and industry-recognized best practices and the failure of the existing testing and certification regime to detect those conditions,. Such an audit should include every component of the voting system, all electronic logs, removable media, and escrowed source code. Cast paper ballots should be examined for authenticity and then recounted in order to have confidence that the tabulated vote count matches the paper ballots. Because of the obliteration of audit trail data, audit techniques which rely upon small, statistical sampling of results (so-called “risk-limiting audits”) are not reliable. No person can trust any result obtained from this system in any election in which it was used due to the extreme insecurity of this voting system.

Although this examination addresses the local Mesa County, Colorado election results stored on the Mesa County EMS server, similar destruction of election records and the security weaknesses that enabled it are highly likely to have occurred across Colorado and possibly other jurisdictions. The configuration of the

³⁵ Appendix A, VSS, Retention Requirement

³⁶ If not for the action of the Mesa County Clerk, who forensically preserved the Mesa County election records by backup of EMS server hard drive, the auditable record of the partial EMS server log files that remained from the November 2020 General Election and the April 2021 Grand Junction Municipal Election would have been destroyed by the Secretary of State's action and direction. That destruction of election records by DVS and the Secretary of State would have precluded a forensic audit of those elections and prevented the exposure of the voting system vulnerabilities as they existed in the November 2020 general election and the April 2021 Grand Junction Municipal Election. Failure to meet statutory-security compliance requirements would have been hidden from both public officials and the public. Neither the Secretary of State nor DVS instructed election officials to properly preserve these critical electronic records prior to these destructive “updates” and instead instructed them only to preserve ballot images and related election project files.

system is required to be tested by EAC-accredited testing labs, controlled through certification by the Colorado Secretary of State, and specified by Dominion Voting Systems (DVS), so it is almost certain this system is used throughout Colorado, and it is likely very similar, if not identical to systems used in other states.

Examination of the EMS server found that unauthorized Microsoft SQL Server Management Studio software³⁷ (“SSMS”) was installed on 5/17/2017 at 06:49:44 AM. Given that the “trusted build” process was used in 2019 and overwrote all previous data on the Mesa County EMS server, SSMS must have been installed by DVS on its golden image of the D-Suite system; if it were installed by Mesa County staff, the installation date could not have preceded the DVS installation date of D-Suite 5.11-CO in 2019. SSMS remained installed on Mesa County’s EMS server through the backup imaging conducted in May 2021. That software was present on the 5.11-CO EMS server but not listed on the Certification Application or testing report for the DVS D-Suite 5.11-CO system. This failure of the manufacturer to meet, the voting system testing lab to verify, and the Colorado Secretary of State to ensure that minimum Federal Voting System Standards were met, as required by law, is inexcusable and grossly violates industry standards. Only after this software was noted in an expert report, dated December 13, 2020, and submitted in connection with a widely publicized vote switching controversy in Antrim County Michigan involving DVS D-Suite systems, did DVS submit an application for certification for version 5.13-CO, dated Jan. 13, 2021 which listed SSMS as an installed software component.³⁸

Name	File Ext	Logical Size	Category	File Created
📄 Ssms.exe	exe	720,632	Executable	05/17/17 06:49:44 AM (-4:00 Eastern Daylight Time)

Figure 1 - SSMS Installation Date on Mesa County EMS server

The Colorado Secretary of State should have been aware that this separate software component (a completely separate download from Microsoft) was required to be listed on the application for certification, tested by a federally-accredited lab, and certified. The addition of MS SQL Server Management Studio is not necessary to the election process, and allows any party with access to the EMS server to alter cast ballots, tallies, databases, ballots, and audit records with up to full administrative permission.

Examination revealed fundamental flaws within the security configuration of the Mesa County Election Management System (EMS) server used in the November 2020 general election and the April 2021 Grand Junction municipal election that show conclusively that this voting system and its software, as delivered by Dominion Voting Systems and certified by the Colorado Secretary of State, is uncertifiable under Colorado law because it contains unauthorized, untested and uncertified software in violation of the law, is configured in a manner that violates mandatory VSS and industry best-practice security standards, allows “intentional manipulation and fraud” that the VSS standard prohibits, and fails to log system events and preserve audit trails required by VSS in a manner that makes determination of election integrity extremely difficult, and maybe impossible.

Nationwide, various election officials have denied qualified third-party investigators the access to election system equipment including logs, network and security equipment configurations, and network diagrams,

³⁷ D:\Program Files (x86)\Microsoft SQL Server\140\Tools\Binn\ManagementStudio\Ssms.exe.

³⁸ See Antrim Michigan Forensics Report, Allied Security Operations Group, December 13, 2020.

that might allow the detection of unauthorized access and operation of voting systems. This report demonstrates why this is a dangerous development because the denial of access prevents the discovery of the full extent of the failure of election security and election records integrity.

The techniques used in this report employ basic network troubleshooting techniques that can readily be executed by persons with minimal skills. In fact, software found to be already installed on the EMS server (Microsoft SQL Server Management Studio was downloaded and installed on the test workstation, while Fing and SQL Pro from the Apple App Store were installed on an iPhone). In each instance, the software was launched and access was granted. It was so simple that calling the test an “attack” is almost inappropriate, since standard publicly-available software was used without modification and connection was made in an industry standard manner to the default port assigned for SQL databases.³⁹ The server had no security implemented other than userID and password, and even that is easily bypassed.⁴⁰ In this case it was not a smart examiner but the exceptionally insecure configuration of the voting system that was at fault in failing to meet the requirements of law. That exceptionally insecure configuration is an open invitation to the average hacker, and indeed almost anyone with basic skills, to be able to change election results.

But it is not the average “hacker” or even cyber-criminals that provide the greatest threat to election integrity. While it has been stressed that these *relatively simple* intrusions could be done by anyone with a reasonable understanding of networks, the fact is that nation-state adversaries have long attacked and subverted the critical infrastructure of the United States,⁴¹ as documented in Appendix D. The extreme sophistication of these nation-state actors' cyber threat capabilities has persisted for decades, evolved far beyond the knowledge of the average citizen, and the history of publicly-known attacks document it beyond question. Malicious actors, including foreign nation-states, our most capable and persistent adversaries, already know how to subvert insecure systems, like this election infrastructure.

The evidence of foreign interest in our voting systems is too important to bury in a footnote: four (4) Korean students, at 2 different Korean universities, authored the paper [A Study of Vulnerabilities in E-Voting System](https://www.researchgate.net/publication/315040247_A_Study_of_Vulnerabilities_in_E-Voting_System), Xing Shu Li, Hyang ran Lee, Malrey Lee and Jae-young Choi, *Advanced Science and Technology Letters Vol.95 (CIA 2015)*, pp.136-139, https://www.researchgate.net/publication/315040247_A_Study_of_Vulnerabilities_in_E-Voting_System. Section 2 discusses “hybrid election systems” that are exactly what the Dominion Democracy Suite elections systems are.

Continued suppression of the knowledge of this system’s extreme security failures, long known to foreign nation-states and others, does not further the security of critical infrastructure election systems – indeed, elections have taken place and are ongoing while these known security failures have been left unaddressed.

For example, in his September 21, 2021 Declaration, Professor Halderman attached an email string with CISA dated August 18-19, 2021, wherein he requested that the federal district court allow him to

³⁹ The standard port for SQL database access is 1433. When this port is found open, it is obvious that it provides access to a database system. The port number can and should be reassigned to another number to improve security, making the discovery of database access more difficult, and is an example of multi-layered “Defense in Depth.”

⁴⁰ Appendix K.

⁴¹ <https://www.whitehatsec.com/blog/2020-election-security-the-urgent-need-to-address-vulnerabilities-in-voting-systems/>

immediately provide his sealed expert report to CISA because of the threat posed to the election systems in sixteen states—including Colorado—by DVS machines with ICX software that can be used to “steal votes.” In that August, 2021, exchange, CISA agreed to receive Halderman’s expert report detailing these security failures. However, even though Professor Halderman testified in his Declaration that this threat was “urgent,” and that it would take “months” to fix these “critical vulnerabilities,” CISA inexplicably waited to even seek Prof. Halderman’s report until more than five months had passed—to January 21, 2022.⁴² The voting systems Halderman described as critically vulnerable were used in the November, 2021, elections in the U.S., including in Colorado. Thus, the suppression of knowledge of security failures has indeed harmed election security and facilitates continued malfeasance.

The security and configuration of the equipment images examined to date leaves no doubt that our voting systems are dangerously insecure, and renders absurd any claim of election integrity.

This examination has demonstrated the ability for any individual to change the calculated vote totals in the internal database tables used in an actual election, bypassing any Dominion Voting System software security and access controls, with no record preserved in log files that are meant to comprise an audit trail of election records. It demonstrates how trivially election results data can be tampered with and even changed completely by someone with physical access to the EMS server, or by using a non-DVS computer attached to the network, or even by using a cell phone or mobile device if wireless access has by any means been enabled on the network.

⁴² Statement of Interest [by CISA], *Curling et al. v. Raffensperger et al.*, 1:17-cv-02989-AT, Docket No. 1269-1 (filed February 10, 2022), (ND Ga.).

EXAMINATION METHODOLOGY

Description of the Examined System

The voting systems used in Mesa County, Colorado, like other systems used across the state and the nation, are made by Dominion Voting Systems (DVS). Many of these voting systems are comprised of an industry-standard computer⁴³ that uses a Microsoft operating system and a combination of proprietary Dominion application software and non-proprietary, commercially available software. This provides a foundation for election-related functions including creating election projects, defining ballots, capturing and storing the election data in a secure database management system, tabulating and counting the votes, and reporting election results.

The Mesa County Election Management System (EMS) server runs on the Microsoft (MS) Windows Server 2016 operating system, and it employs a database management system known as Microsoft SQL Server (SQL Server). The security of the server depends largely upon the proper configuration of the operating system, network, and the SQL Server.

The design of the voting system includes the functional capability to adjudicate ballots that the computer cannot accurately interpret. Adjudication, in this regard, means nominally, that a person sits in front of a computer terminal, a ballot image is shown on the screen, and this person chooses the option that they feel the voter intended to choose. Adjudication is facilitated by a software application that runs on the EMS system (part of the DVS software) and, normally on one or more Adjudication workstations. If unauthorized code is executed on the EMS system, including on Adjudication workstations or other DVS workstations authorized to be connected to the EMS server, or if an unauthorized user is accessing or has accessed an Adjudication workstation, the adjudication function may be executed to adjudicate ballots without the intervention or knowledge of any authorized operator.

This process requires that the EMS server (which stores and provides access to the election databases and ballot images) be connected to a network. While necessary for the adjudication function to work in the present design of the voting system, this design requirement significantly raises the risk of abuse, especially considering the failure to implement required security.

The Mesa County election director at the time reported that the D-Suite 5.11-CO network consisted of a single network switch connecting only specifically-designated components of the voting system, including the EMS server, adjudication workstations, an EMS server client workstation hosting the Election Event Designer (EED) software, and a Network Attached Storage (NAS) file server.⁴⁴ DVS documents the connection of these systems in their manuals. Therefore, while the EMS server may not have been directly connected to the Internet (it is impossible to rule out, without access to all logs which should have been generated and preserved), it was connected to other computers via a network to allow specific voting system devices to communicate with each other. These other computers must be fully examined to assure

⁴³ An “industry-standard” computer is comprised of common components (motherboard, bus, memory, processors, communications, input/output ports) in a common architecture, e.g., the type of computers one purchase in big box stores and find in use in a home-use or business setting, running office productivity and web-browsing software.

⁴⁴ The term Network Attached File Server is, in this case, a misnomer. DVS uses the term NAS, however it is a shared disk drive on the EMS server itself. In this report, I may use the term synonymously, but there is a difference that will be noted where relevant.

that no connection to external devices or networks (including the Internet) occurred, because connection to other computers exposes the EMS server to a common “Island-Hopping attack,⁴⁵” which is where every device attached to the EMS network may have a direct or indirect path to and from a device or network outside of the election network, providing a path for an attacker’s movement through networked devices to the target. For example, the computers in a home are typically all connected to each other via a wired and/or wireless network, and because the home router is connected to the internet, all devices in that home also have a path to the internet.

The voting system network (based on DVS manuals, EMS server image information, and election official input) was reproduced, both with a virtual network environment and again with a physical Ethernet network composed of cables and a small desktop network switch, to allow the network connection of a Test Workstation used in this report. This configuration was used to test access to the EMS server by a person sitting in front of the EMS server, and again to test access to the EMS server by even a non-Dominion computer that connects to this network. To test whether access from a device with more limited capability such as a mobile phone was possible, a wireless access device was added to the network to simulate the hardware used in Mesa County and the enabling, through misconfiguration or malicious action, of one or more of these wireless devices to provide access, even temporarily. Because I did not physically see or examine the original setup of the voting system network in the Mesa County facility, and due to the destruction of log data by both improper configuration and the overwriting of log files, it is not possible to provide conclusive forensic verification that the voting system was not connected to unauthorized external networks or devices, including wireless devices.⁴⁶ It should be noted that seven internal wireless adapters, and twenty-eight wireless-equipped ICX devices, were ordered as components of the Mesa County DVS D-Suite system, as supplied by DVS. In addition, a Dell E310DW wireless-capable network printer was configured as the default printer on the Mesa County EMS server. This brings the total number of wireless access devices to a total of thirty-six devices.

The EMS server has a software firewall. The purpose of having a firewall is to address the risk of access to the EMS server from all unauthorized devices, users, networks, methods, ports, Internet Protocol (IP) addresses or groups of addresses, and during specific time periods. However, a firewall must be specifically configured (programmed) to perform these functions. One risk of a software firewall is that all users with administrative access can change its programming because it resides on the EMS server; a separate hardware firewall device with its own non-shared password mitigates this risk. Per the VSS and required

⁴⁵ In an Island-Hopping attack, a threat actor gains access to a target computer remotely, through other, connected computers or devices. E.g., a target computer (which we’ll call “A”) is connected to computer or device “B” (e.g., a network printer). Computer or device “B” is connected to computer or device “C” and computer/device “C” is connected to computer/device “D”. It is not necessary that they all be connected in a single physical network. In fact, most modern computers have one or more wireless communications devices; such a wireless capability could allow the access that enables an Island-hopping attack. It is not necessary that the connection be of long duration. The attacker might enter and compromise computer “D” from the global Internet over a wireless connection, determine that computer “C” is connected, break-in to computer “C, move through its connection to computer “B,” and finally to computer “A” (which is may be particularly vulnerable if there is an assumed trusted relationship/connection between computers “B” and “A.” This chain of connection and intrusions ultimately allows the complete compromise of the target computer.

⁴⁶ More detail will be provided in a subsequent forensic report.

by Colorado Law,⁴⁷ risks that must be addressed by a voting system include “Preventing access to vote data, including individual votes and vote totals, to unauthorized individuals.” The EMS server firewall was found to be programmed specifically to permit access to back-end database services, enabling access to vote data and vote totals⁴⁸ on the Mesa County EMS server from ANY IP-address, globally, at any time. This configuration fails to meet requirements in the law, as well as every industry best practice recommendation for firewall rule configuration.

SQL Server, a database management system (DBMS), installed and used on the EMS server (which stores and manages the election databases) is accessible using any software tool supporting connection to SQL Server, employing Windows Authentication. One of the most common and freely available tools is known as Microsoft SQL Server Management Studio (“SSMS”). SSMS is free and available to download from Microsoft from any internet connection. In this examination it was downloaded from Microsoft, installed on the test workstation, and in a matter of minutes, used to easily and directly access the back-end election database and change any data in it. Searching the internet for ‘how to install SQL server management studio,’ the first result was: <https://docs.microsoft.com/en-us/sql/ssms/download-sql-server-management-studio-ssms?view=sql-server-ver15>, which walks anyone through installing the software while other readily-accessible online videos walk even a novice through the installation.

But even that is not required for anyone with physical access to the EMS server, because SSMS software was found already installed on the Mesa County EMS server image. This software is not on the list of certified software for DVS D-Suite 5.11-CO nor reasonably expected on a voting system, due to the vulnerability it introduces. This addition in itself violates the stated certification of the voting system.

Software (SSMS) that allows direct access to the back end of the election results database and allows changing vote totals was found installed and functional on the Mesa County EMS server. The software firewall, that could have severely restricted access, was programmed instead to allow access from anywhere in the world. Although the VSS does not specifically address firewall configuration, it does specify addressing this kind of risk, and the firewall, supplied by Microsoft as part of the computer operating system could have and should have been programmed to limit access, at a minimum to only those Mesa County devices required to connect to the EMS server (the few other DVS D-Suite computers and devices necessary could be restricted by their specific IP addresses, for example). Such a configuration would also prevent the wireless access demonstrated by my tests and documented in this report, by disallowing its connection, had the firewall been used to control this database access (port 1433, or an alternate port, explained later in this document). However, given the presence of internal wireless devices as part of the DVS D-Suite system, a properly configured firewall rule on the EMS server that restricted access from only other Dominion devices on that network still may not prevent unauthorized access from occurring through the individually-authorized yet wireless-capable devices.⁴⁹ Possibly most alarming, I found a firewall rule that allows global (from anywhere in the world) access, is not supplied by Microsoft, and must have been explicitly created. Allowing global access is extraordinarily irresponsible, particularly given that SSMS enables direct access to the vote data. This dangerous combination constitutes what is commonly known

⁴⁷ See VSS Volume 1, section 6.1.

⁴⁸ This firewall could have prevented access but instead specifically allowed it.

⁴⁹ This means that the security implemented on every one of these connected devices must be as strong as that of the server that holds and tabulates ballots.

as a “back door” into the voting system, and together with deleted audit trails presents an undetectable path for unauthorized access to, and illegal manipulation of, election data. The failure of the software firewall is not the only access control that was misconfigured. Access control mechanisms in the DBMS itself failed to prevent the access demonstrated in these relatively simple tests.

It must be emphasized that this test was done on a virtual replica of the Mesa County EMS server, created from an image of that EMS server’s hard drive, and not on the actual in-use election system.⁵⁰

For all practical purposes, the term “Mesa County EMS server” is used to mean the logical image⁵¹ of the Mesa County EMS server recreated from the forensic, integrity-controlled Encase Forensic Archive of the actual Mesa County EMS server. The original forensic image of the system was obtained using Access Data’s Forensic Tool Kit Forensic Imaging software. Access Data is an industry-standard forensic software vendor. I had no access to the actual Mesa County EMS server hardware and have relied upon forensic images of that server furnished by legal counsel to create a virtual replica of the EMS server.

Access was attempted and established to the (replica) EMS server to determine the degree to which the EMS server was secured in accordance with legally-mandated VSS standards. The results were alarming. It was found that the SQL Server databases on the Mesa County EMS server were unprotected, beyond a simple password that can be bypassed.⁵² While many potential security restrictions were possible, it was found that surprisingly few were implemented. The SQL Server software on the EMS server was set up with a Windows Firewall with Advanced Security features, however, an explicit firewall rule on the EMS server allowed access directly to the SQL election databases back-end from any IP address in the world.

Security settings relevant to the SQL Server and access to the databases were examined. A subsequent report will address the comprehensive security implementation. This report focuses upon the EMS server’s failure to protect the election databases and the ease with which they can be accessed by any bad actor to change election results.

⁵⁰ A forensic image of a hard drive is a bit-for-bit copy of the user accessible data storage area residing on the data storage mechanism used by the computer system. For a complete discussion of this definition, see Appendix J.

⁵¹ The exact view of disk storage data as seen by the EMS server computer.

⁵² Appendix K.

FORENSIC ANALYSIS

SYSTEM IDENTIFICATION

The Mesa County, Colorado EMS server analyzed in this report is capable of operating on a local area network (LAN). The network consists of several systems, including servers and workstations. The server that was evaluated was named EMSSERVER. It is running the Microsoft Windows Server 2016 operating system.

The forensic evaluation and reviews were based upon a forensic image⁵³ archive collected from the Mesa County EMS server. The forensic image of the EMS server examined in this work was collected on May 23, 2021, before the Secretary of State staff, assisted by DVS personnel, installed their “Trusted Build” software update, as documented below. The serial number of the hard drive shown in the collection data set verifies the data origin to be the physical device.

The backup image was obtained, using forensic imaging methods (an AccessData FTK Imager), from the DVS D-Suite EMS Standard Server, version 5.11-CO, in Mesa County, Colorado, as used in the November, 2020 election. The acquisition data are presented in Figure 2.⁵⁴

⁵³ A forensic image (forensic copy) is a bit-by-bit, sector-by-sector duplicate of a physical storage device’s user accessible storage area using specialized hardware and software. To be technically accurate, hard drives contain a “service area” that is not accessible by the user or the Operating system, nor by forensic software; this service area is accessed by the drive’s internal controller. The service area is used by the firmware in the disk drive to identify defects in the media introduced during manufacture as well as those identified during operation. Making a perfect magnetic storage platter would be prohibitively expensive thus they are made to be fault tolerant, and the defective areas are simply skipped by using a defect-map. Forensic imaging is a much more comprehensive representation of the state and configuration of the imaged system than could be obtained using simple file backup methods. Forensic Imaging copies data from the subject data storage media without altering the original data in any way. The image includes all files, folders, and unallocated, free, and slack space as well as copies of internal Microsoft files that are protected from access during a normal backup (including the MS “Registry database” and other protected files). These forensic images include not only all the files visible to the server operating system but also deleted files and fragments of files left in the slack and free space as well as every digital bit of data present on the storage medium. When multiple disks are configured into a Redundant Array of Independent Disk (RAID) array, the RAID controller provides a “logical view” of every bit on the media to provide a sector-by-sector bit-for-bit copy of the storage medium; this permits, for example, the use of two identical disk storage devices to provide double the space of a single device, or two devices configured as mirror images of each other to provide failure redundancy. While there are many different configurations for RAID subsystems, a RAID subsystem provides the exact same view of the storage medium and data access to a forensic imaging process as it does to the computer in which it is installed.

⁵⁴ To the extent that personal identifying information was identified in Figure 2, it has been removed. This in no way affects the accuracy of the findings in this report or the evidence.

Created By AccessData® FTK® Imager 4.2.0.13

Case Information:

Acquired using: ADI4.2.0.13

Case Number: 052321

Evidence Number: 00003

Unique description: EMSSERVER

Information for F:\EMSSERVER\EMSSERVER:

Physical Evidentiary Item (Source) Information:

[Device Info]

Source Type: Physical

[Drive Geometry]

Cylinders: 121,534

Tracks per Cylinder: 255

Sectors per Track: 63

Bytes per Sector: 512

Sector Count: 1,952,448,512

[Physical Drive Information]

Drive Model: DELL PERC H730 Adp SCSI Disk Device

Drive Serial Number: 00222e64128c016e1d004fc54220844a

Drive Interface Type: SCSI

Removable drive: False

Source data size: 953344 MB

Sector count: 1952448512

[Computed Hashes]

MD5 checksum: 3d7cf05ca6e4 2db765bf5c15220c097d

SHA1 checksum: eab06a7ea23586de2746b9142461717e075f5c9f

Image Information:

Acquisition finished: Sun May 23 2021

Figure 2 - Mesa County, Colorado EMS server (5.11-CO) Forensic Image Attributes

AUTHENTICITY

When forensic images are acquired, a hash function⁵⁵ is computed. This hash function is far more than a checksum, despite the “checksum” reference in Figure 2. The mathematical complexity of the hash function is sufficient such that there is only an infinitesimally small probability that any two different source files can produce the same resultant hash.⁵⁶ This hash can be used at any time to validate the integrity of the image to ensure that it has not been edited, modified, or changed in any way. The hash function result from the acquisition of data appears in the text above but also appears inside each respective archive and authenticates the data by demonstrating it has not changed since it was acquired. Moreover, two different hash functions (MD5 and SHA-1) are in the image and have never been shown to be simultaneously compromised in the same attack.

The hash function results were compared and match the data from the original collection of the forensic image. This provides the greatest mathematical assurance possible that the data in the forensic image examined is a true, authentic and unaltered copy of the original disk data.

Further confirmation that these are genuine images from the Mesa County EMS server has been provided by the Colorado Secretary of State’s office. See:

<https://www.sos.state.co.us/pubs/newsRoom/pressReleases/2021/PR20210817MesaCounty.html>⁵⁷

Chain of Custody

Digital chain of custody is the record of preservation of digital evidence from collection to presentation in the court of law. This is an essential part of the digital investigation process. The chain of custody is probative that the digital evidence presented to the court remains as originally collected, without tampering. The image analyzed in this report was obtained through AccessData FTK Imager 4.2.0.13.

⁵⁵ A hash function is a mathematical algorithm that converts an input (e.g., the bits of a file, or all the files on the hard drive) of arbitrary or variable length into an encrypted output of a fixed length. The purpose of the hash in this case, is to create a “signature” for the file or hard drive, such that any other party at any other time, can compute the hash of the file, files or hard drive and confirm that they are identical, because the hash outputs match.

⁵⁶ While the SHA-1 128-bit algorithm has been found possible to compromise, the attack required 9,223,372,036,854,775,808 computations of the algorithm. This is the equivalent of 6,500 years of single-CPU computations or 110 years using today’s modern Graphics Processing Units (as used in mining cryptocurrency). This attack required the use of two specifically-designed different files that produce the same hash, created by expert mathematicians explicitly for this purpose. Such an attack may be within the capability of a Nation-State or by spending an enormous amount on cloud computing. In its application as a sophisticated checksum, the effort to change an original dataset into a specific altered dataset with the same hash would present astronomical difficulty much greater than the 9.2 quintillion (quintillion means $\times 10^{18}$) computations in the attack referenced here, would require extraordinary resources, financing and would be exceptionally difficult to conceal. The likelihood of this occurring is infinitesimally small. The likelihood of this occurring undetectably is virtually zero. The probability of two different message digest algorithms being simultaneously fooled is nearly impossible and has never been shown to be possible.

⁵⁷ Reproduced in Appendix M.

I have reviewed the documented chain of custody for the image and have determined that the chain of custody is complete from the forensic operator utilizing FTK Imager through the source from which I directly received these images. (Because of the pending civil litigation and criminal investigation, the written documentation remains in the custody of counsel for later introduction in court proceedings and thus is not included as part of this report.)

Tools Used

The initial forensic image was acquired using Access Data FTK Imager. Once acquired, Encase Forensic was used to maintain forensic integrity of the archive. Autopsy, Encase Forensic, FTK Imager and Oracle VirtualBox were used to analyze the image. All findings were verified with Encase Forensic examination of the integrity-controlled forensic image.

TEST PREPARATION

The Mesa County EMS server forensic Image was used to recreate a complete and exact replica of the Mesa County EMS server's software, operating system, and even boot code, which was then launched in an Oracle VirtualBox⁵⁸ virtual computer environment for the examination. This technology is commonly used in software development and testing. This exact replica was used for this examination.

The image was evaluated to gather technical information, including the integrity of the data stored on the system. No effort was made in this analysis to reverse-design, de-compile, or reverse-engineer the compiled binary Dominion Voting System software. Operating system configuration relevant to the operation of the system as well as DBMS configuration was examined. Results relevant to this investigation are documented.

Screenshots are presented that can be used to review and verify these findings and provide step-by-step instructions to reproduce and validate these results. The security of the system has been compromised by the vendor, the Voting System Testing Lab and the Secretary of State's unlawful certification that the system meets all the requirements in law, and exacerbated by false statements that voting systems are safe, secure and have strong integrity. These test results verify the fact. These screenshots were obtained from the mounted forensic images of the EMS server. These results can be reproduced by anyone.

While many of the EMS server settings can be determined from operating system configuration records, it is much easier and far more understandable to view the same information with the Microsoft applications designed for this purpose. The software that serves as the host for the DVS D-Suite voting system applications is the intellectual property of Microsoft, e.g., Windows, SQL Server, and SSMS. The configuration values, or "settings," are determined by the end user, in this case DVS or the Secretary of State of Colorado, but are not proprietary. These are the settings that must be examined, as part of a comprehensive examination, when a voting system is tested for certification.

⁵⁸ The VirtualBox environment provides all of the resources that a server provides, including central processing units (CPUs) and network interfaces. Virtual means that many of the functions normally executed by dedicated computer hardware are instead performed in software, and the interfaces present on the original server are emulated by the host computer's interfaces. None the less, a virtual environment allows us to operate an operating system and application programs *as though* they were running on the actual server hardware.

The security of the entire voting system depends on the totality of all the hardware and software, *combined with* the configuration settings and records of system activity preserved in system log files. Similarly, the security of a home depends not just on having 3 doors and 21 windows, but also whether each of them are locked, as well as whether each of them are monitored on video (equivalently, access being logged) and whether they are each monitored by an alarm system.

The design of the system can be more secure or less secure, inherently, just as a house with 1 door and 1 window is more secure than a house with 10 doors and 20 windows. But voting system testing labs (VSTL) are explicitly required to check and verify these critical settings.

Below are presented screenshots from two different computers used in the testing environment. Each step is explained in detail so that one can easily follow along.

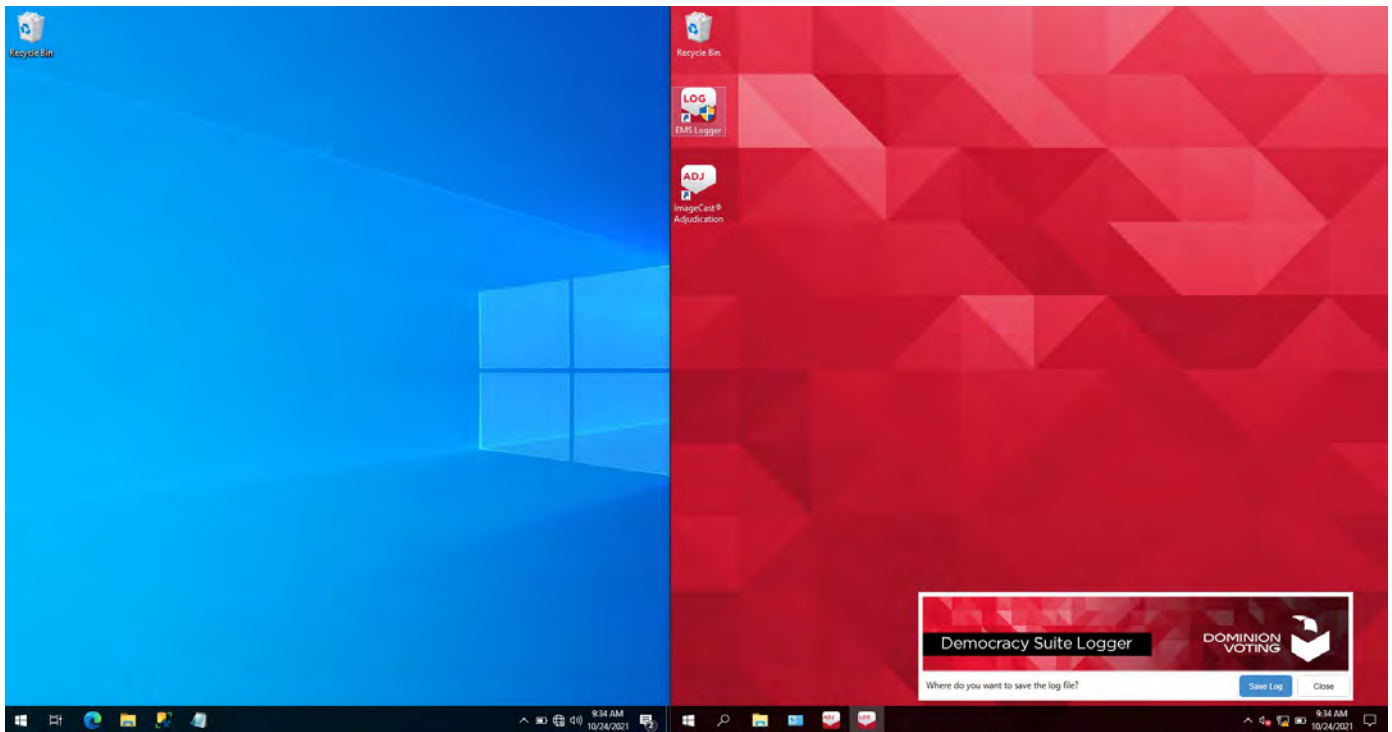


Figure 3 - Test Workstation and Dominion EMS server

On the left side in blue is the Test Workstation running the Microsoft Windows 10 operating system that was used as part of testing. On the right side in red, the emulated Mesa County EMS server, from the EMS Server image, is displayed. The EMS server operating system is Windows Server 2016 and is configured exactly as it was when the image was taken on May 23, 2021. These computers are connected to the same network⁵⁹ for testing.

⁵⁹ The EMS server has its IP address assigned as 192.168.100.10, just as it was while in operation in Mesa County. The Windows 10 computer is also set up on the same 192.168.100.0/24 network just as any device could have been connected at Mesa County. The figures shown in this report are taken from two “virtually” connected virtual environments on a single computer, but the results were verified and duplicated using two different computers and

Both systems are hosted in Oracle VirtualBox virtual environments on an isolated virtual network (emulated within VirtualBox) for the first test – these two computers⁶⁰ are the only computing devices connected to this virtual network.

The tests were repeated a second time using a physical network connection from a stand-alone test workstation with Windows 10 (within a separate Oracle VirtualBox instance, for forensic sterility) connected by Ethernet cable to a Netgear GS108 gigabit network switch, and then to the VirtualBox instance of the Mesa County EMS server's host computer.

This implementation, and testing with a physical network, together, exactly mimics the functionality of the Mesa County EMS server because it is running the exact operating system and application software, identically configured because it is an exact copy created from the integrity-controlled forensic image. Thus, its response and security controls are identical and well-suited for examination in this manner.

The Mesa County EMS network was connected to other components of the EMS D-Suite, but these components neither participate in, nor could prevent the accesses demonstrated in this test (if not compromised and exploited). They are, with respect to the conclusions of these tests, irrelevant, notwithstanding the possible additional data paths to external networks they may offer in either direction.

a physical network and network switch, i.e., the test's connection between the two systems made no difference on the results obtained.

⁶⁰ The reference to "Computers" in this paragraph specifically refers to the operational system comprised of electrical computing devices which perform identical functions and the software installed and configured to operate those devices. For example, an Intel i7 Central Processing Unit (CPU) performs identically on every computer motherboard provided that all of its features are properly included in the electrical design of the motherboard. The main characteristic of a computer is determined by the Operating System, its configuration, and the application software and its configuration. Thus it is entirely appropriate to examine the Operating system, application software and their respective configurations to understand the computer system's operational capability and function. The reference to the software as "computers" is intended to describe the software's purpose, capability and functionality as used in Mesa County as a computer system, not to a specific device.

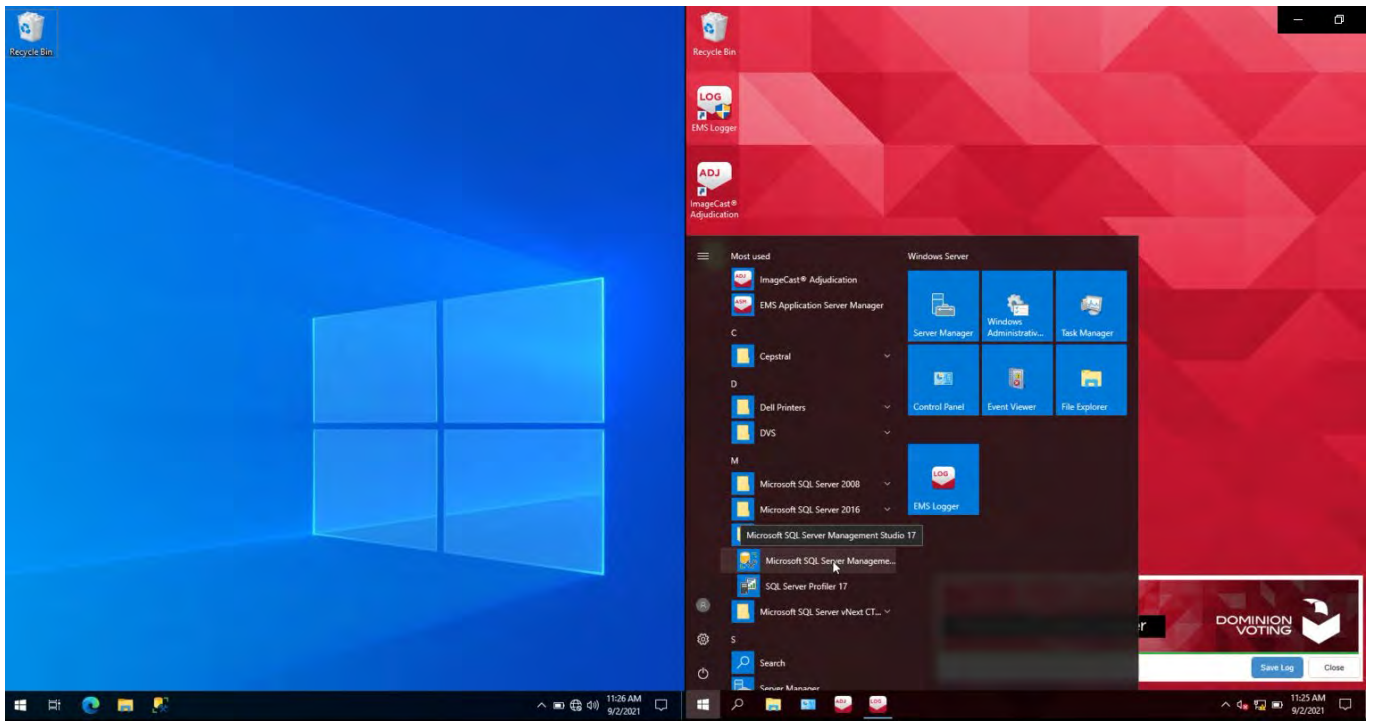


Figure 4 - Installed Microsoft Software

As the Dominion EMS server was examined, the installed Microsoft SSMS software was found listed on the Start Menu.

The presence of SSMS software on the EMS server was unexpected because it enables direct access to the EMS server databases, bypassing the DVS application software. Properly-designed software developed with security in mind would strictly require all database access of any kind (including backup and maintenance) to go through security/tracking/auditing components as part of the design.

The very dangerous side effect of having or allowing Microsoft SSMS software on a voting system is that it can enable surreptitious access to the voting database and is a concern if it is configured to allow such access. Therefore, it is necessary to examine the EMS server's entire software configuration.

Finding 1: The Mesa County EMS system used in the 2020 General Election had Microsoft SQL Server Management Studio 17 installed as configured by Dominion Voting Systems. This software is not listed on the official test report or application for certification. As it was not tested, the unauthorized installation of this software violates and renders illegal the certification of the voting system for use in an election.

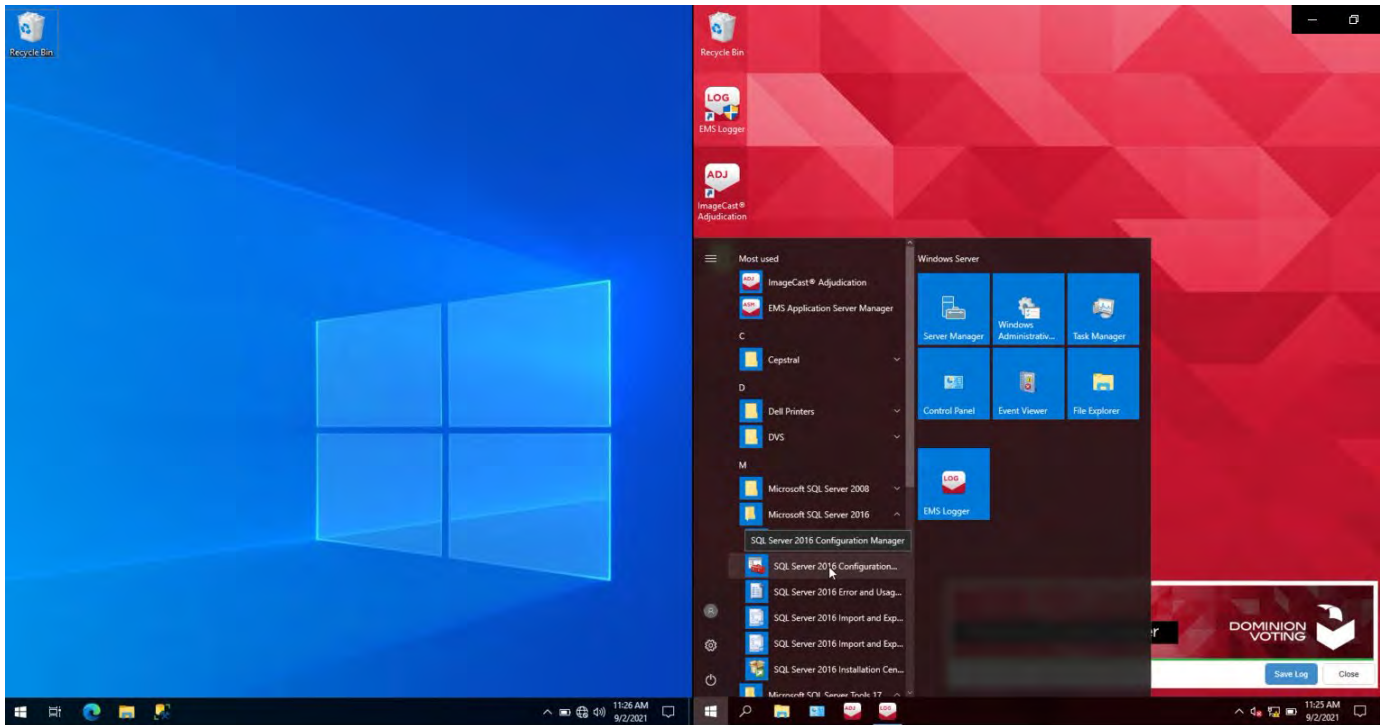


Figure 5 - SQL Server 2016 Configuration Manager

To determine how the SQL Server is configured and whether unfiltered and uncontrolled access is permitted, I examined its configuration through the software application provided by Microsoft entitled “SQL Server 2016 Configuration Manager” as shown in Figure 5.

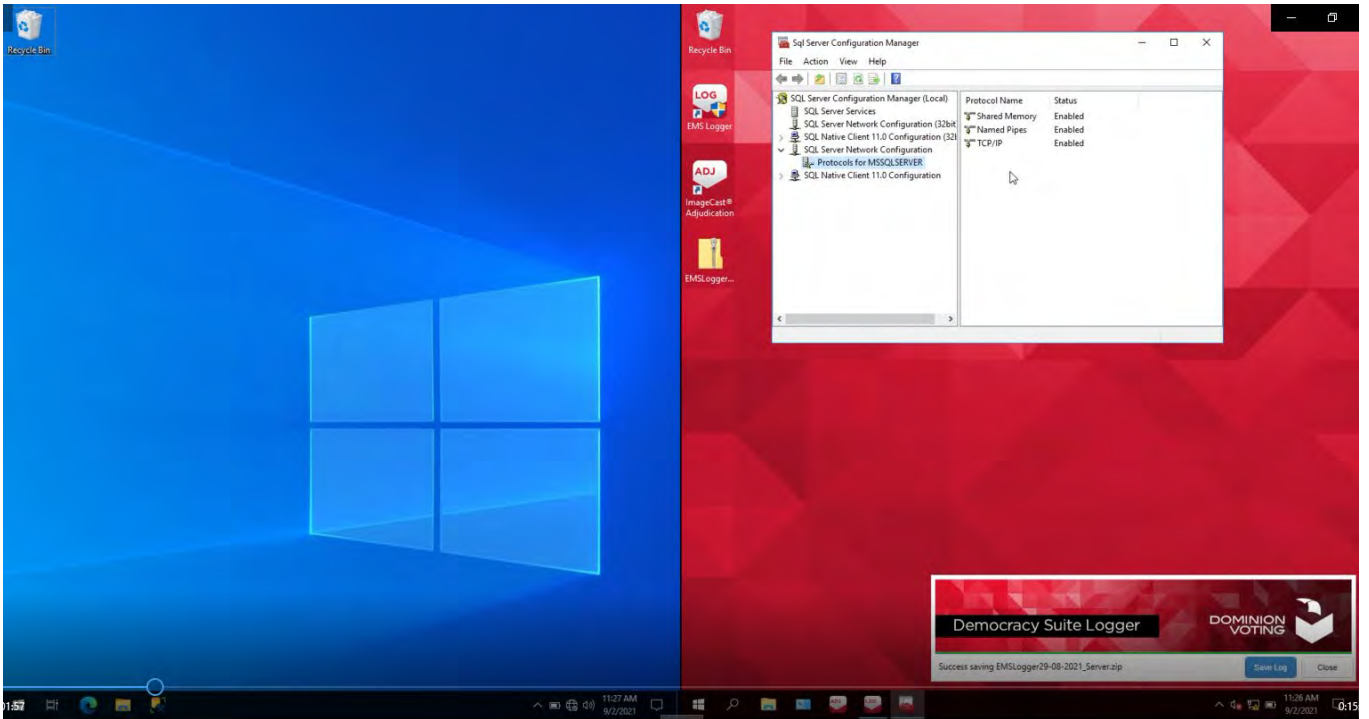


Figure 6 - SQL Server 2016 Configuration Manager – Network Protocols enabled

All three of three possible SQL server protocols were left “Enabled,” providing pathways to the database above what are required for operation. These extra pathways can severely reduce system security.

Under the SQL Server “Network Configuration” the menu item is selected titled “Protocols for MSSQLSERVER” that shows that more protocols are enabled than should be, especially for a “secure” system. While one of these may be necessary, all three being enabled presents an unwarranted risk.

Protocol Name	Status
Shared Memory	Enabled
Named Pipes	Enabled
TCP/IP	Enabled

Microsoft states, in its SQL server documentation⁶¹ that:

“To enhance security, SQL Server disables network connectivity for some new installations. Network connectivity using TCP/IP is not disabled if you are using the Enterprise, Standard, Evaluation, or Workgroup

⁶¹ <https://docs.microsoft.com/en-us/sql/database-engine/configure-windows/default-sql-server-network-protocol-configuration?view=sql-server-ver15>

edition, or if a previous installation of SQL Server is present. For all installations, shared memory protocol is enabled to allow local connections to the server.”

For an election management system, it is entirely inappropriate and irresponsible to enable Shared Memory or TCP/IP access over an unsecured network connection, and particularly careless and irresponsible to enable these together with “Named Pipes.” Shared Memory access permits an intruder to install malicious software and to execute arbitrary commands with full administrative privileges if exploited. Given the exceptionally minimal protection implemented on this server, if any connection were made to a network that provides a path to the Internet⁶² by the EMS system, any other computer connected to the Ethernet network would be granted access to the TCP/IP ports⁶³ enabled by the EMS server and a hostile party would be able to penetrate and alter the EMS server.⁶⁴ In the examined state of the EMS server, if this network *or any computer connected to this network* were connected to the internet either directly or indirectly, by wire or wireless, a hostile party *anywhere in the world* would be able to penetrate and alter the EMS server, including altering actual election records, like tabulated vote databases.

A computer system configured in this manner should never be used in any critical infrastructure or high security environment and, as a voting system, should be immediately decertified and those responsible for creating and selling such system investigated.

While multiple security mechanisms exist within a Microsoft Windows 2016 server, including the Microsoft Windows Defender firewall, SQL database permission restrictions, Operating System security Policy, Group Security Policy, file access control lists, and much more,⁶⁵ some were configured not to protect the server but instead to allow all “local” and “remote” access. Tests conducted in this examination demonstrate that not only are those explicit programmed settings misconfigured, but that no other security mechanisms within the installed hardware and software prevented the ability to access and change election data, or even to provide any warning of such drastic and consequential access.

⁶² Given the exceptionally large number of wireless devices in this election infrastructure (thirty-six), particularly in the context of the plethora of improper security configuration mistakes made in this installation, examination of every device in the infrastructure including the wireless printer must be undertaken before the network can be considered secure; absent appropriate systems log data, such a determination might not be possible.

⁶³ TCP/IP networks identify computer systems by their IP (Internet Protocol) address. TCP/IP further identifies the specific service (email, file transfer, database access, etc.) to be used on the destination computer using a port number transmitted within the beginning of the packet (in its header). Standards identify the assignment of port numbers to specific services, for example, web browsing uses port 80, encrypted web browsing uses port 443, email uses port 25, and database access using the Structured Query Language (SQL) uses port 1433. There are 65,536 available port numbers. Ports 0 through 1,023 are assigned to commonly used services/protocols, 1,024 through 49,151 are sometimes registered to a specific service, and those remaining are available for dynamic use (e.g., as needed). One can conceptually think of these ports in the same way we think of channels on cable TV – each is associated with specific content.

⁶⁴ For example, see CVE 2018-8273, CVE 2021-1656, CVE 2020-0618 at <http://cve.mitre.org> and Microsoft Knowledgebase KB 4073225 regarding the “Meltdown” and “Spectre” vulnerabilities presented by the “management engine” back door in every CPU manufactured since 2007 whether Intel, AMD or ARM processors.

⁶⁵ See the US Department of Defense Security Technology Implementation Guides (STIGs), at <http://public.cyber.mil>

There is a great misunderstanding about intrusion into computer systems. Many people conceive of it as depicted by Hollywood, where an intrusion takes several minutes or significantly longer. While this makes for good drama, it is not realistic at all. In the real world, malicious actors – particularly hostile nation-states, e.g., China, Russia, North Korea and Iran to name a few, have extremely sophisticated cyberwar capabilities. They are capable of intruding and *altering data* in a matter of less than a few seconds and they engage in persistent cyber operations to penetrate and compromise supply chain, industrial base, trusted vendors, academia, and government offices which might someday afford access.

Intrusion can be accomplished without a direct connection to the target computer. In the case of a voting system, using the example of an Adjudication Workstation connected via wired Ethernet to the EMS, if the Adjudication workstation has a wireless (Wi-Fi) interface, such a connection might be automatically connected to external devices and networks without the EMS or Adjudication workstation operator ever noticing it, especially since all laptops today have both wired Ethernet and Wi-Fi interfaces which might enable an Island-Hopping attack. Thirty-six (36) wireless devices were identified in the Mesa County DVS D-Suite system (e.g., on the DVS D-Suite ICVA computers and ICX tablets and one Dell E310DW wireless printer, with IP address 192.168.100.11, set as the default printer on the EMS server). Any other connected device, including a printer like the one installed on the Mesa EMS infrastructure,⁶⁶ creates an increase in this risk exposure. This is why an Internet connection in any device or computer, even several connections removed, is so extremely dangerous to critical systems. To mitigate this risk, the US Department of Defense (DoD) maintains special closed networks for sensitive information, which are forbidden to have internet connections or connection to any system with an internet connection.

Appendix D lists some of the more notable nation-state cyber-attacks as well as a link to an online video of one cyberattack that completely destroyed a power generation facility. Adversaries constantly scan and probe every computer on the internet, and through those computers, other devices and computers not directly connected to the internet, to identify weakness well in advance of the need for an attack. Today's attacks occur very quickly, in a matter of seconds.

⁶⁶ At Bell Laboratories in the 1980's, printers that used the Postscript language were exploited (to leverage their computational power) in this manner because they were the first to have a bi-directional communication connection (e.g., able to talk back to the host computer, over a network). Today's printers all have this capability and present a risk of being a component of an Island-Hopping attack.

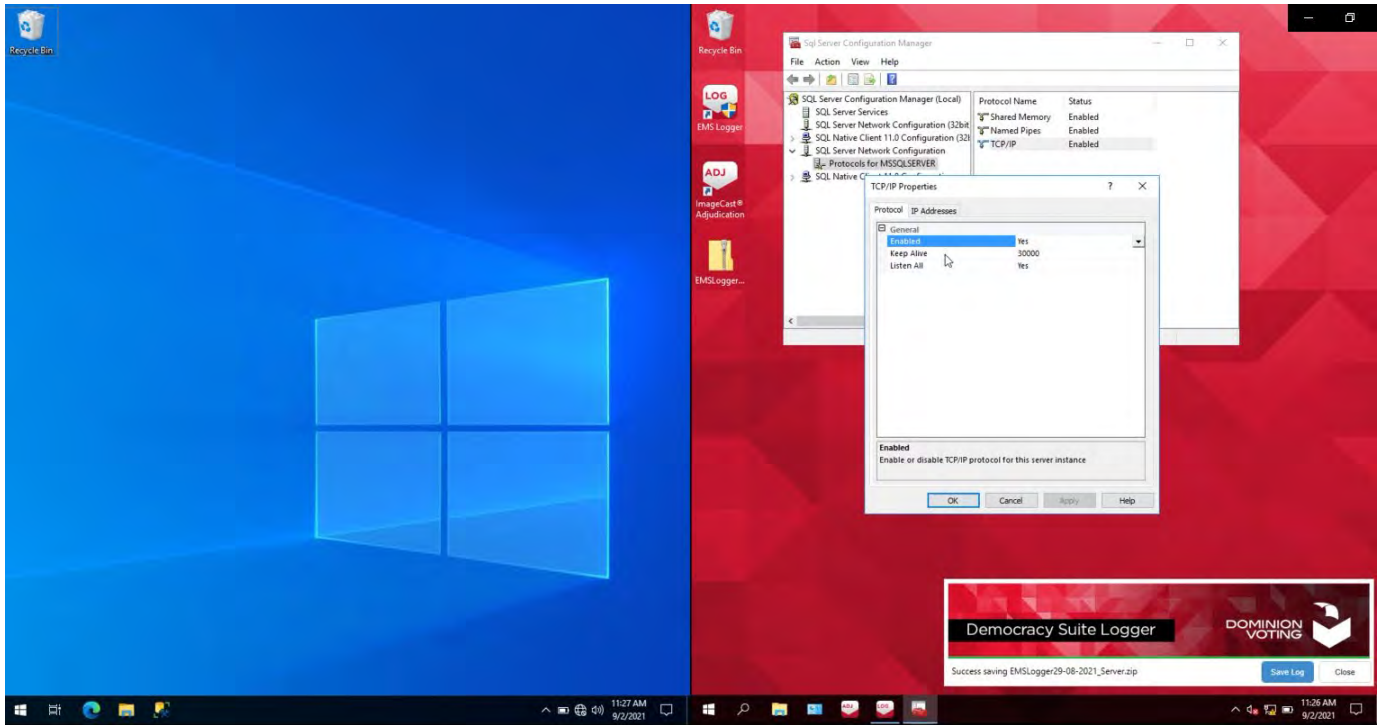


Figure 7 - TCP/IP Properties

The TCP/IP protocol setting in Figure 7 has “Enabled” set to “Yes” on Mesa County’s EMS Server, and the configuration setting above has the parameter “Listen All” set to “yes” indicating that the SQL Server will listen on every network connection. More detail for the TCP/IP protocol is in Figure 8.

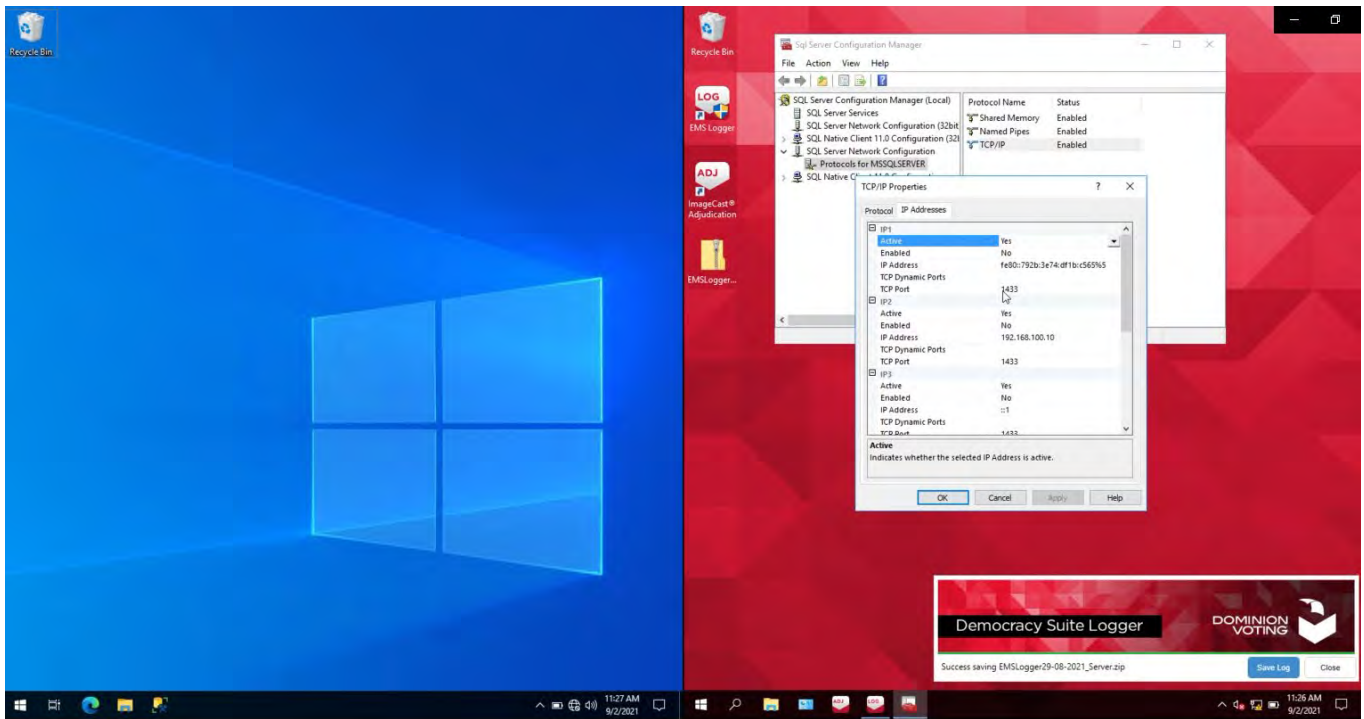


Figure 8 - TCP/IP Properties of SQL Server, attached to port 1433 the standard (default) port.

Figure 8 shows the SQL server is bound to and active on all Ethernet interfaces. This allows multiple electronic pathways to the server over multiple network connections should someone connect a cable into that jack. Also important to note is the default port number 1433 being used, instead of a more secure alternate port.

IP2 shows the IPv4 address 192.168.100.10, an IP address assigned to be used by the Mesa County EMS server. For a discussion of IP addressing fundamentals, see Appendix C. IP Addressing Fundamentals.

The Mesa County EMS server is a Dell PowerEdge T630 server, serial number 4NV1V52, and has 3 Ethernet interfaces (or Network Interface Cards (NICs)) – 2 of them assigned to the computer itself and one assigned to a separate controller (the iDRAC, Integrated Dell Remote Access Controller) which can be used to allow remote control of the computer including power-on, power-off and privileged access to the computer, via this integrated remote access controller (iDRAC). The interfaces accessed via the Server Configuration Manager (shown in these Figures) are those IP addresses assigned to the computer and do not include the interface assigned to the iDRAC.

A conclusive determination that these IP addresses had a connection to another network, even the Internet, is not possible without examining the physical system, as well every other device connected to the network. Most network firewall/router devices use translation (network address translation, NAT, or port address translation, PAT) and most computers/devices with multiple network interfaces (Wi-Fi, and wired Ethernet, for example) can be compromised to implement an Island-Hopping attack (using malicious software that provides translation, even though standards may prohibit it).

Absent a full forensic examination of all network and computing devices, it can be challenging to factually conclude that connection to the global Internet was, or was not, present and in operation. Given that network systems are designed to support Internet connectivity, other evidence (including the alteration,

addition or exclusion of votes, or data in log files, for example – See Report #1) must be considered, may be the only artifacts that enable detection or conclusive determination, and may indicate a probability that such a connection may have been in use.

I was told that when this exact copy (forensic image) of the Mesa County EMS server was taken, the Mesa County EMS server was connected to a (wired) computer network via its Ethernet interface. Configuration data forensically extracted from the EMS server, including some log remnants and registry configuration data validate this information about the connection to a network.

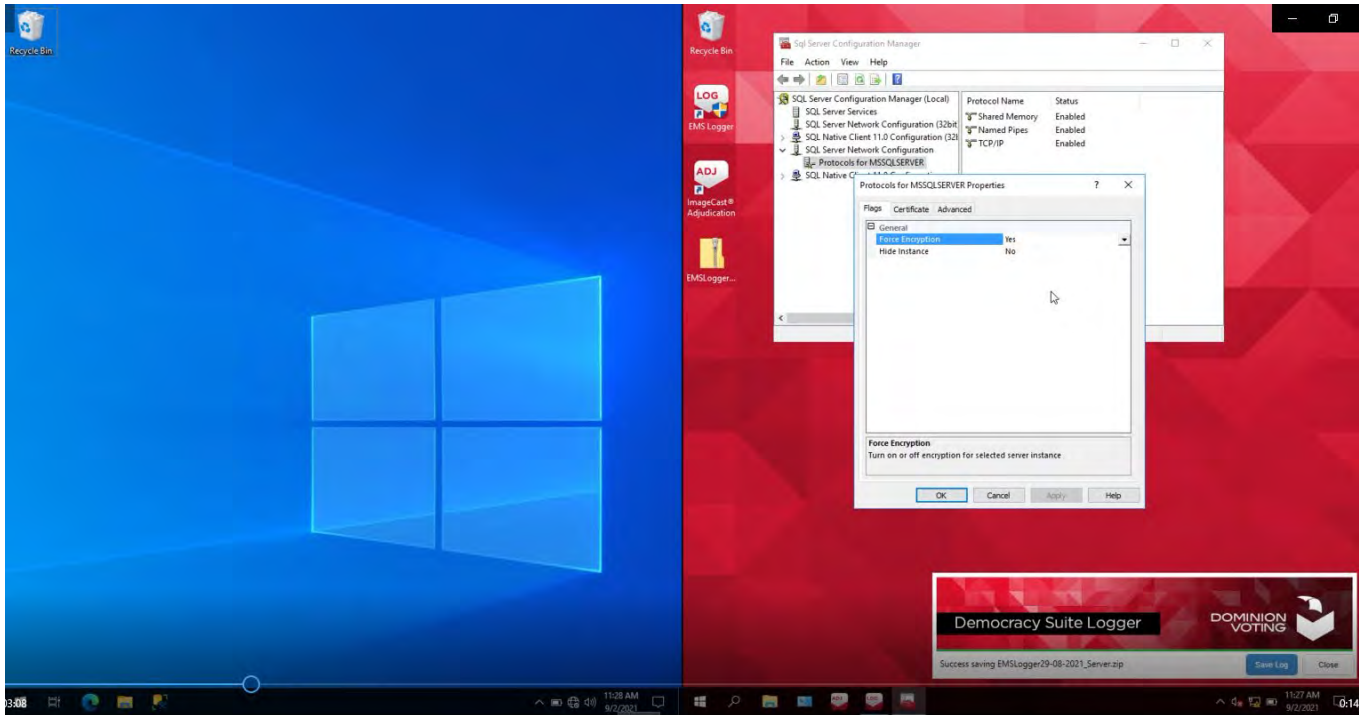


Figure 9 - SQL Server Properties

The SQL Server service is configured to force network communication to be encrypted. This is an expected configuration; however, it is crippled by what was found next.

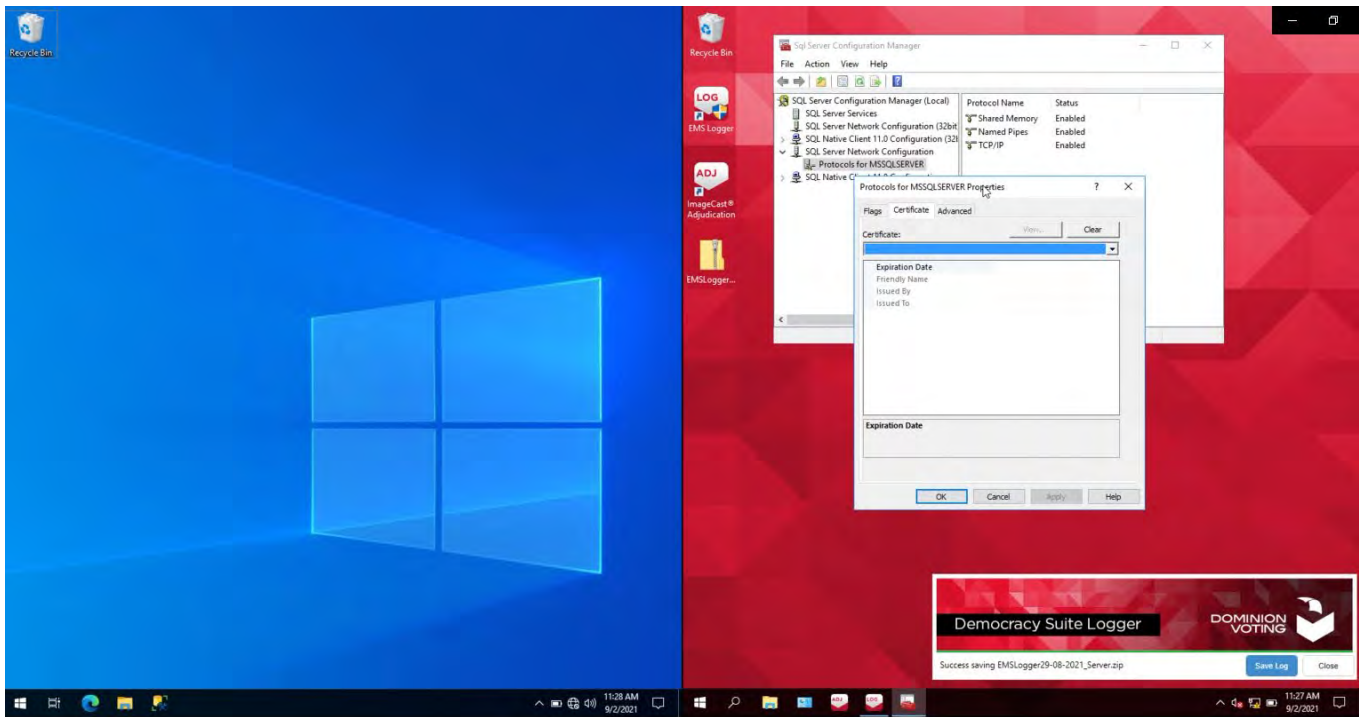


Figure 10 - Encryption is enabled but No Encryption Certificate is configured

No encryption certificate is configured, which causes the server to use a 'self-signed' certificate that is extremely vulnerable to a common man-in-the-middle attack. This means that the communication to and from the voting database itself could be intercepted, viewed, and changed, without detection.

A man-in-the-middle attack is explained in Appendix H.

The SQL Server Documentation directly provided by Microsoft clearly states “Self-signed certificates do not guarantee security. The encrypted handshake is based on NT LAN Manager (NTLM). It is highly recommended that you provision a verifiable certificate on SQL Server for secure connectivity. Transport Security Layer (TLS) can be made secure only with certificate validation.” (<https://docs.microsoft.com/en-us/sql/relational-databases/native-client/features/using-encryption-without-validation?view=sql-server-2016>)

EXAMINATION OBJECTIVE 1:

Determine whether calculated vote totals can be altered by anyone with physical access to the logged-in EMS server.

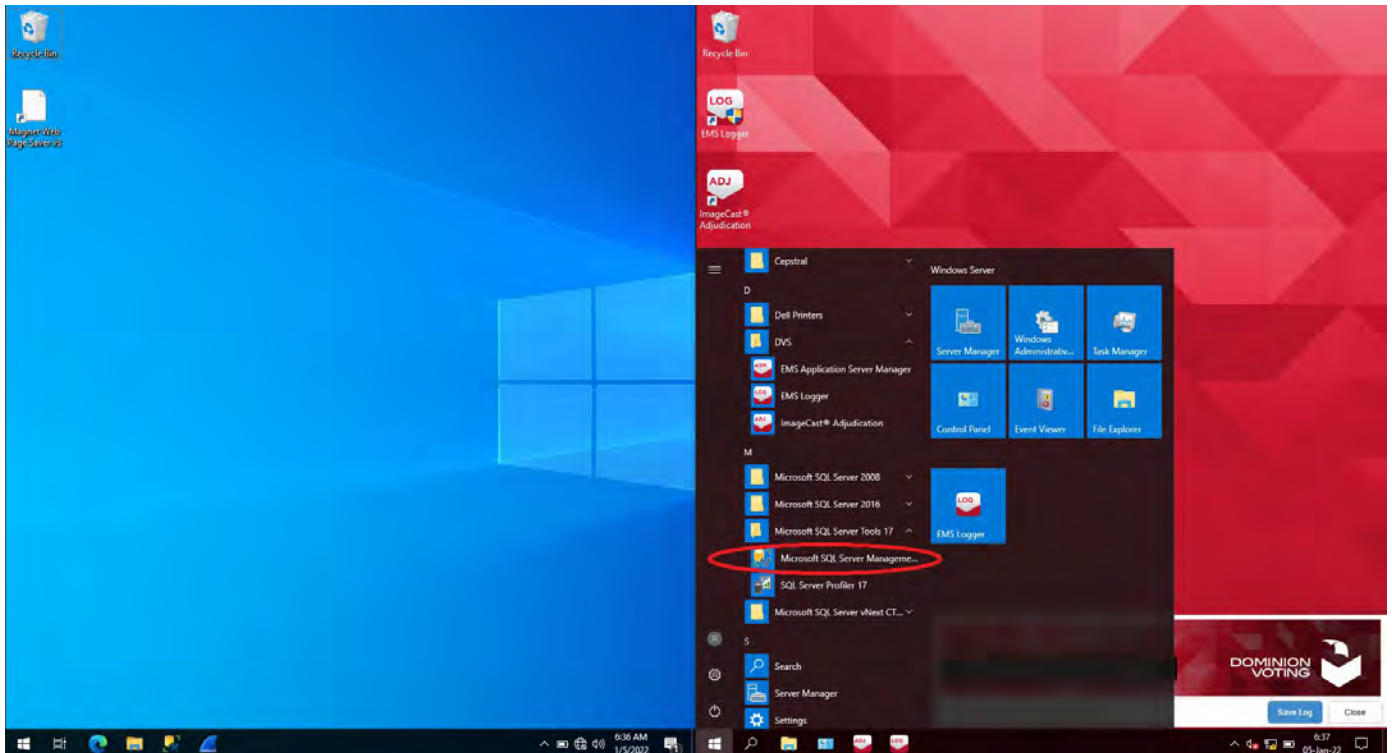


Figure 11 - SQL Server Management Studio (SSMS) software showing in the EMS server Start Menu

Microsoft SQL Server Management Studio (SSMS) allows direct back-end access to and manipulation of SQL Server databases. Figure 12 shows this software is found already installed on the EMS Server.

The VSS explicitly prohibits voting systems from allowing any users to change calculated vote totals, or an individual vote, or to compromise ballot security; the VSS also mandates the retention of all audit trails for 22 months specifically to enable detection of civil rights violations or intentional manipulation and fraud, and to support litigation and prosecution. SSMS enables that prohibited ability, as demonstrated in this test.

The Mesa County EMS was protected by only a (Windows authentication) password, as this test demonstrates. The use of a password alone is not secure; this fact is taught routinely in training for the board certification “Certified Internet Systems Security Professional” (CISSP), emphasizing the principle of “Defense in Depth,” e.g., multiple layers of security.

Passwords are compromised often.⁶⁷ As early as 1985, the US Government published, in its “rainbow series” of security publications from the DoD, the “Green book⁶⁸” guide to password management. While the password management recommendations in the guide are considered obsolete today, its appendices explain the mathematical calculation for the probability that a password can be guessed based on the complexity of the password, how often the password is changed, and the speed with which a computer can execute those guesses. Today’s computer processor execution speed (CPU clock rate) is 5,000 times faster than computers were in 1985. Today’s gaming home computers are 5 times faster than the fastest computer in the world was in 1985,⁶⁹ and systems used for crypto-mining may be as much as 100 times faster than that fastest 1985 computer.

Password insecurity alone presents an extreme and unacceptable risk.

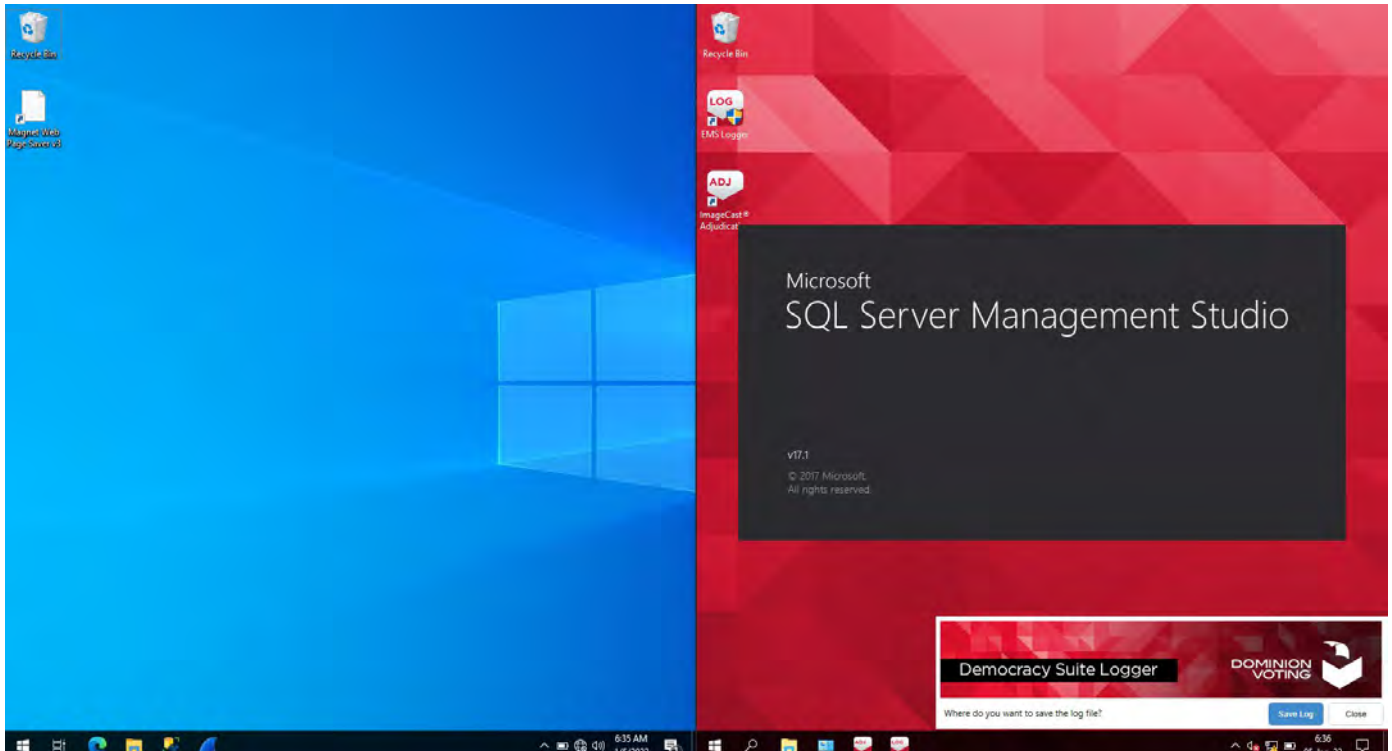


Figure 12 - SSMS is installed and starting on the EMS server system.

The SSMS starts up without any problem or warning when a user clicks on it.

⁶⁷ Accounts in public media support this fact. These are only several of many such references:

<https://www.westernjournal.com/az-audit-exclusive-election-systems-password-hasnt-changed-2-years-shared-time/> and <https://www.csoonline.com/article/3266607/1-4b-stolen-passwords-are-free-for-the-taking-what-we-know-now.html>

⁶⁸ <https://csrc.nist.gov/CSRC/media/Publications/white-paper/1985/12/26/dod-rainbow-series/final/documents/std002.txt>

⁶⁹ A Cray X/MP supercomputer operated at a clock speed of 1 GHz, or 1 billion clock cycles per second in 1985, while the first home PC clock speed was typically 1MHz.

Not only can SSMS be used on a separate computer, not part of the DVS system, to directly access the back-end server databases, it can be used directly by any person with physical access to the logged in server itself (screen, keyboard, and mouse), such as rogue election staff, cleaning staff, etc.

In addition to bad-actors from outside the election staff, any individual election staff worker that has access to a logged-in EMS server also is allowed the ability to go directly into the back-end of the database and add votes, change votes, delete votes, swap votes, and countless other alterations, bypassing all DVS application software. Even an honest individual could accidentally allow data to be changed without their knowledge in a matter of seconds by innocently attaching a USB flash drive with hidden programming/malware on it.

Anyone with unrestricted physical access and knowledge of the userID can make similar changes without even a password, if the standard user account is left logged-in. Someone with advanced security knowledge can access the system without a password, as I was easily able to do.

In this test the Microsoft SQL Server Management Studio is used to demonstrate unauthorized access to the election databases. However, the use of Microsoft SSMS is not even required – a popular piece of software manufactured by SQL Pro (e.g., non-Microsoft software) is shown in the third test in this report, to provide the same access from the more limited computing power of a mobile phone.

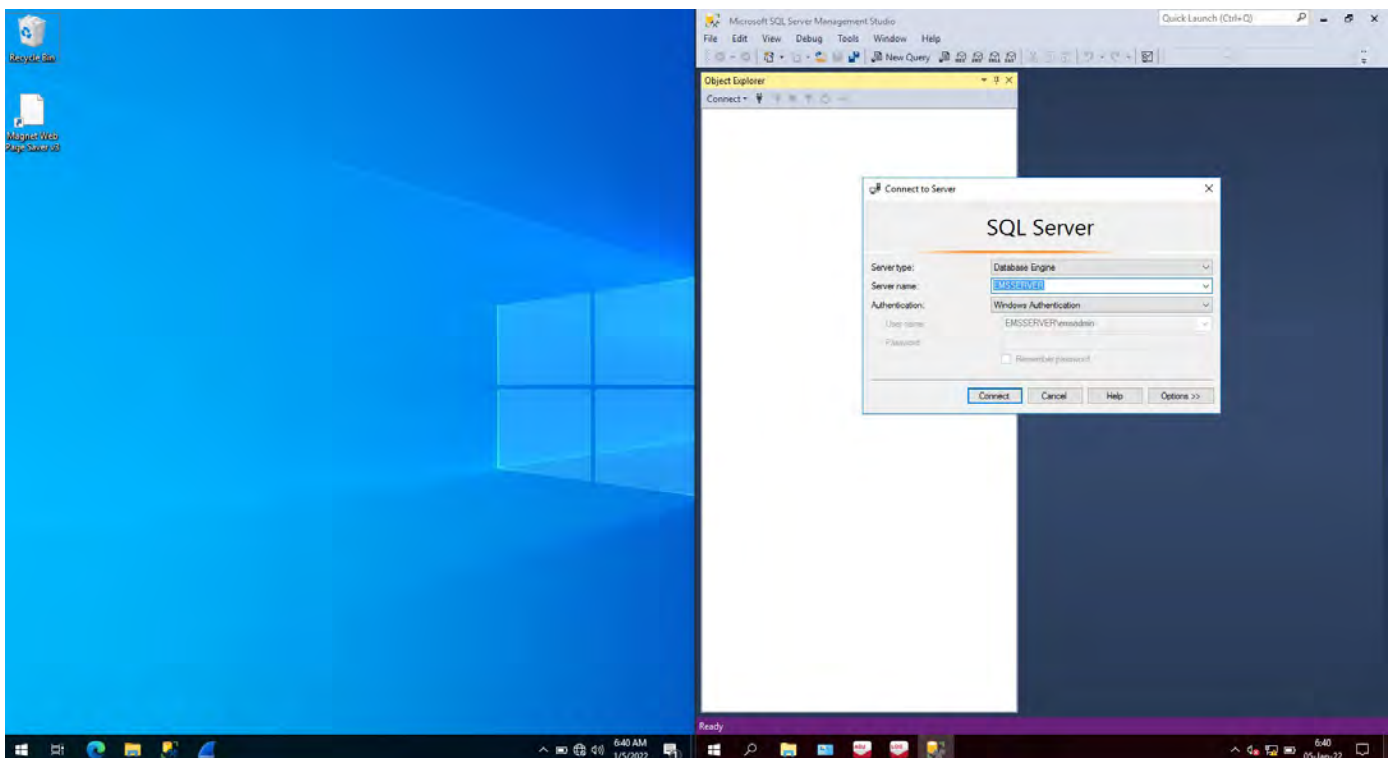


Figure 13 - Logging in to the SQL Server using SQL Server Management Studio

When SQL Server Management Studio (SSMS) first starts, connection entries are already pre-filled-out. The user doesn't need to type a username or password, and needs only to click the 'Connect' button to get into the back-end databases.

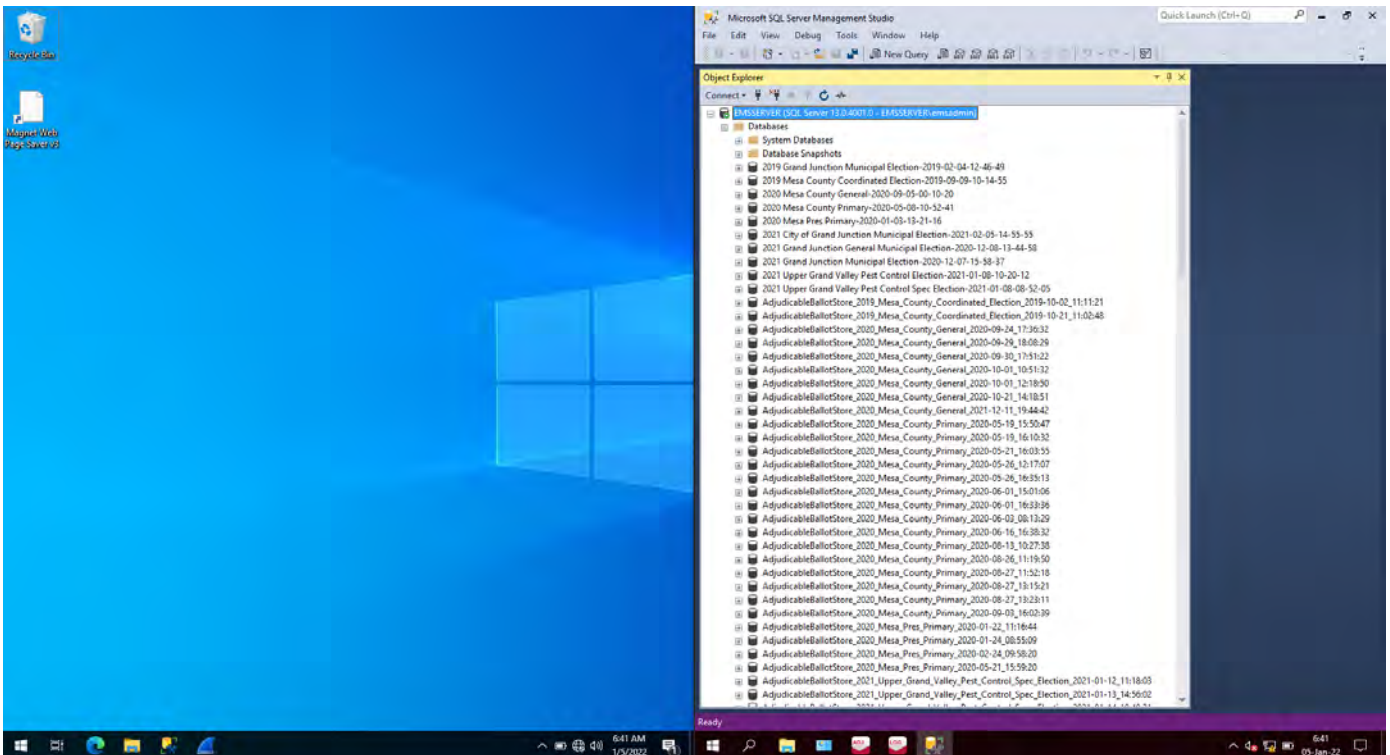


Figure 14 - SSMS enables direct access to the internal databases to anyone logged in to the EMS server

After clicking 'Connect,' and then the '+' sign next to 'Databases' all the internal databases are shown to be accessible. It took only four clicks of the mouse to get here into the back-end of the voting databases.

One of the many election databases that are shown is from the 2020 US General Election. The US Presidential Primary of 2020, among many others, can also be seen.

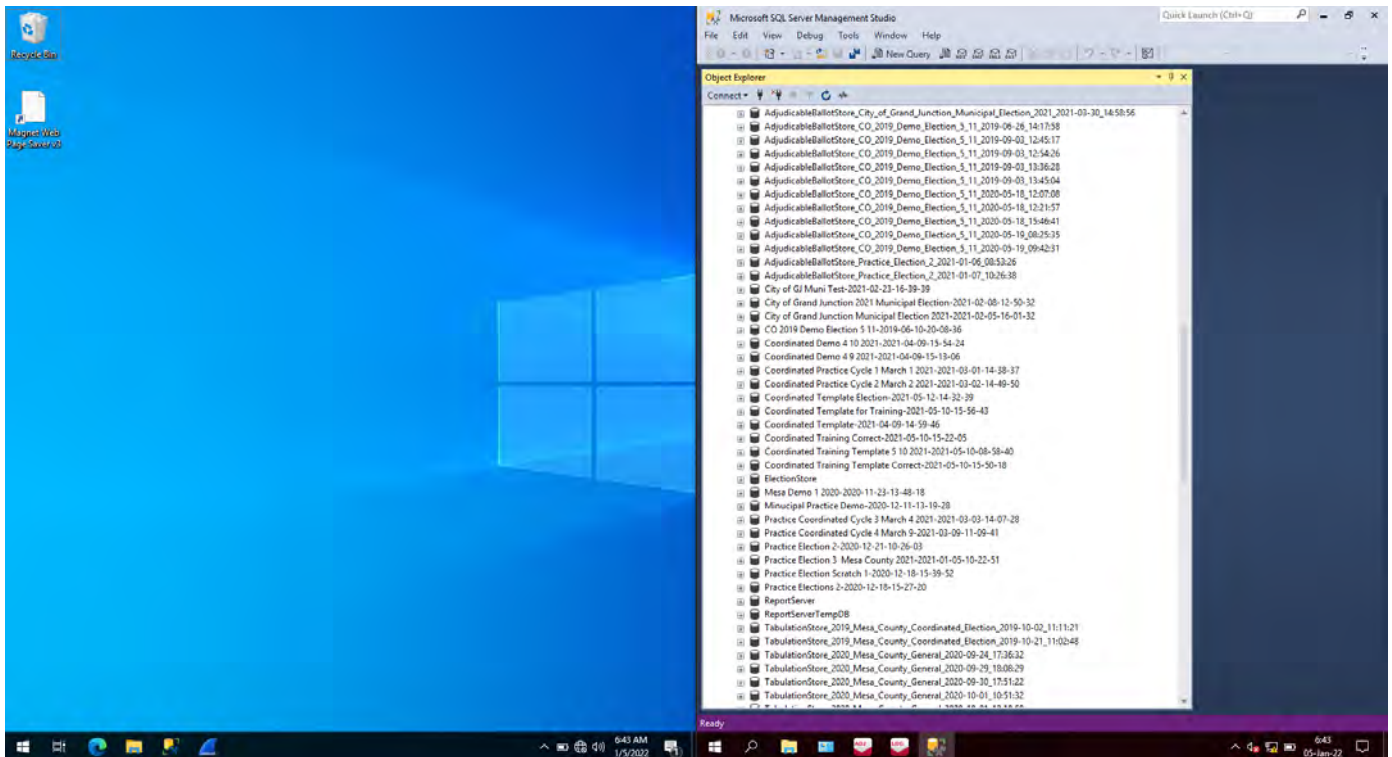


Figure 15 - Databases from many prior elections are fully accessible

Here can be seen accessible many elections from the City of Grand Junction, Mesa County, as well as adjudication and tabulation databases from many of these elections.

The presence of databases from previous elections on the EMS server, provide a rich library of information that can be used to understand and identify potential vulnerabilities in the EMS. While these records are required to be retained, they should be maintained off- system, securely archived, inaccessible to the EMS or any user.

The presence of prior election databases on the EMS server also offers an extensive and convenient repository for copy and paste modifications of election data, not only for the 2020 election but for any prior listed election as well.

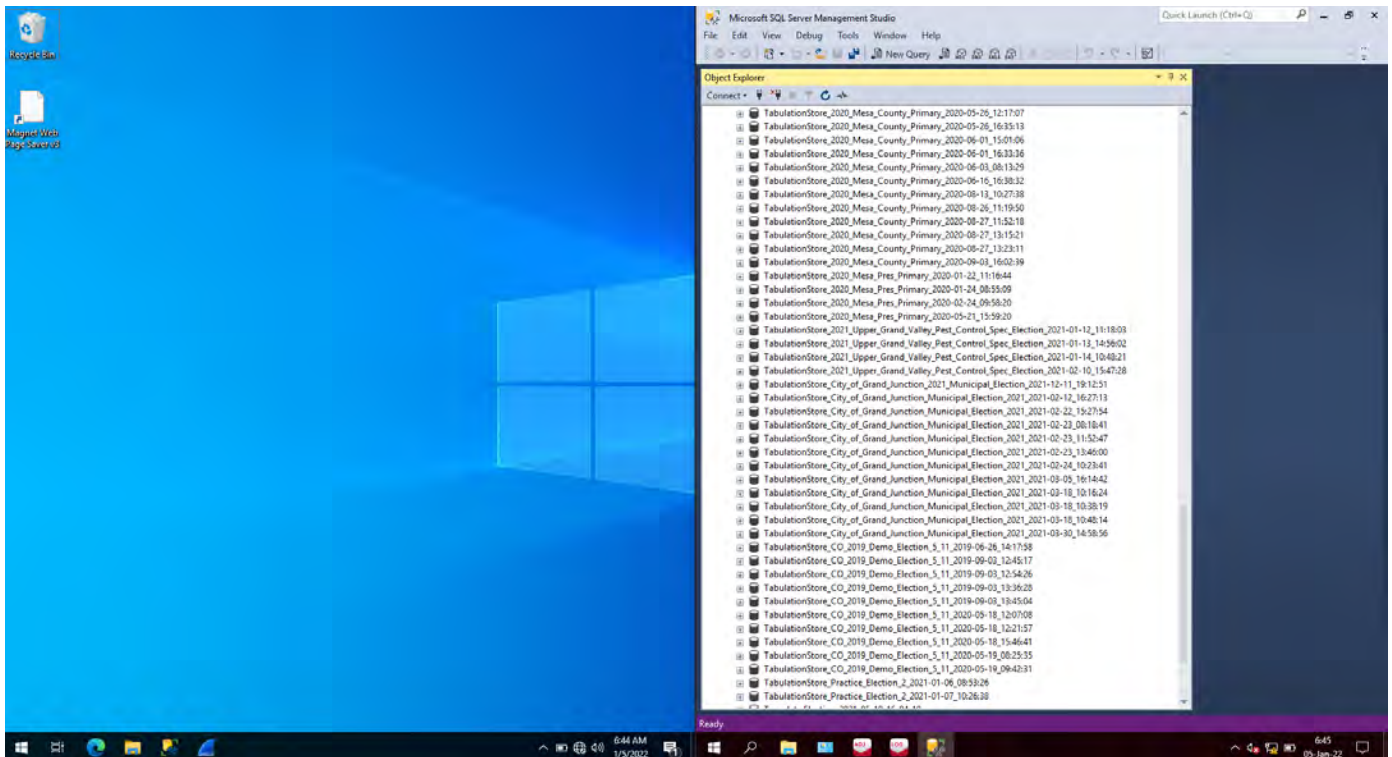


Figure 16 - Additional databases used in previous elections

Many TabulationStore databases are shown here, including even a TabulationStore for the Upper Grand Valley Pest Control Special Election.

Figure 16 is a continuation of the list in Figure 15, demonstrating that far more than one screen of databases are accessible.

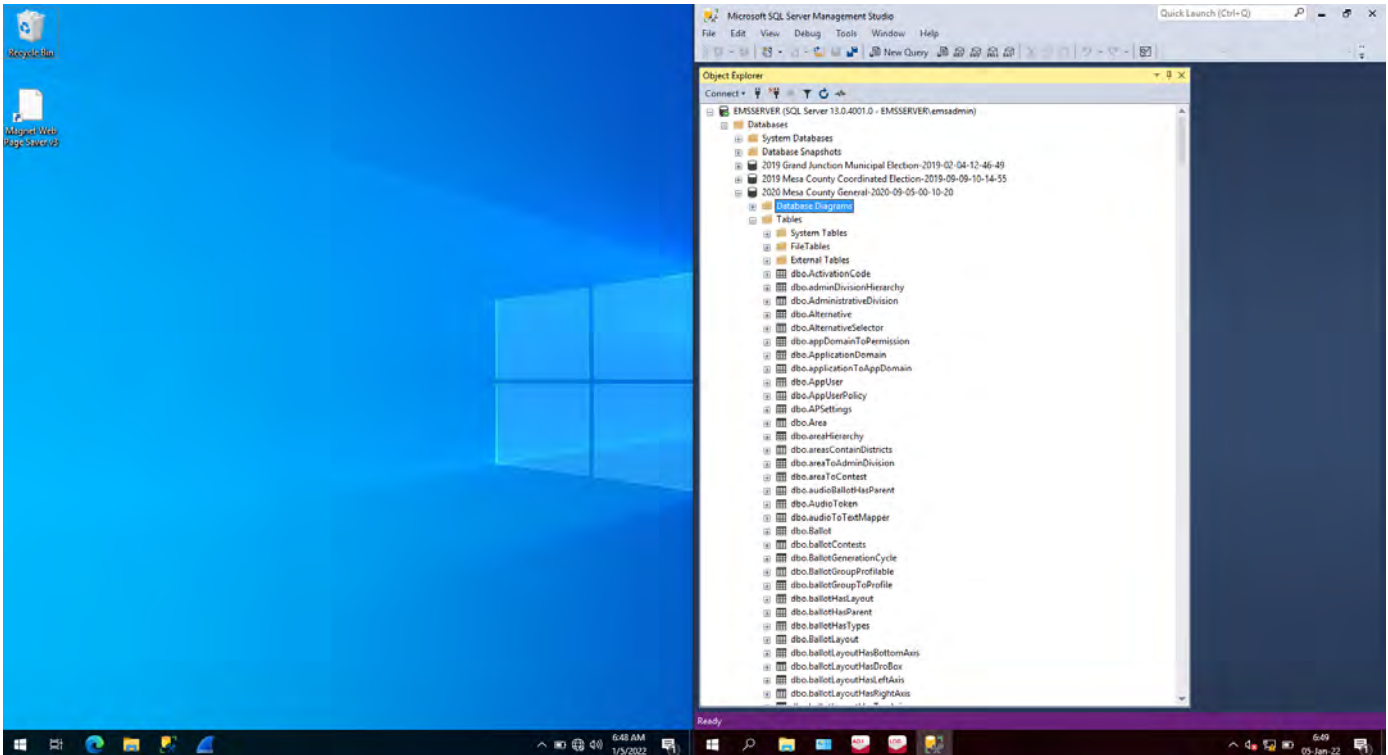


Figure 17 - Internal database tables, including ones with counted votes are accessible

The '+' sign next to the 2020 Mesa County General database was selected, followed by the '+' sign next to 'Tables.' A list of all internal database tables for the 2020 Mesa County General database is now shown. Nothing has stopped me from accessing this. Not a single warning has shown on screen.

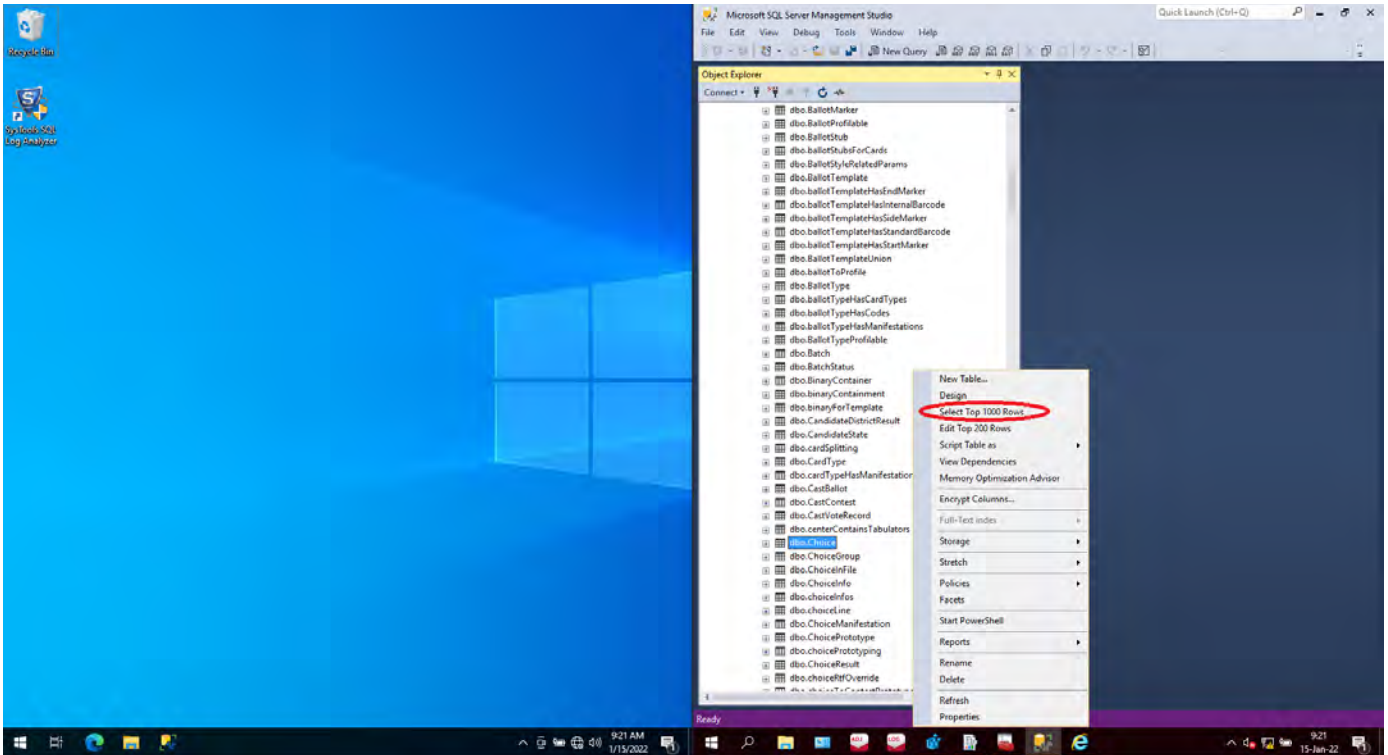


Figure 18 - Menu Option to Select the Top 1000 rows

As an example, one of the tables, 'dbo.Choice,' was selected by scrolling down and right-clicking, then choosing 'Select Top 1000 Rows' by clicking on that option. This instructs the database server to show me the top 1000 rows in the database table.

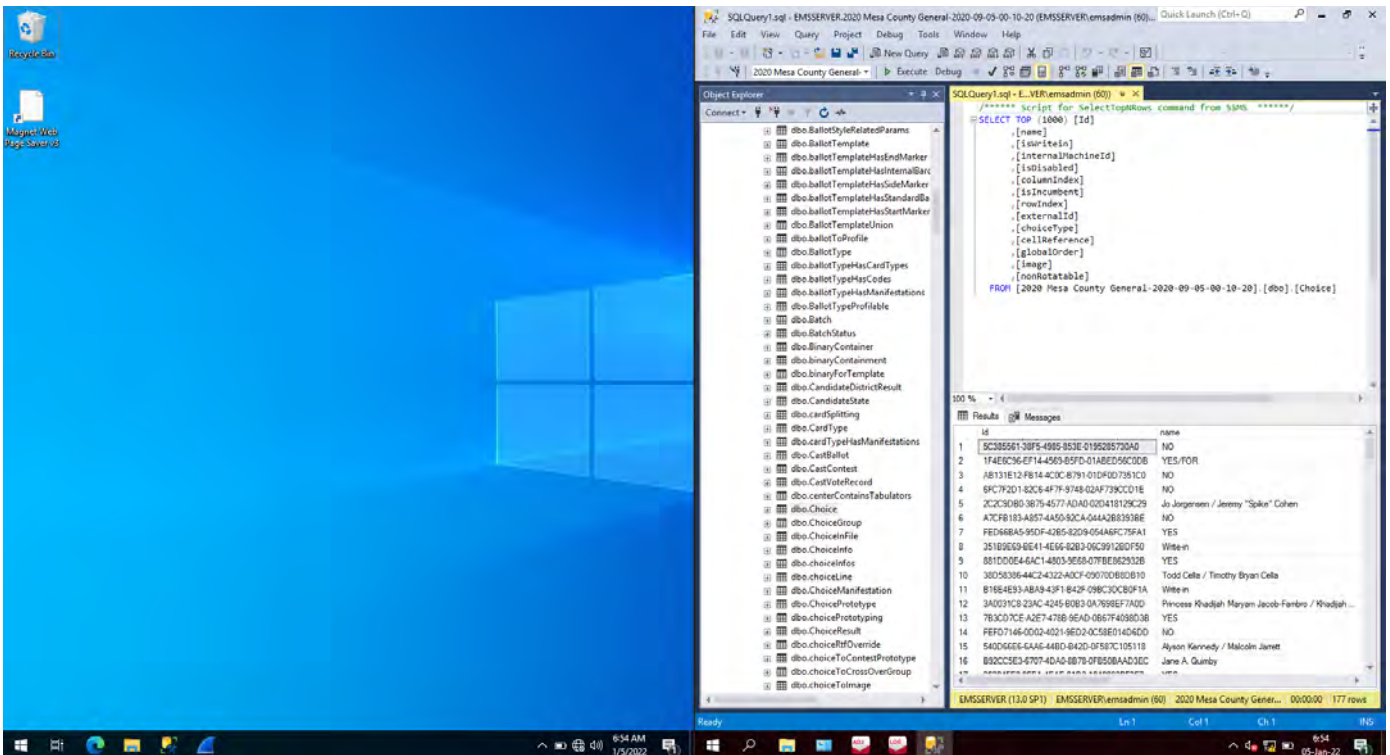


Figure 19 - Accessing the Ballot Choice database table

I was able to easily open the Ballot Choice database table. The computer retrieved all 177 rows of data from this table in the database. This corresponds to 177 different ballot choices in the election. I have still not been blocked, nor has the system provided any warning that anyone is directly accessing the voting database.

Each election “contest” is defined, together with candidates and the rules for voting, e.g., “pick one, pick two, pick three, etc.,” depending on the specific item, for example, commissioners of a town, and the number of seats open in this specific election.

On the right side of the screen in the upper right pane is displayed the SQL Query (SQL program script) that is automatically filled-out by SSMS. The user merely just needs to know how to click the mouse button. The automated query shown is used to retrieve data (the top 1000 rows), and the data columns listed that will be retrieved are also shown. On the bottom right pane the response from the request is shown. The first two columns display on screen (‘Id’ and ‘name’) but the scroll bar allows one to scroll to the right to see the remaining 12 columns.

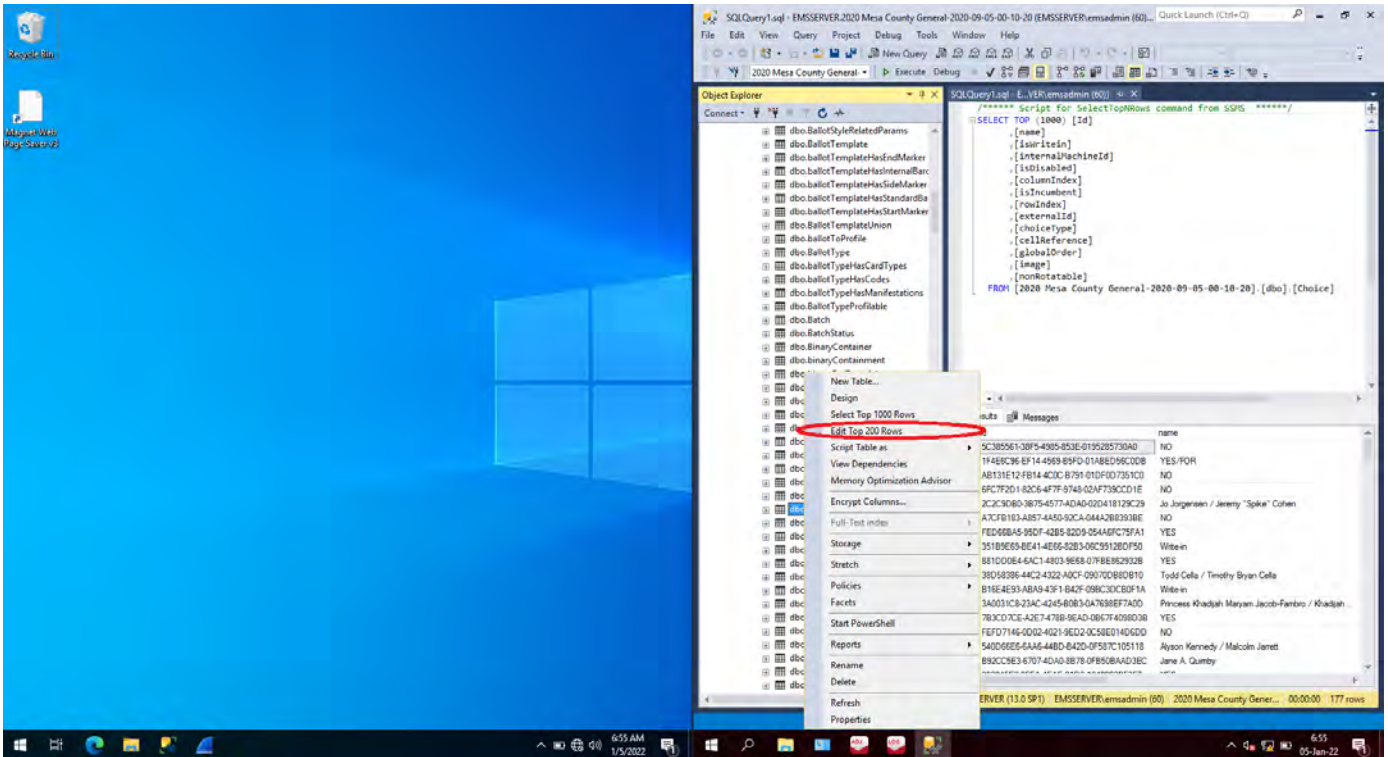


Figure 20 - Test to determine if the Ballot Choice Table can be edited to easily flip the votes

I now right-click the table again and select the menu option to Edit the Top 200 rows of the database to determine if it will also allow me to directly alter the data.

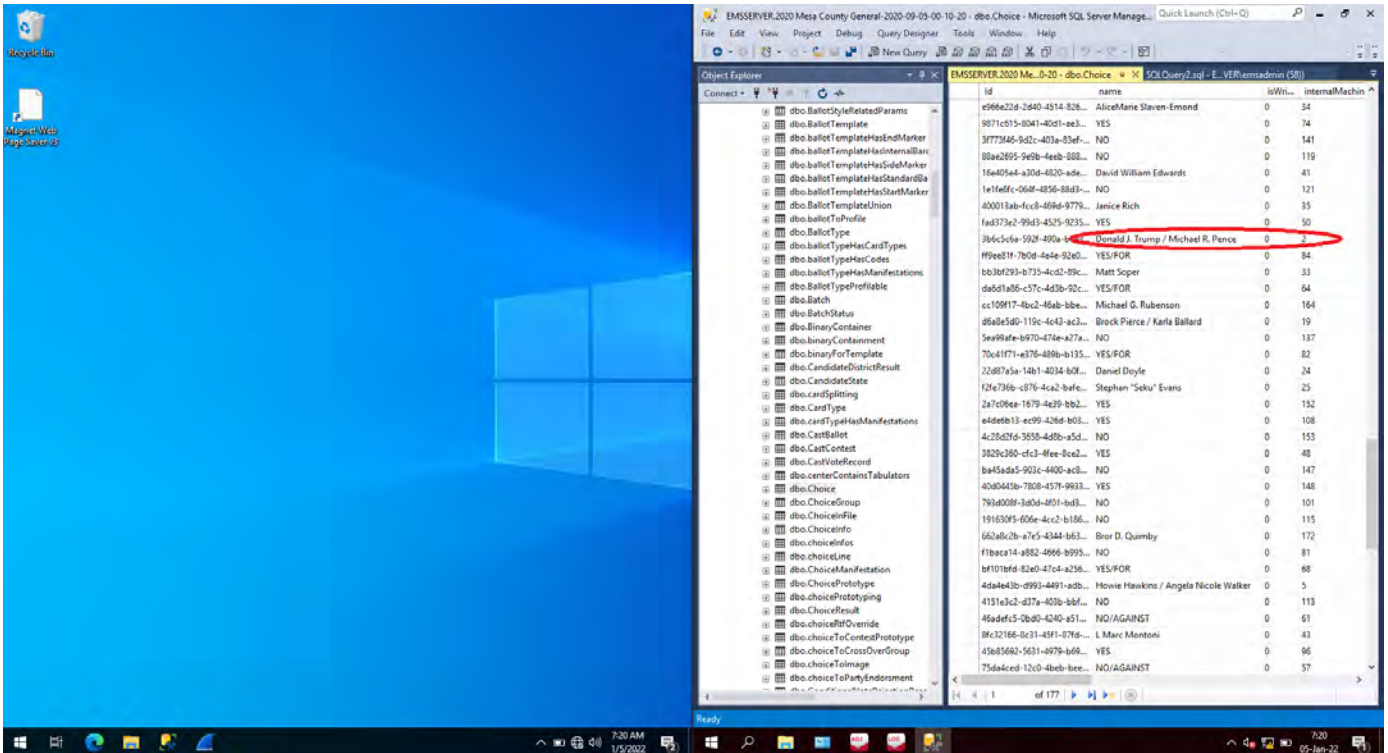


Figure 21 - Candidate settings for Trump

The computer responds to the request and shows all 177 rows of this Choice table in a spreadsheet-like display. Note here that the Choice 'Donald J. Trump / Michael R. Pence' has an internalMachineld of '2'.

Note the first four columns are:

- Id – A unique identifier to identify the particular choice.
- Name – The 'title' of the choice on the ballot.
- isWritein – Possibly used to signify if a particular choice is a write-in field.
- internalMachineld – Another unique identifier to identify a particular choice used to produce reports.

The internalMachineld parameter is an indirect reference to the counted vote for candidates. Because the reference is indirect (i.e., a number rather than a key index that is common to the candidate's identity throughout the database), the reference can be easily changed, flipping the vote, and is extraordinarily difficult to identify. In database design, this is an example of bad design practice that breaks the "referential integrity" of the database and enables the potentially malicious action demonstrated here.

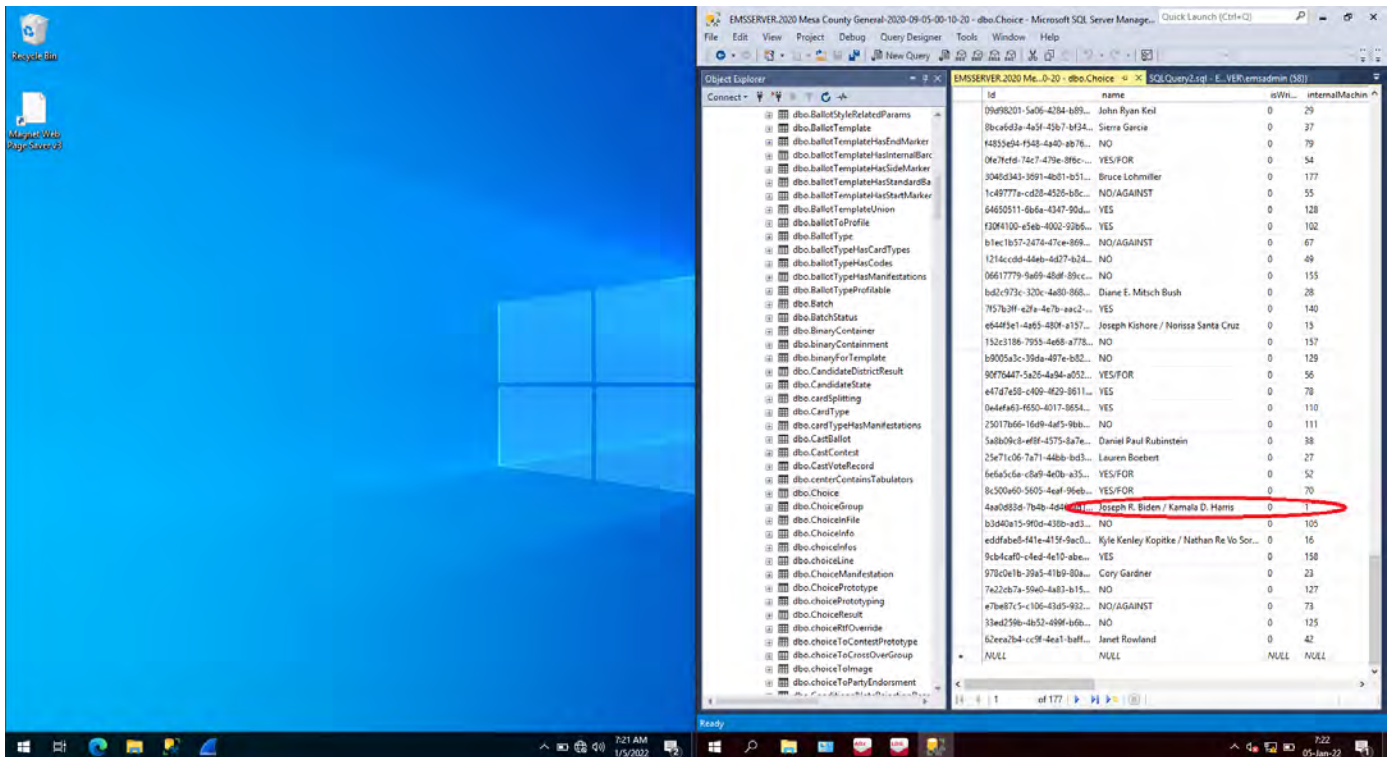


Figure 22 - Candidate settings for Biden

The 'Joseph R. Biden / Kamala D. Harris' choice has an internalMachinelD of '1.'

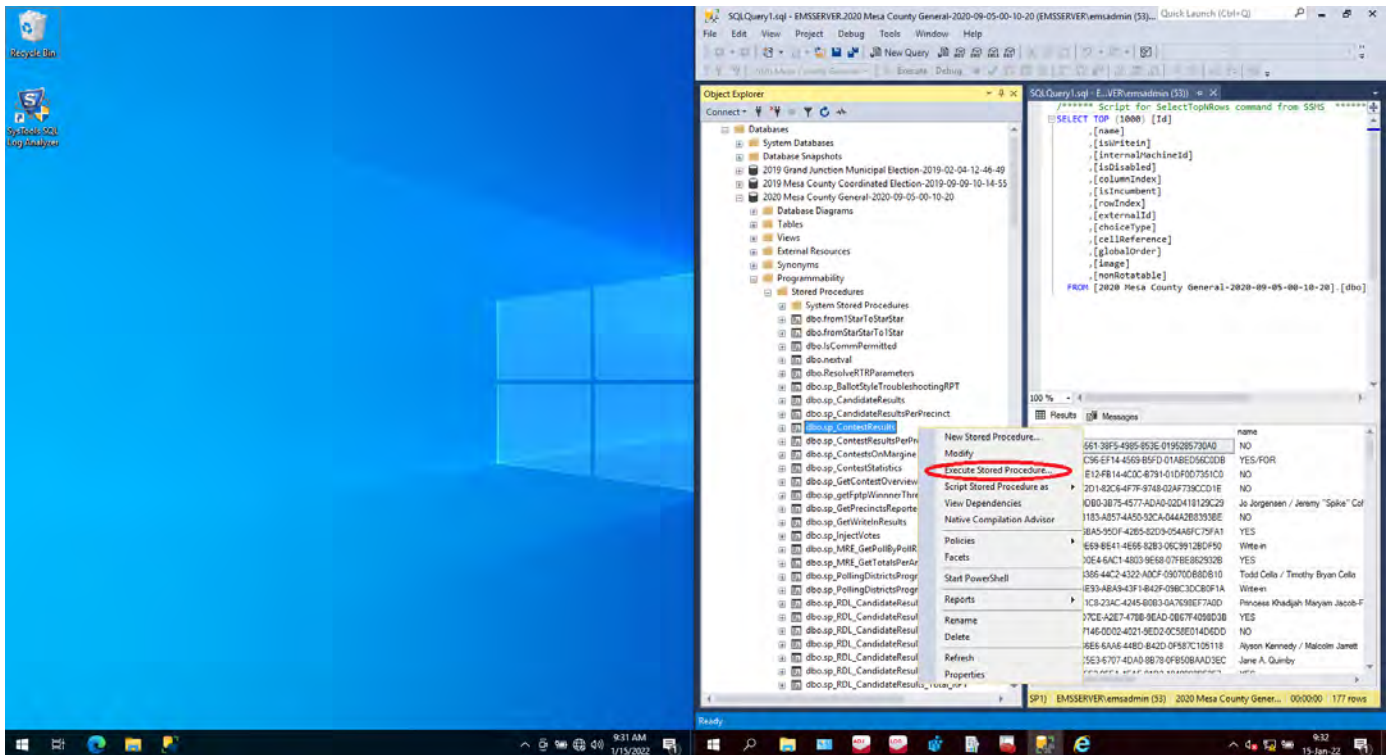


Figure 23 - Pulling up the results report prior to attempting the alteration

Prior to attempting to make a direct change that would alter the results of the election, the Stored Procedure 'dbo.sp_ContestResults' is executed to query the current contest results. These steps involve only a few clicks of the mouse.

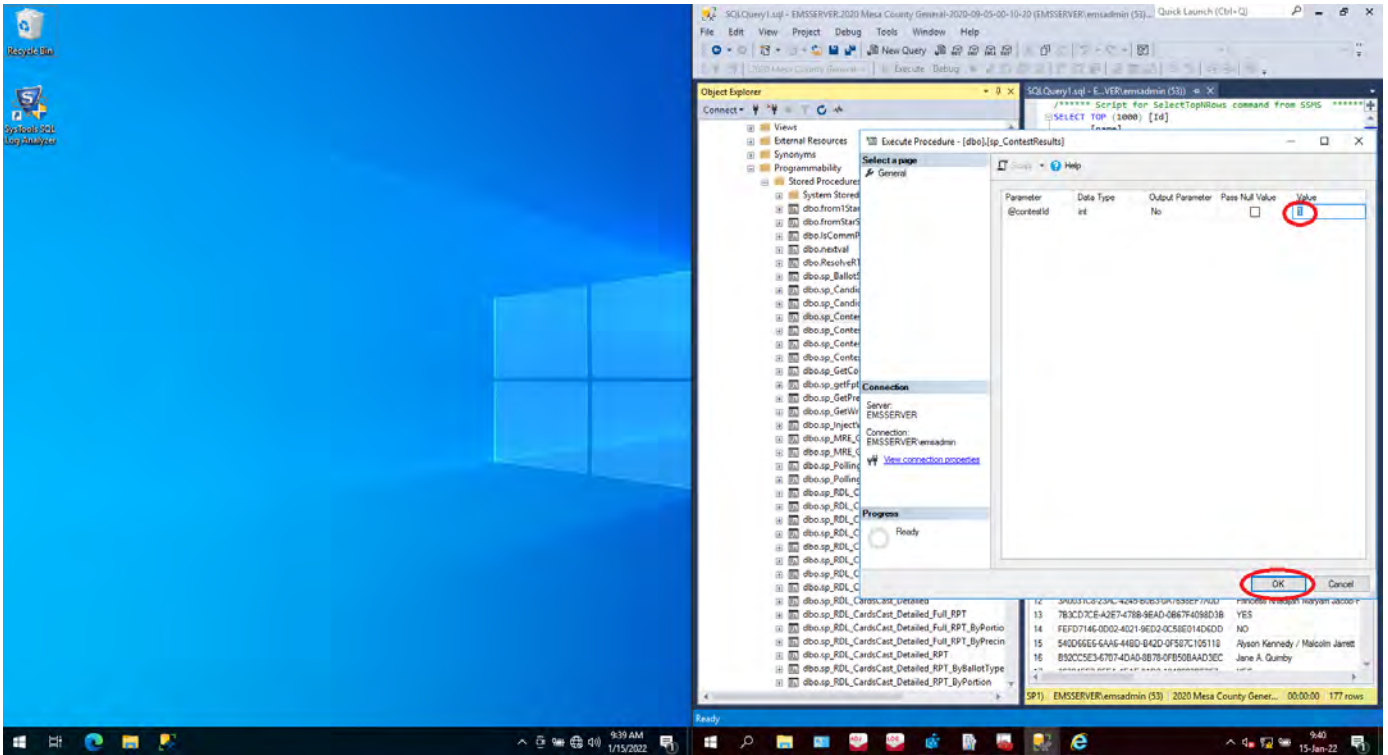


Figure 24 - Run Stored Procedure to pull up a report of Presidential Electors

The computer then prompts for which ContestId to query. A '1' to signify the Presidential Electors is entered, then 'OK' is clicked.

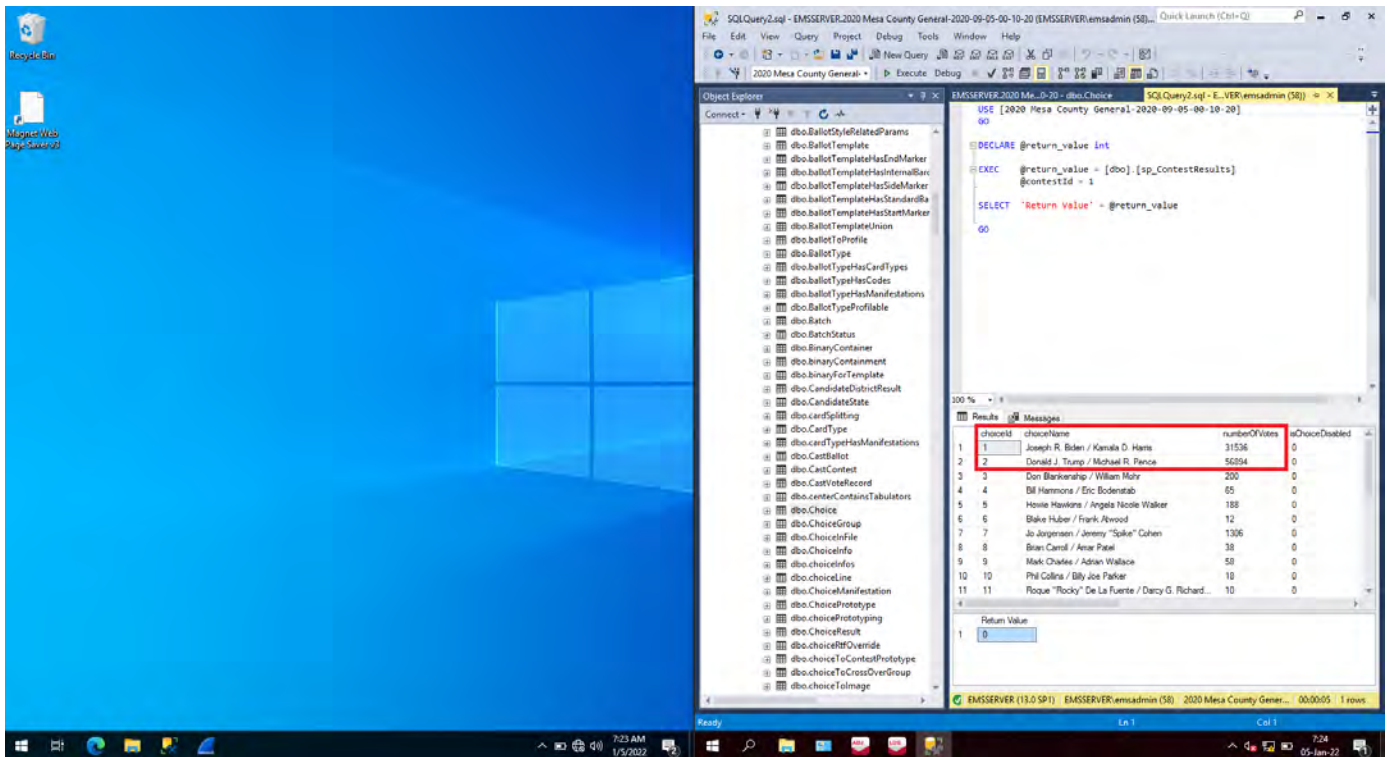


Figure 25 - Retrieved Vote Totals

This report shows the total number of votes for the Presidential contest:
 'Joseph R. Biden / Kamala D. Harris' as having 31,536 votes, and
 'Donald J. Trump / Michael R. Pence' as having 56,894 votes.

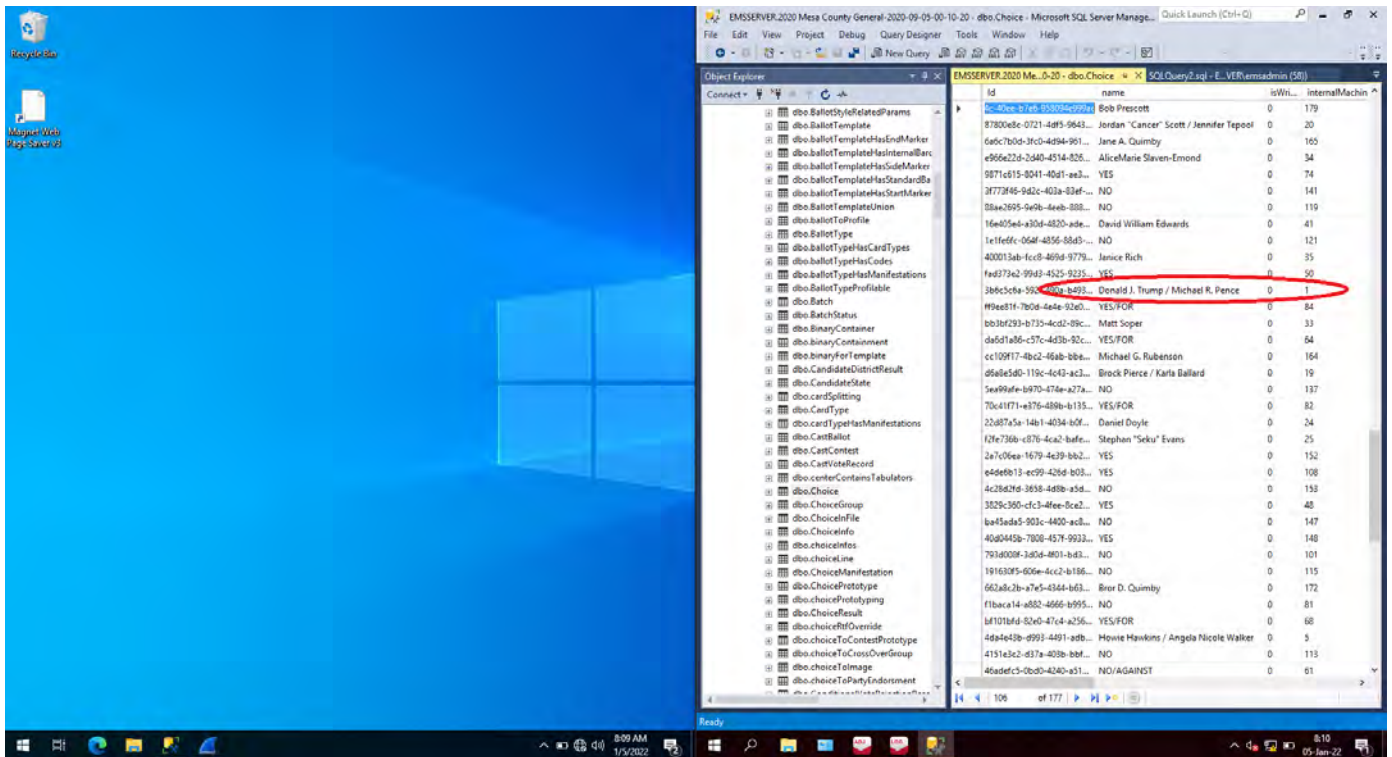


Figure 26 - Candidate number for Trump modified

Here, I change the Trump 'internalMachineld' from a '2' to a '1.' The SQL Server Management Studio allows the change without any hesitation or warning that a crucial piece of data was changed. The lack of good design and very poor referential integrity allows this.

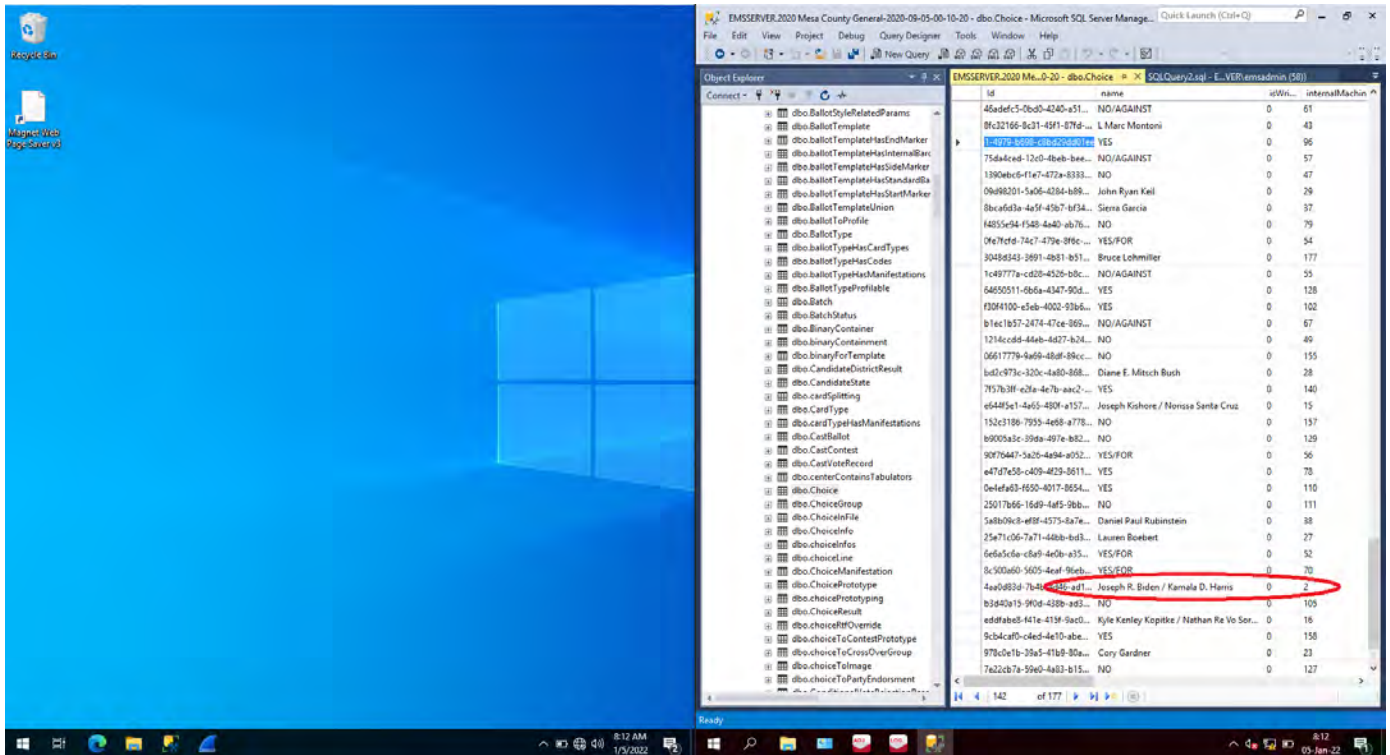


Figure 27 - Candidate number for Biden modified

Next, I change the Biden 'internalMachineld' from a '1' to a '2.' Again, there is no error message or warning given by the system.

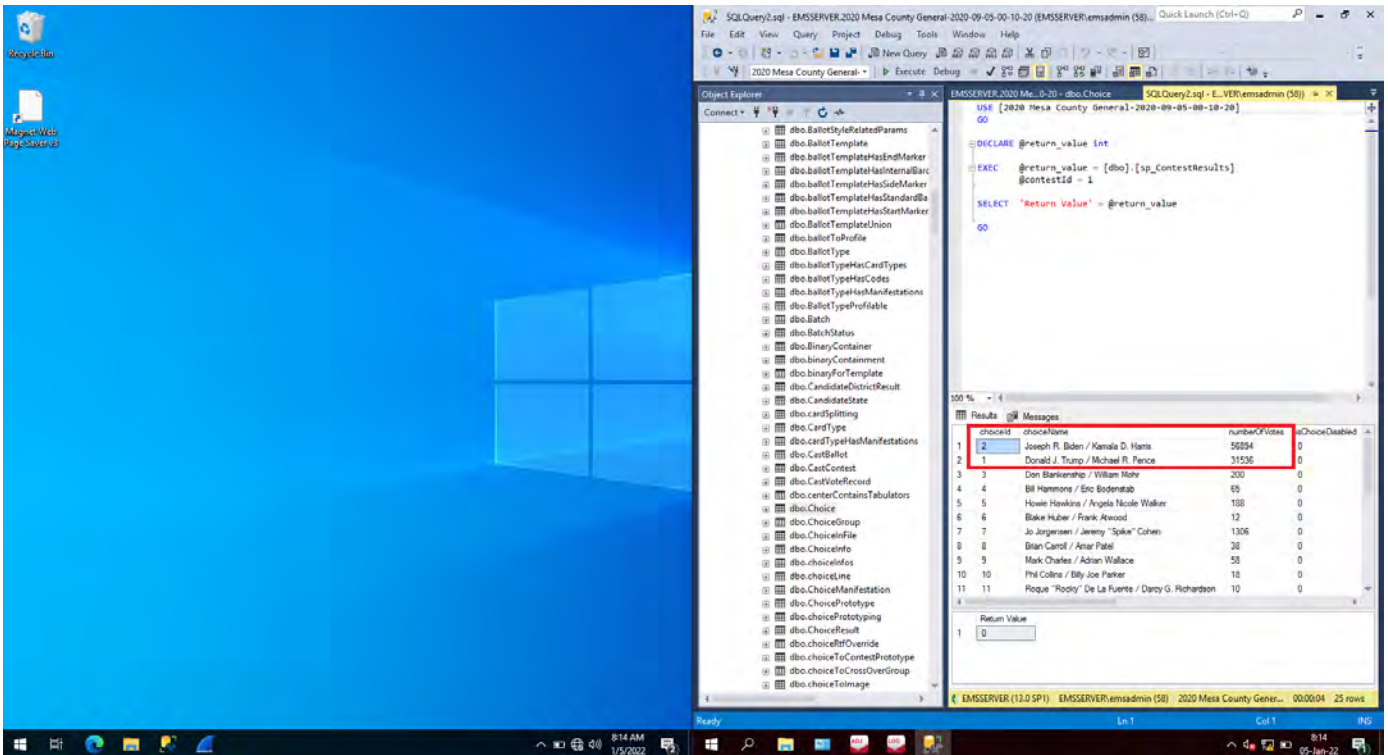


Figure 28 - Vote totals retrieved again after modification.

Making only these two small changes, which can be done in under a minute by an individual sitting in front of the voting system server, resulted in a flip of 25,358 votes. This demonstrates the ease with which someone can completely alter the results of the election on this EMS server with only a few mouse clicks and 2 keypresses on the keyboard with the software that is built-in to this voting system. This is only one in countless ways election data could be altered.

When the stored procedure is executed to retrieve the vote totals again, the vote totals for Biden now show 56,894 and the total for Trump shows 31,536.

By changing only two values in the election database in less than a minute, I have flipped 25,358 votes, completely changing the vote total results in the election database. The change was made using Microsoft SSMS software already residing on the EMS server, without needing to enter any additional password, and without a warning about the risk of changing this information.

Finding 2: The existence and use of unauthorized and uncertified Microsoft SQL Server Management Studio (found on the EMS server in Mesa Co. and in other counties around the country), allows and facilitates the bypass of Dominion Voting Systems' software to alter calculated vote totals in the election database by anyone with physical access to the logged-in EMS server.

It is important to understand how easily this was done, and therefore how quickly such a change can be made. It was not necessary to change the 88,430 votes in the database, but rather only two index values, the internalMachineld values, to completely flip the result of this county's votes.

Finding 3: It is a simple task to flip votes and therefore very easy to do quickly.

Finding 4: The insecurity of the Mesa County EMS server, in concert with unauthorized, uncertified software, allowed the alteration of the election result, flipping the vote from one candidate to another, with trivial difficulty.

Let us also distinguish the claim being made here:

It is not asserted in these findings that this 'Vote Flipping' was performed on this server during the 2020 election, but rather the design and configuration of the system permits it, and due to the extraordinary lack of security and the unauthorized, uncertified software installed on the system, the voting system itself was, and is, completely uncertifiable and wholly unsafe to use for any election.

To be explicitly clear, this demonstration is about the lack of security and the access that insecurity and unauthorized software allows, and it is explicitly not about the vote totals in any election from this server. The lack of efficient logging and the destruction of the required log files prevent any assertion to the contrary in this analysis.

Whether votes were 'flipped' using this process, or the countless other ways that could be used, requires examination of computer system logs and database logs, and other data, and will be separately addressed. In this finding, it is demonstrated that it is possible, and that the defects in the security and certification of the system are extraordinary and far beyond simple errors and omissions.

EXAMINATION RESULT 1

Vote totals can be altered by anyone with physical access to the logged-in EMS server.

EXAMINATION OBJECTIVE 2:

Determine whether the calculated vote totals can be altered by any person using a non-Dominion computer directly or indirectly connected to the EMS server network.

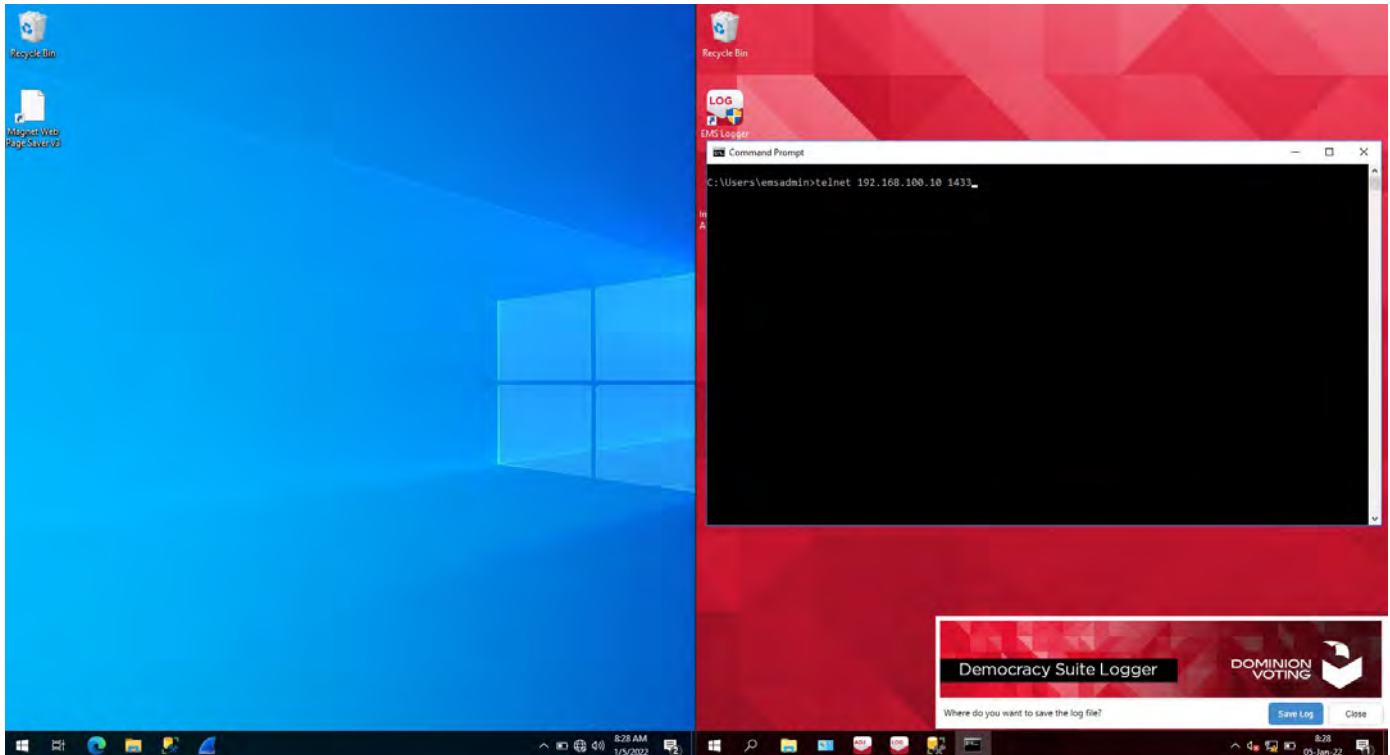


Figure 29 - Accessing port 1433 with Telnet

The telnet command is used to test to see if direct network connection to the database port is possible.

'Telnet' is a common network diagnostic tool used by IT and Cybersecurity professionals for communicating with a telnet server, and other text-based TCP services.

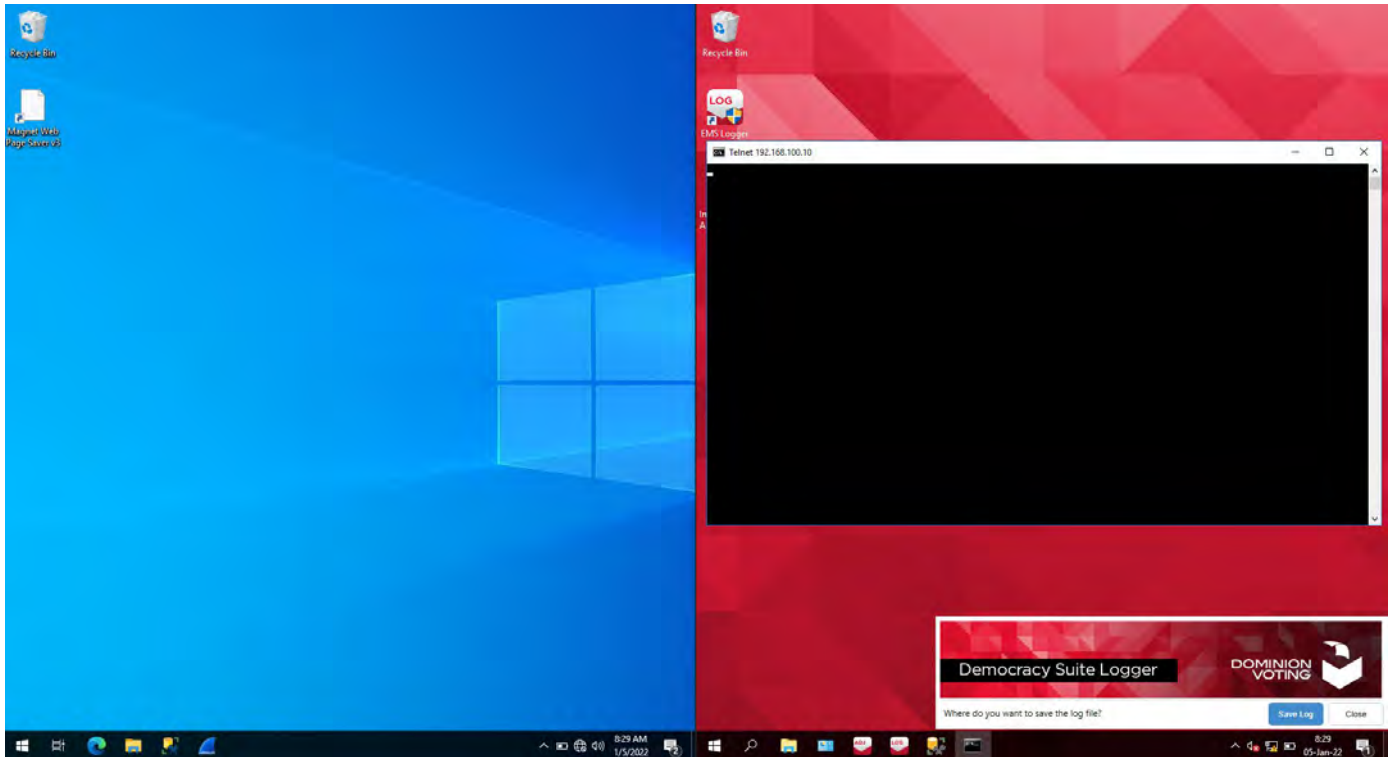


Figure 30 - The EMS server network interface appears to answer a connection to port 1433

The blank window with the cursor in the top left indicates that the connection was indeed successful, and the database service is now waiting for input.

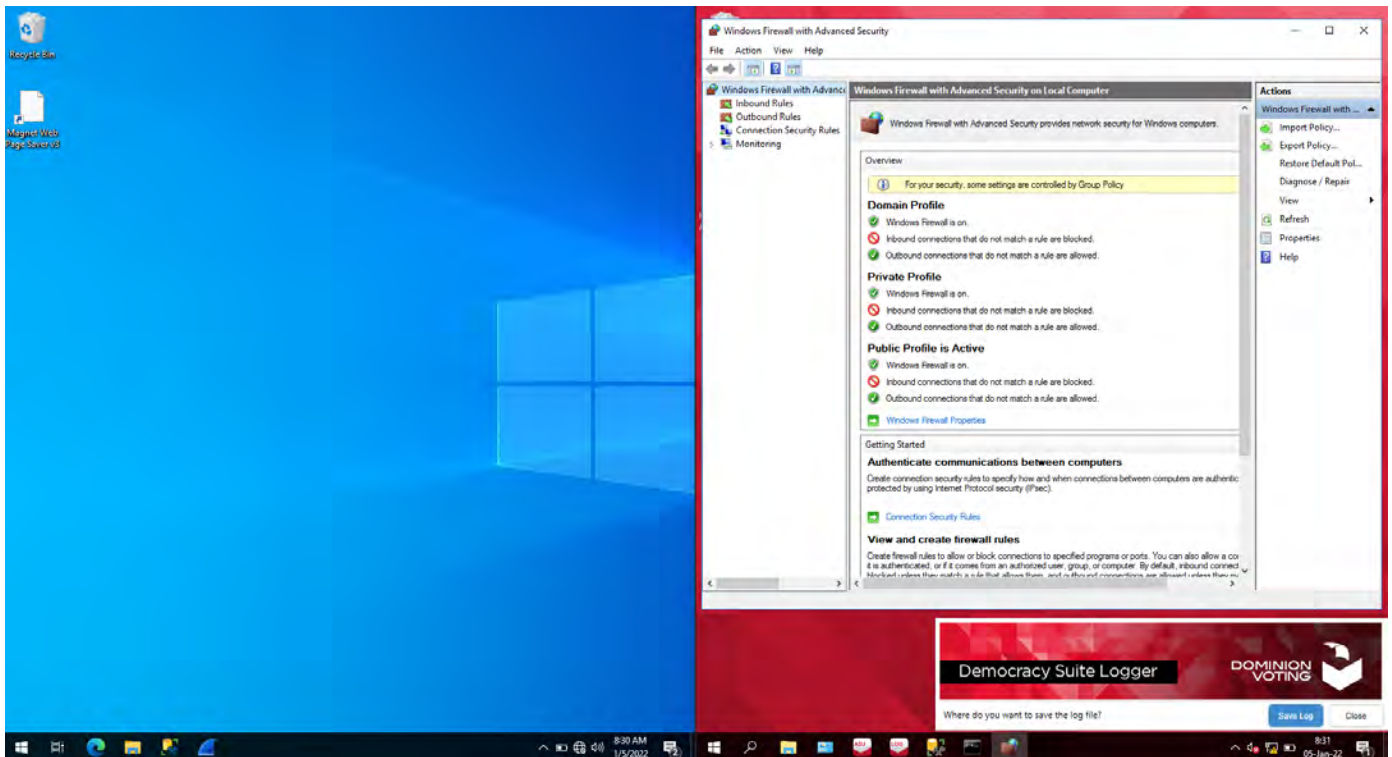


Figure 31 - EMS server has the 'Windows Firewall' enabled

Because it was trivial to connect directly to the database server on port 1433, the firewall was then checked to see if it was enabled on the server. This figure shows that the Windows Firewall with Advanced Security is installed and enabled, however the configuration of the firewall must now be examined to see why it allowed this activity.

The Mesa County EMS server contained firewall software, but it is the specific configuration of the firewall that is unsafe. In this screenshot, the firewall is shown to be enabled. For each profile ("Domain," "Private," and "Public"), the settings are the same:

- Windows Firewall is on. <- **GOOD**
- Inbound connections that do not match a rule are blocked <- **GOOD, but requires further inspection.**
- Outbound connections that do not match a rule are all allowed. <- **RECKLESS FOR A 'SECURE' SYSTEM**

Before going further, it is important to understand what a Firewall is and how it operates. A Firewall is a device that evaluates computer traffic on a network, and based on rules, allows or denies each specific connection. The rules in most common firewalls contain:

- the source IP address,
- source port number,
- Internet Protocol number,
- destination IP address,
- destination port number,

- (Some firewall rules may contain dates and times, for example Monday to Friday 8 am to 5 pm),
- the action to Allow the connection,
- Block the connection,
- Drop the connection, and
- whether to log the connection.

Typically, the rule base is evaluated from top to bottom in order, and the first rule that matches the connection is applied (and the rest of the rule base is skipped). For ANY connection that did not match previously – it is blocked by the Firewall.

It is notable that outbound connections that do not match a rule are set as “Allowed” in this EMS server. For a critical infrastructure voting system, such a configuration is completely reckless. Per VSS⁷⁰ and industry best practices systems that require connection should be explicitly specified, and no other outbound connections should be allowed. One of the reasons for such a requirement is that many internet addresses contain malicious software that can be downloaded and installed, sometimes automatically, depending on how they are accessed. The existence of such malicious software has given rise to an entire Anti-Virus and Anti-Malware industry.

⁷⁰ VSS Volume 1, sections 6.4 and 6.4.2

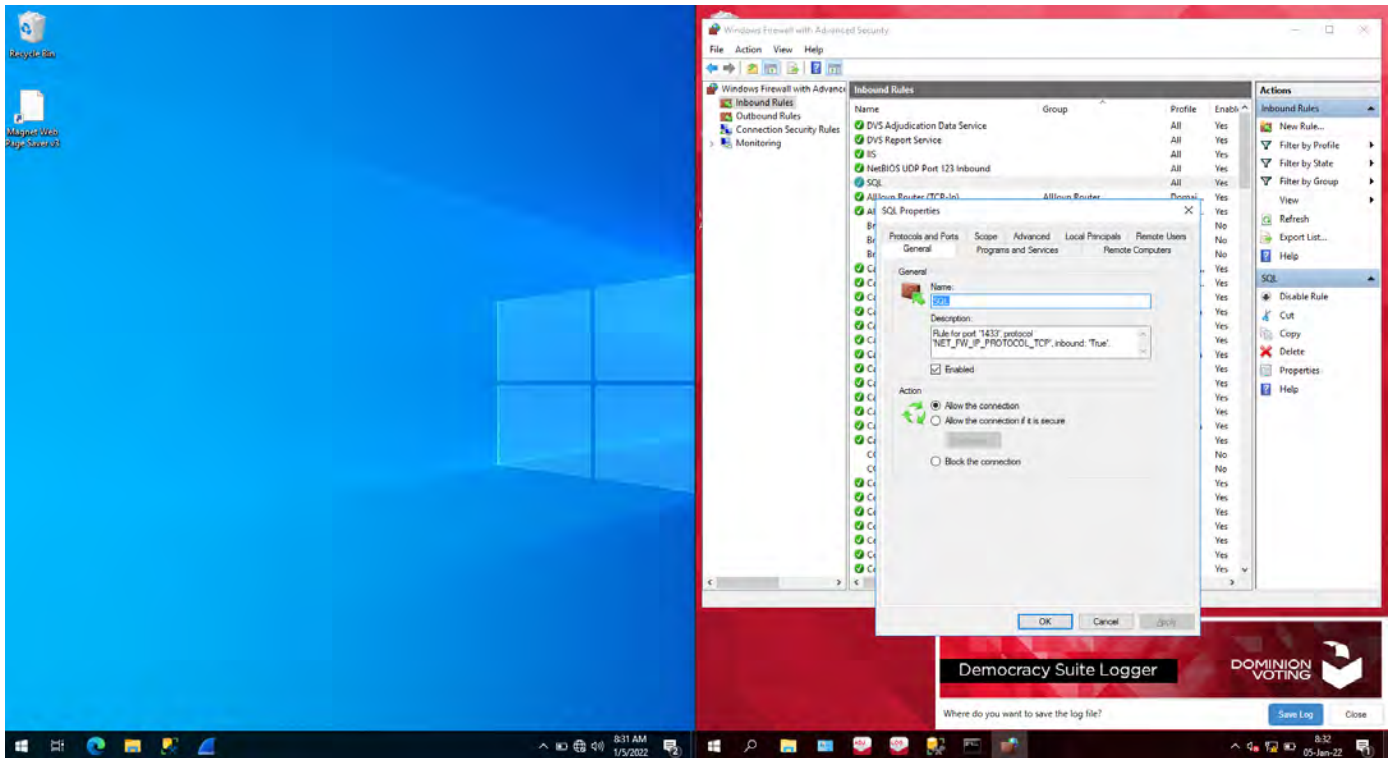


Figure 32 - Windows Firewall Custom SQL entry is enabled

Within the Windows Firewall, a custom firewall rule was found for the SQL service. This rule is not created by Microsoft; it must have been created by another means. The content of the 'SQL' rule is examined and shows the rule is "Enabled," and set to "Allow the connections". Note, the option titled 'Allow the connection if it is secure' just below the chosen option is available however not selected. This means again, the vendor had the option and opportunity to make the system configuration more secure, and neglected to or chose not to, and the individuals involved in the certification either did not check or ignored the vulnerability.

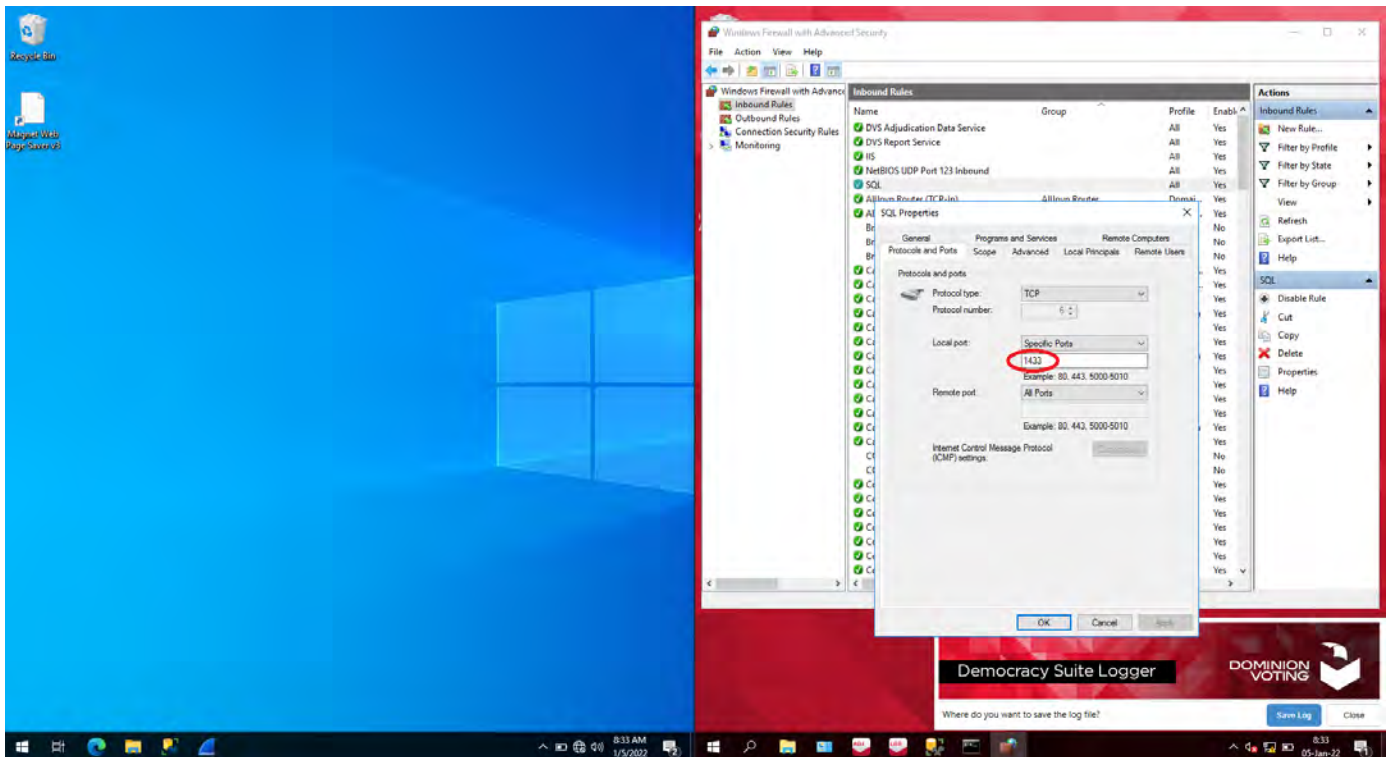


Figure 33 - SQL port 1433 is allowed.

The commonly-known default SQL Service, TCP port 1433 is specifically allowed by this firewall rule.

The port number selected for SQL database access could have been changed so that probing of the computer implicitly revealed less information. This is a recommended technique for high security networks where it is intended that the discovery of systems be disallowed; there are many other recommendations to be followed to truly harden the security of an operating system and its applications.

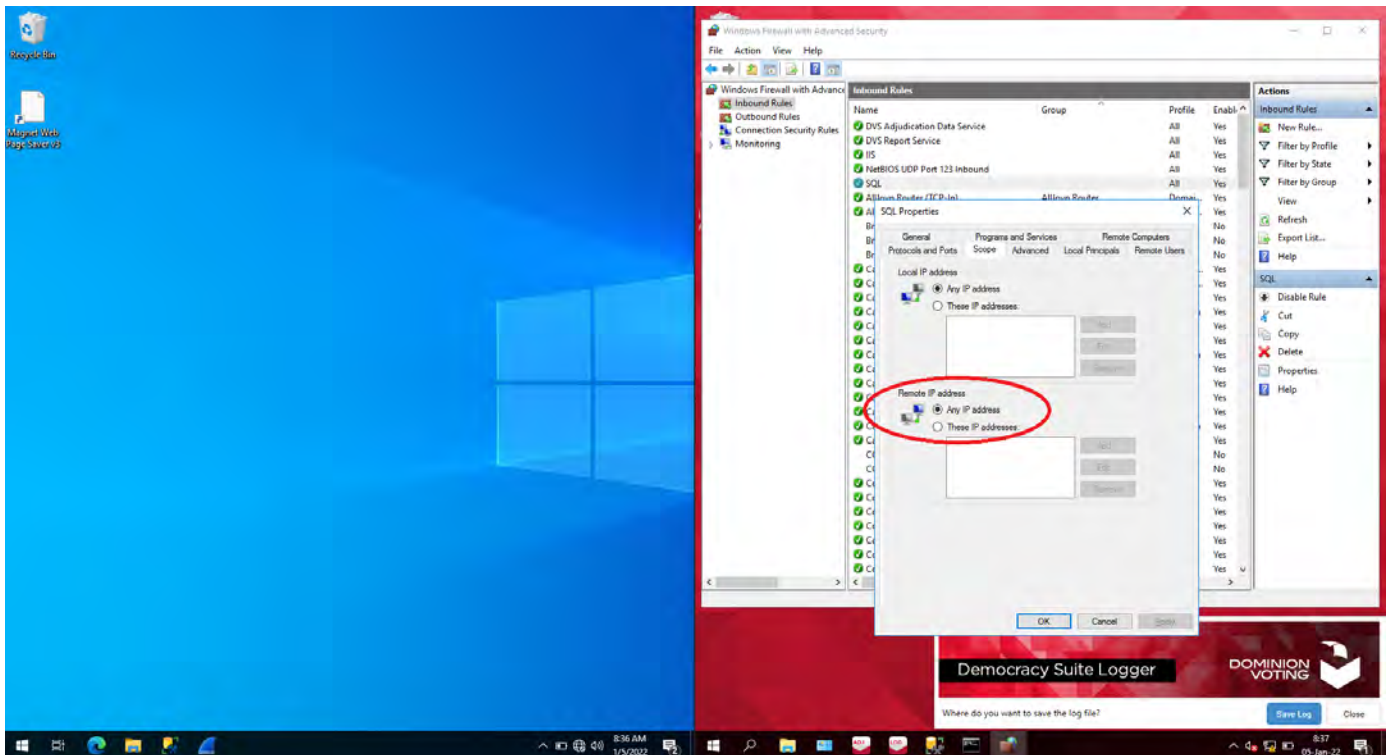


Figure 34 - Access to the SQL database standard port is allowed from ANY IP ADDRESS worldwide.

The IP address of the requesting computer is shown here as 'Remote IP address.' This rule is programmed to allow 'Any IP address' to connect to this port. Any IP address applies to any IP address anywhere in the world.

The ability to make the server more secure has been included by Microsoft and made easy to implement in the graphical user interface (GUI), specifically by allowing for the specification of Remote IP addresses to be accepted (which would exclude all those not explicitly listed). Microsoft documentation states:

“Any computer (including computers on the Internet): Not recommended. Any computer that can address your computer to connect to the specified program or port. This setting might be necessary to allow information to be presented to anonymous users on the internet, but increases your exposure to malicious users. Enabling this setting can allow Network Address Translation (NAT) traversal.”

The option to specify a list of IP addresses is present in the GUI, “These IP addresses:” but is not selected. Again, DVS had the option and opportunity to make the system configuration more secure, and neglected to or chose not to, and the individuals involved in the testing and certification either did not check or ignored the vulnerability.

Instead, they configured the option that Microsoft states is “Not recommended” and “increases your exposure to malicious users.”

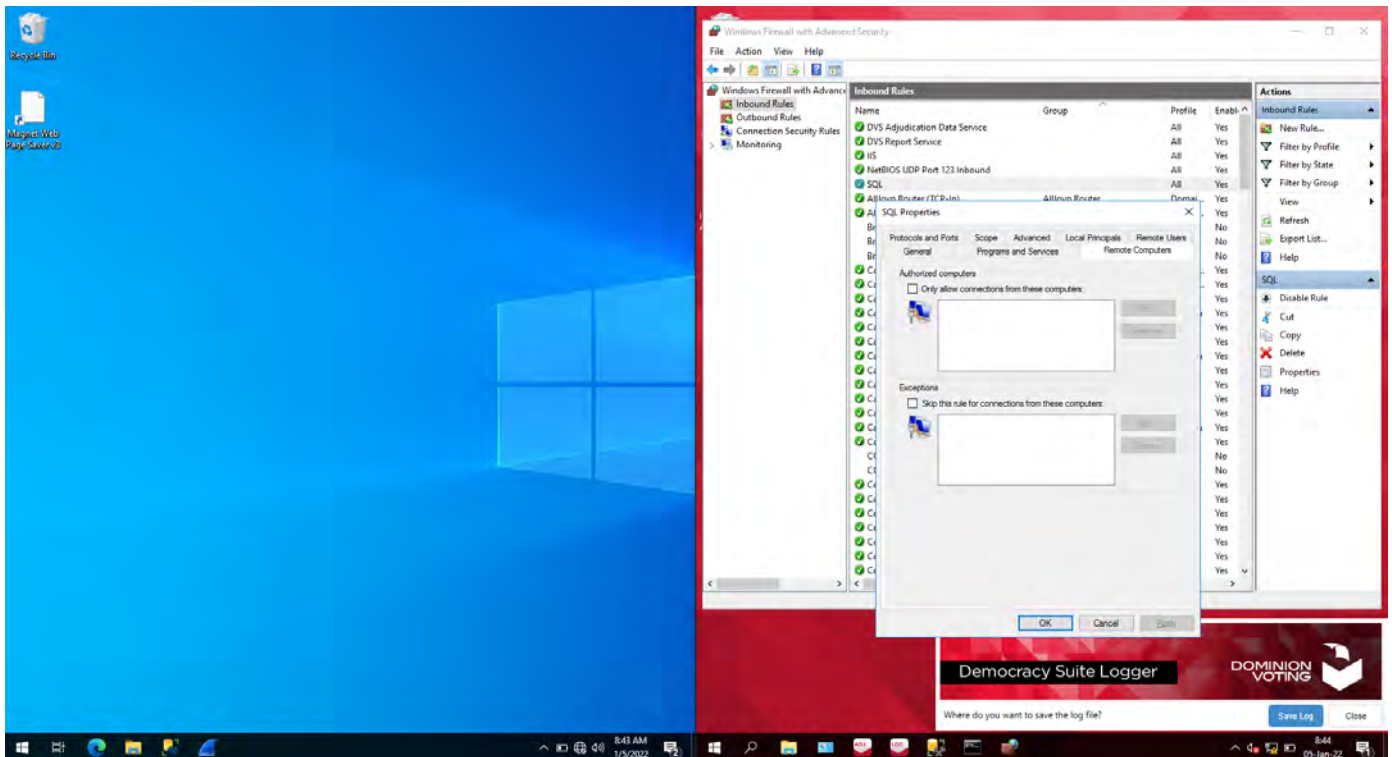


Figure 35 - No additional IP address restrictions or permissions

No restrictions are in place on the firewall that require authentication or integrity-protected communication on the network. The vendor could have specified as “Authorized computers” only those computers and devices deployed within the DVS D-Suite 5.11-CO voting system configuration in Mesa County, and excluded any and all other computers and devices in the world. But the vendor does not restrict that communication and, again, neither the voting system testing lab nor the Secretary of State staff took note or action regarding that neglect of a required security setting. For such a ‘secure’ critical system (“critical infrastructure,” according to the U.S. Government), there is no excuse for this lack of security to help guarantee integrity of each citizen’s vote.

It is possible to restrict access to a designated set of computers and even ensure that the connections are authenticated and integrity-protected. The functionality for this is built-in to the operating system, had the voting system vendor chosen to configure it. This safeguard of network traffic authentication and integrity-protection is available, but unused by DVS in this image of the Mesa County EMS server configuration.

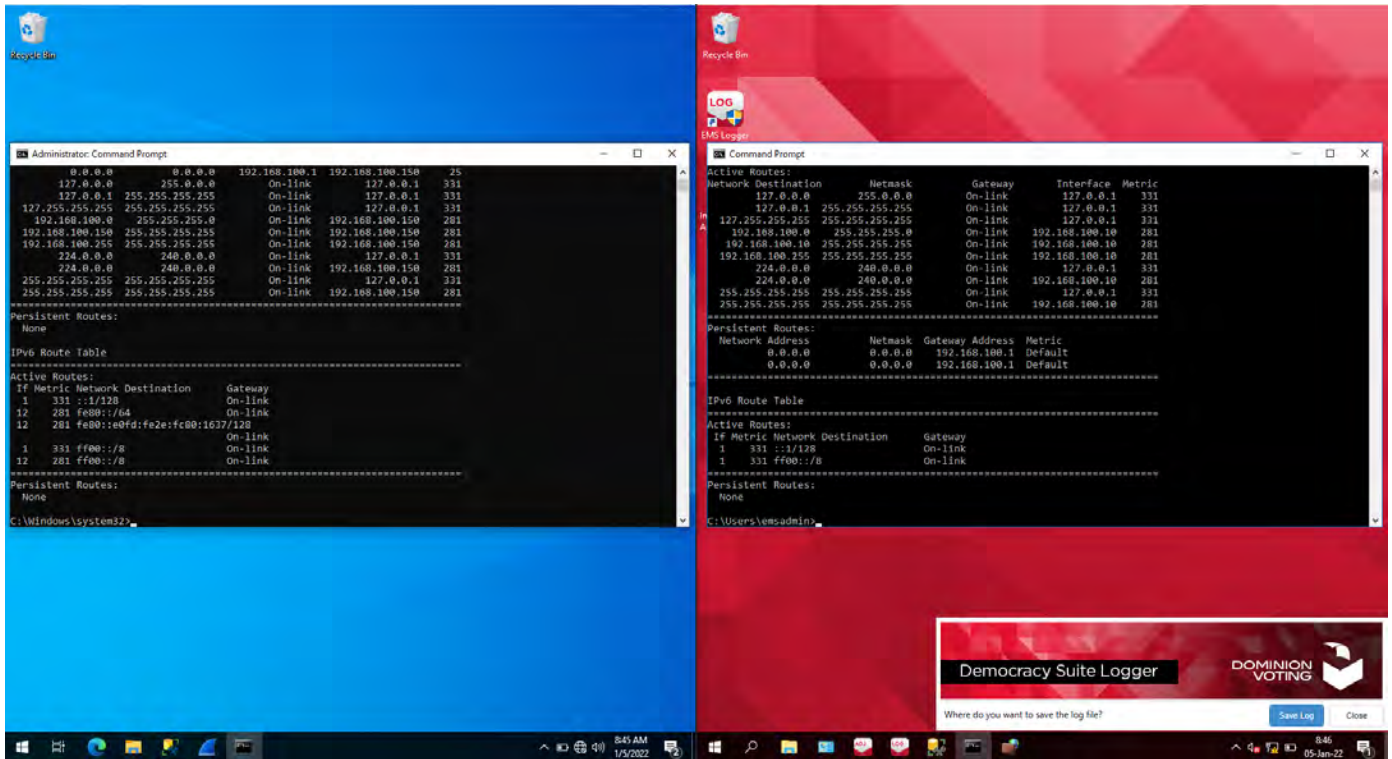


Figure 36 - Test Workstation, 192.168.100.150, and EMS, 192.168.100.10, are on the same subnet

This is demonstrating that the IP address for the Test Workstation on the left is on the same subnet as the IP address for the EMS Server on the right.

This address configuration shows that the test workstation and the EMS server are configured on the same subnetwork, i.e., “subnet,” e.g., they should be able to connect to each other if there is not something restricting them from doing so. If they were not on the same subnetwork, a router would be required but is unnecessary in this examination for the finding demonstrated here.

Testing the connection from an external Test Workstation tests the totality of the EMS server configuration and assures that claims of being able to connect from a separate computer not part of the DVS system are valid. Specifically, this test assures that no additional countermeasures or configuration of the EMS server are overlooked in arriving at this conclusion.

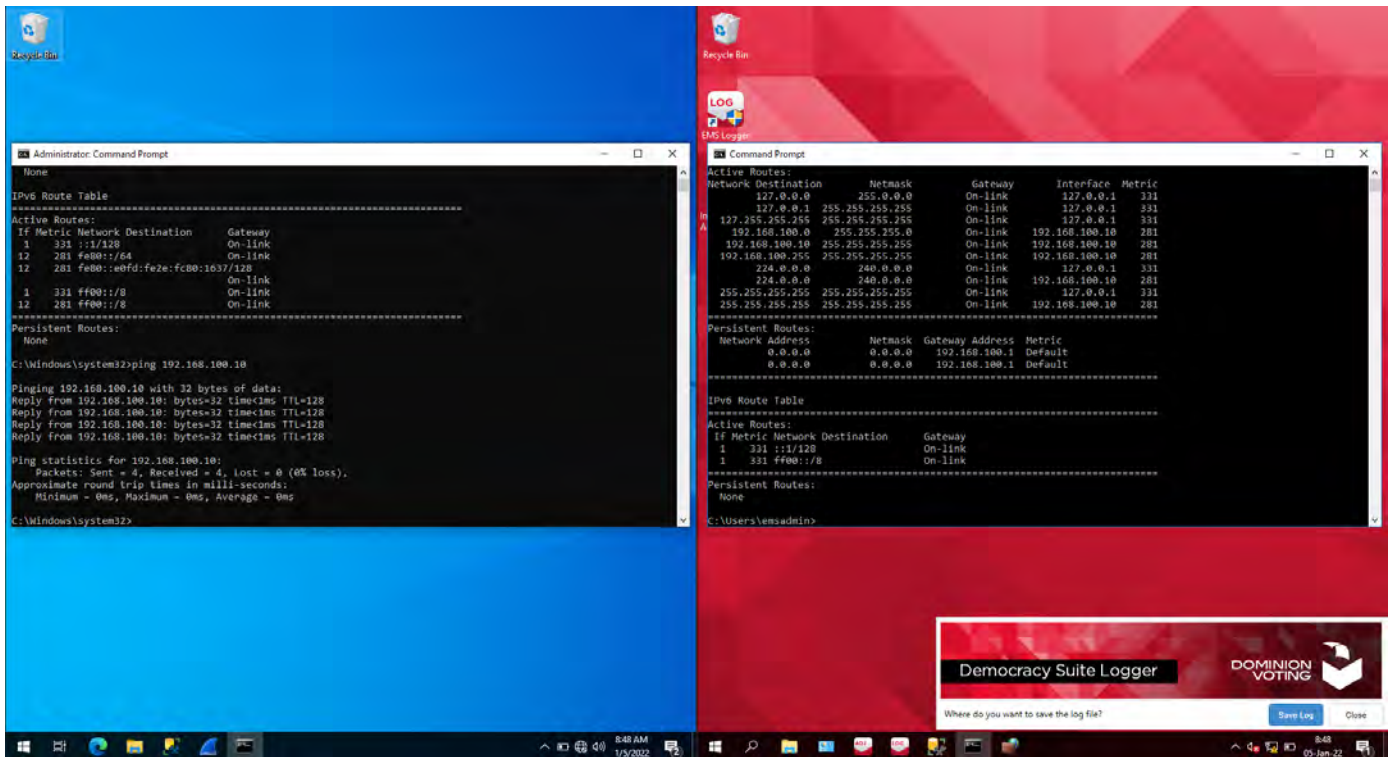


Figure 37 - Mesa EMS server is responding to network ping test.

‘Ping’ is another common diagnostic utility being used to determine if the EMS server on the right responds to the request from the Test Workstation on the left. All 4 responses were received by the Test Workstation from the EMS server, in response to the 4 requests sent by the Test Workstation.

In a properly highly secured network, one would expect the Internet Control Message Protocol (ICMP) request to be disallowed on the EMS server, in order to help prevent the unauthorized or malicious discovery of the DVS D-Suite network structure of devices and addresses.

This test demonstrates the lack of such restriction: the EMS server responded to the request.

The ping test uses Internet Control Message Protocol (ICMP) and transmits an “echo request” to the echo service on a remote computer. The remote computer responds and the original computer records the time it took to return the request. This is commonly used to determine if a device with a particular IP address is present on a network. This test demonstrates that the Test Workstation is connected to the EMS server across the network.

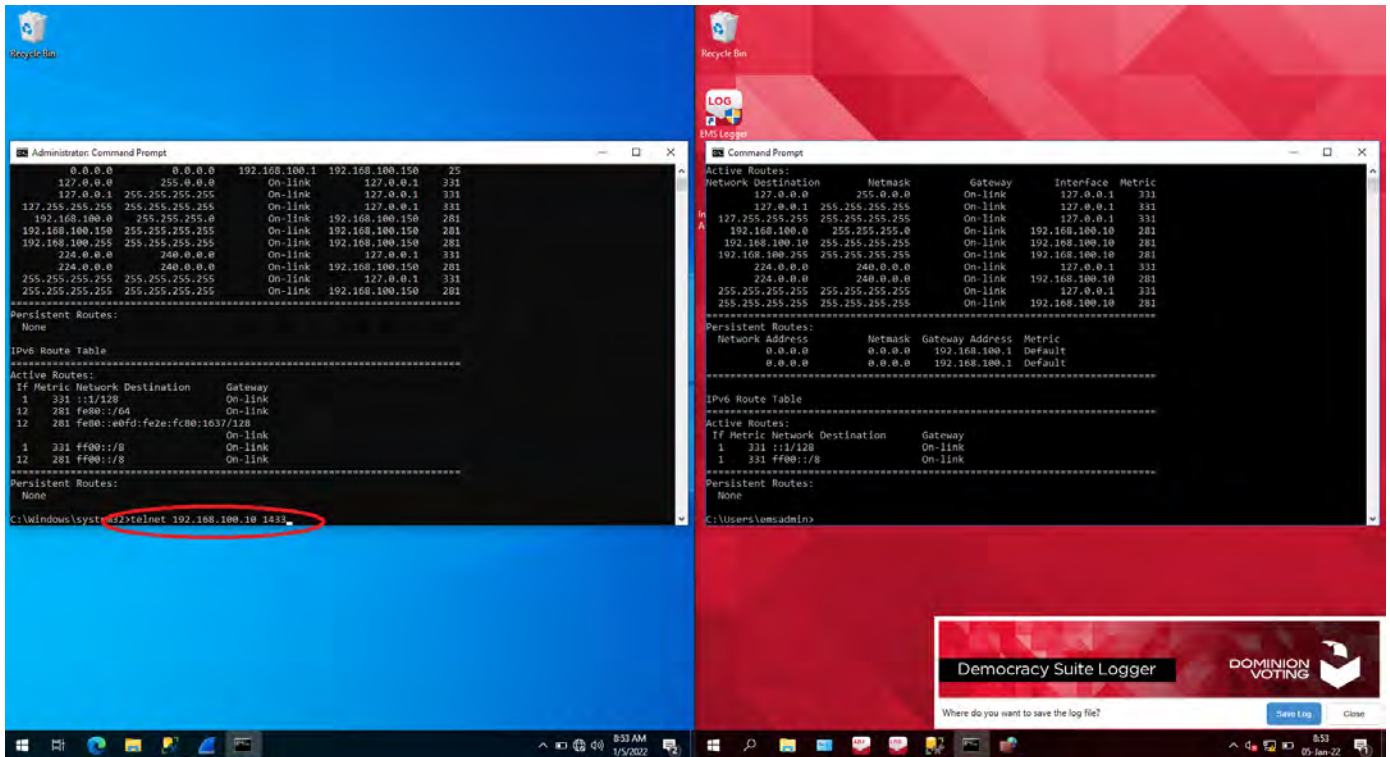


Figure 38 - Telnet connectivity test from separate computer not part of the Dominion system

The same 'Telnet' command (as in Figure 28) is used to see if the commonly-known default configured SQL Server port of 1433 on the EMS server at 192.168.100.10 can be connected to this alternate non-DVS D-Suite system.

Having established that the test workstation can connect to the server IP address, the Telnet command is used to test the connection to the EMS server's SQL service. Previously this connection was attempted from the EMS server to itself. The connection from the Test Workstation, a separate computer not part of the DVS D-Suite system, is attempted here.

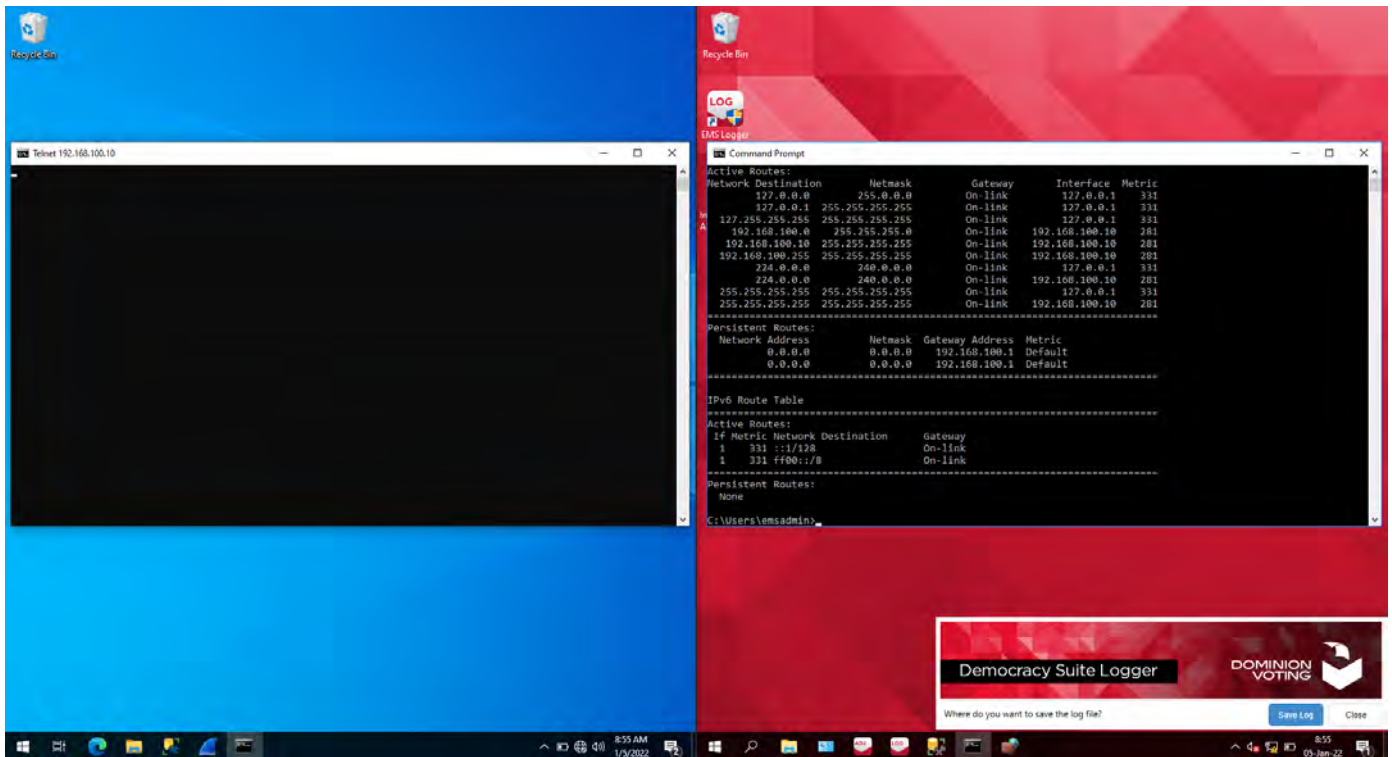


Figure 39 - Telnet to EMS server port 1433 (SQL) succeeds

Just as when this same test was run on the EMS server itself, the connection to the SQL Server port 1433 on the EMS server is successful from the Test Workstation.

The Telnet utility from the Test Workstation is able to connect to the EMS server showing, as in the Telnet test from the server to itself, that the SQL database service port is operating and listening for connections, and accessible from a non-DVS D-Suite computer.

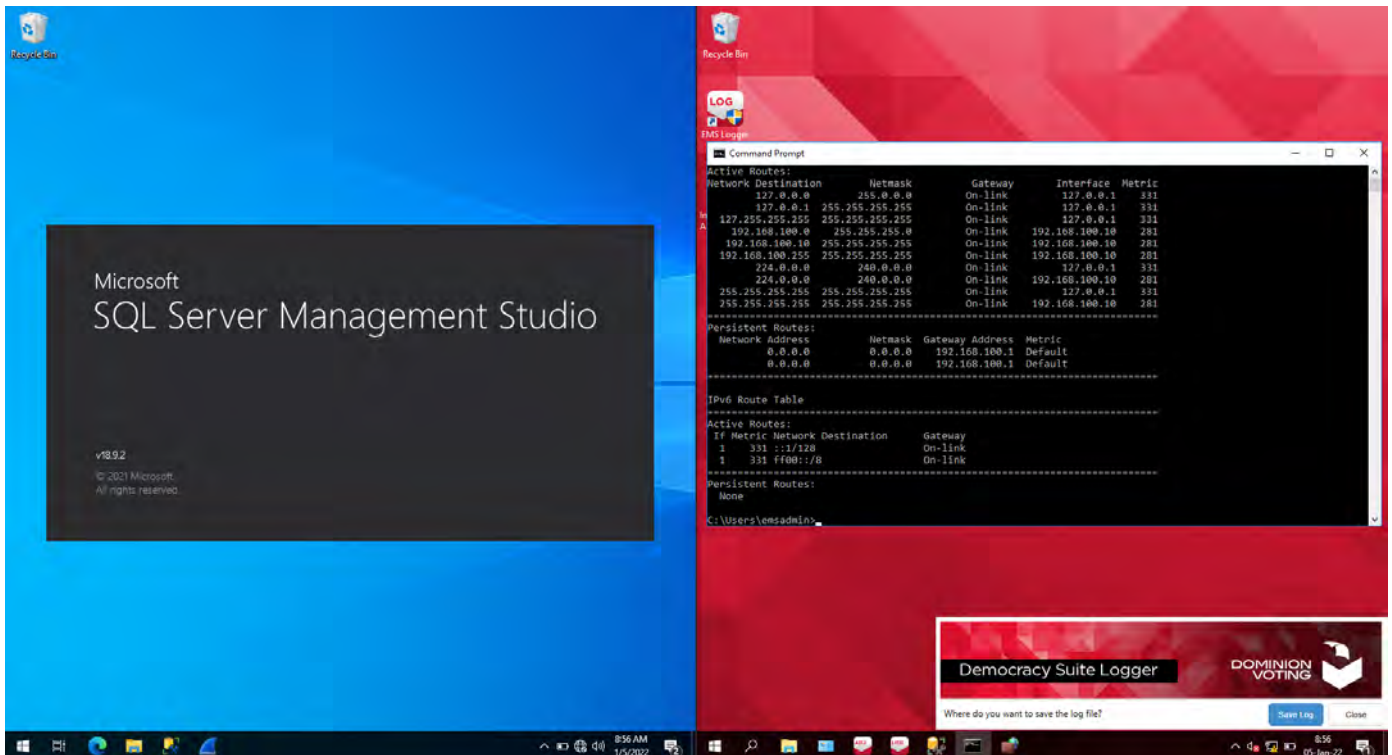


Figure 40 - SSMS access test from separate computer not part of the DVS D-Suite system

SSMS is downloaded from Microsoft and installed on the Test Workstation. Here, it is started, just as it was on the EMS server previously.

Anyone could do this by following the simple directions found with an Internet search for 'how to download SQL server management studio.' There are also many videos on the internet that walk even a novice through doing so.

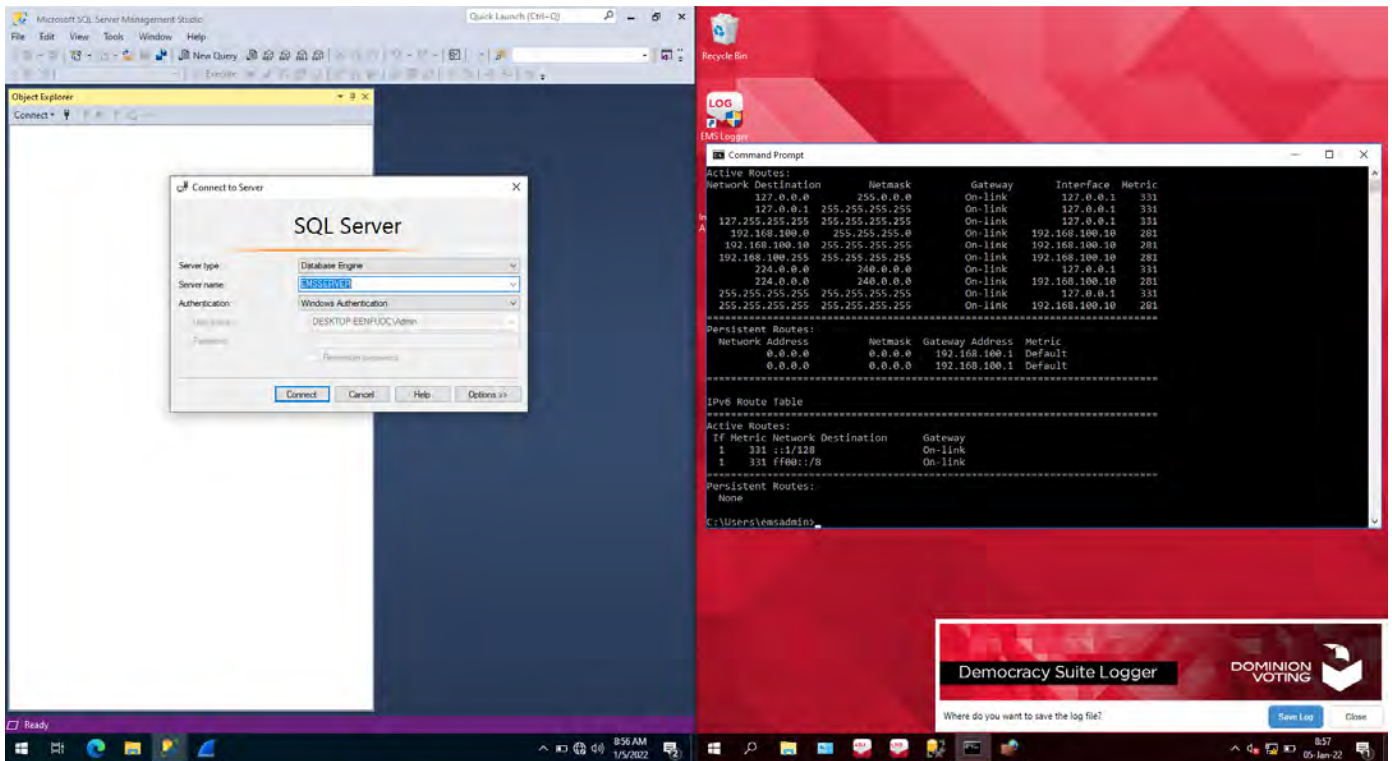


Figure 41 - Log In to the server

A user account was created on the Test Workstation using the same username and password that was used to log in to the EMS server on the right. SQL Server Management Studio was started and the same computer name 'EMSSERVER' was typed into the 'Server name' field on the Test Workstation.

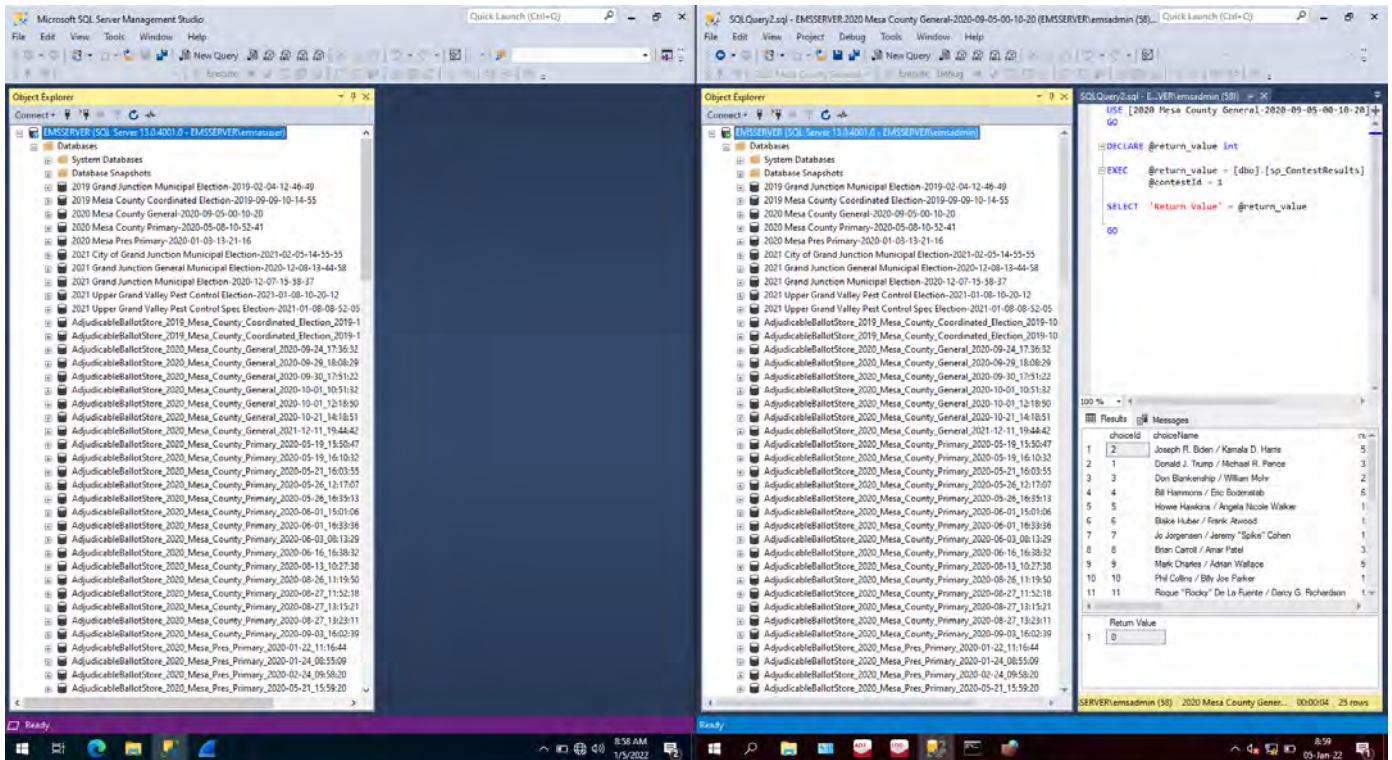


Figure 42 - From a separate Windows 10 computer EMS server database access has been obtained.

After clicking 'Connect,' SQL Server Management Studio connected successfully without so much as a warning. Clicking on the '+' next to Databases reveals the same list of databases available on the EMS server itself, accessible from the Test Workstation.

In Figure 42 I have obtained access to the EMS server from a separate computer not part of the Dominion system and can see election databases. On the left side of the screenshot, the display from the test workstation is shown and on the right side of the screenshot the display from the EMS server is shown. Both systems show the same databases listed. Remote access (i.e., from a separate computer not part of the Dominion system) to the database has been obtained by the Test Workstation.

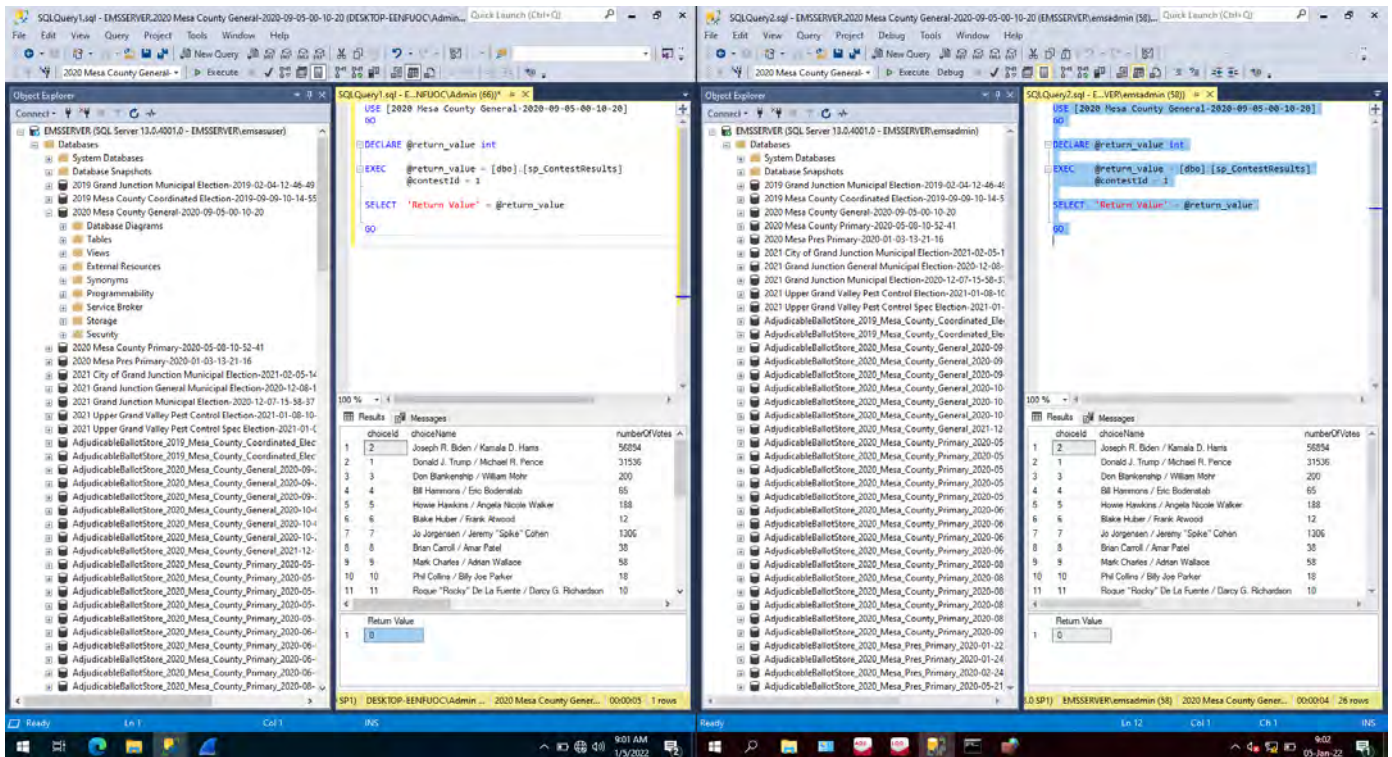


Figure 43 - From a separate Windows computer, the databases can be accessed and reports run.

To confirm this is the data directly from the EMS server, the same report is run on both systems. They both report identical information from the database.

The results display the database in the most altered state in which it was left, showing the flipped 56,894 votes for Biden and 31,536 for Trump from the test illustrated in Figure 28.

Finding 5: The security configuration of the Mesa County EMS server permitted access to election data and records from a separate computer not part of the DVS D-Suite system.

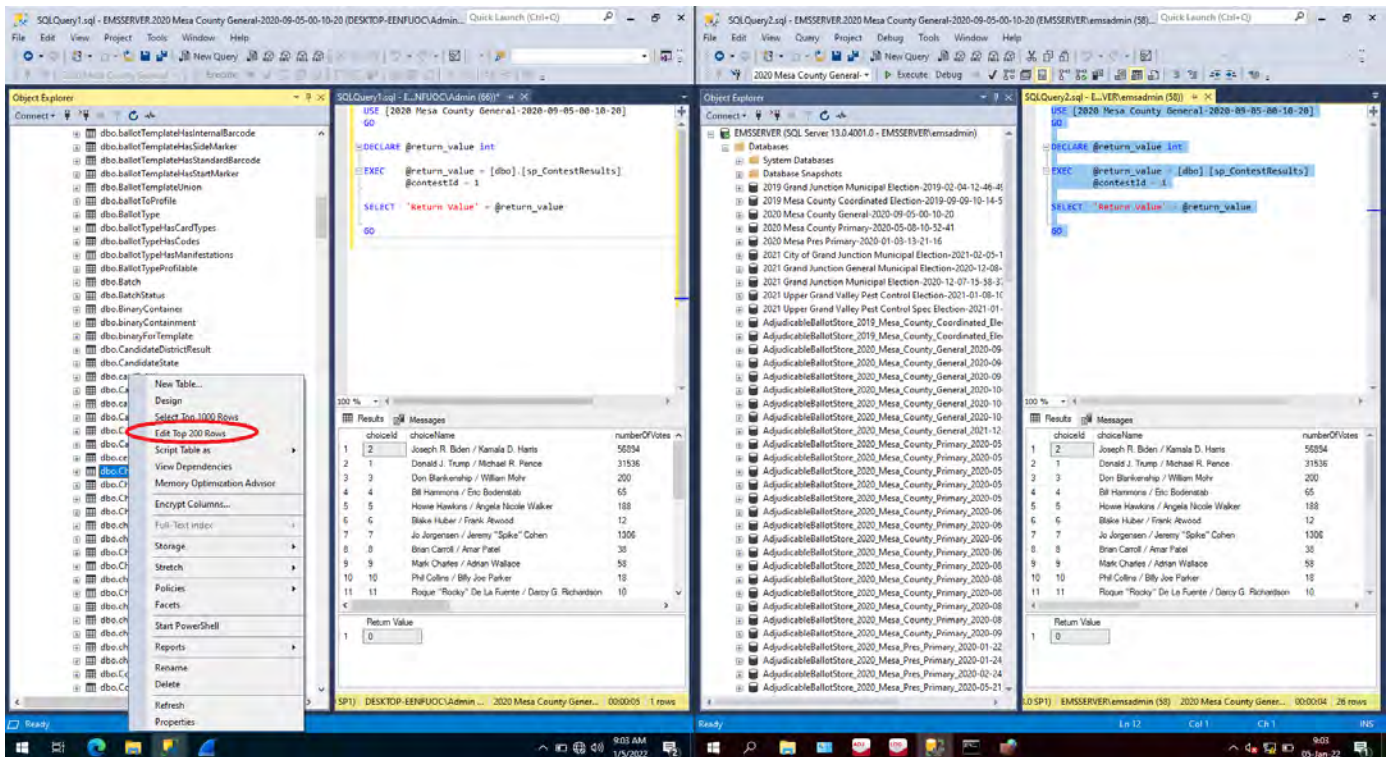


Figure 44 - SSMS permits database Edit

I again right-click on the 'dbo.Choice' table and then select 'Edit Top 200 Rows'.

As previously shown via the EMS server itself, using Microsoft SSMS on a separate computer, not part of the DVS system, access was gained to the same data and the same operations performed as if it was done on the EMS server itself.

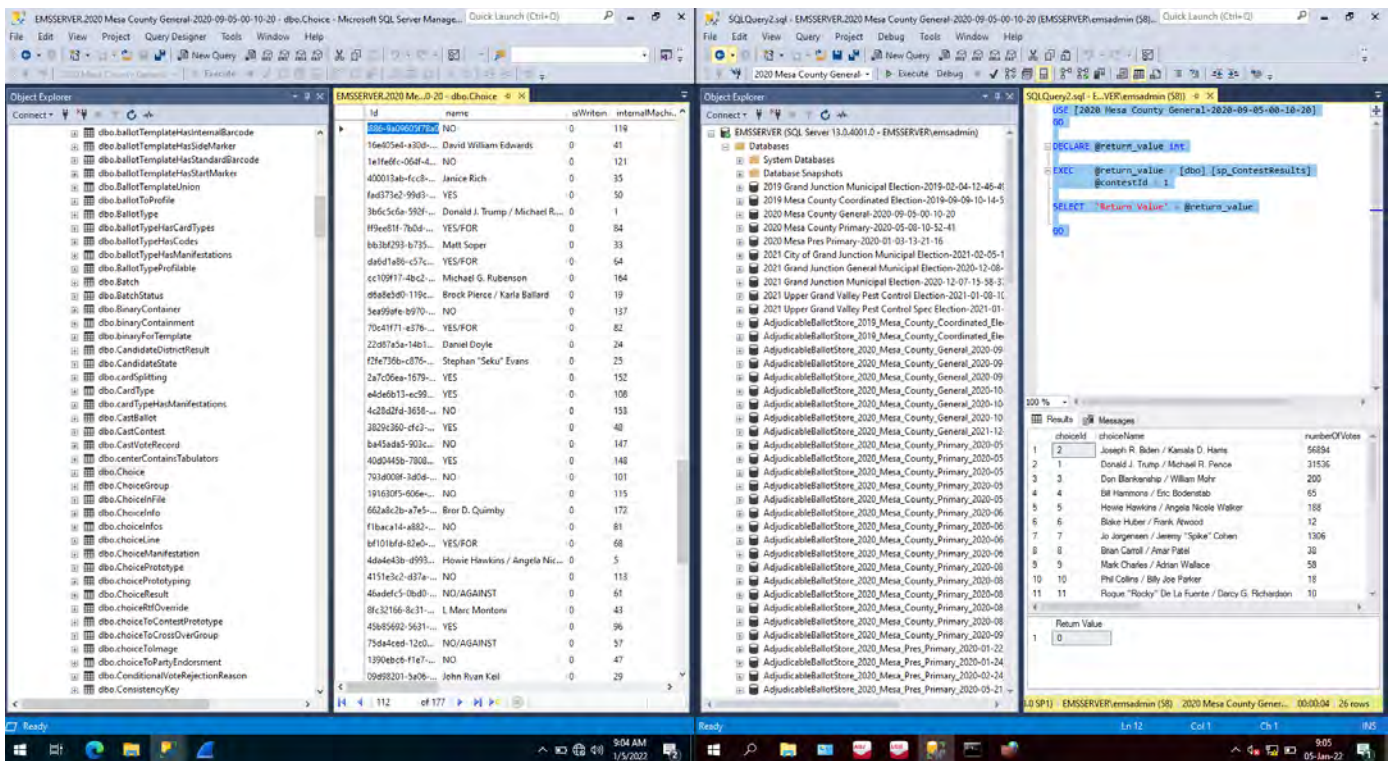


Figure 45 - EMS server Database view from a separate computer not part of the DVS D-Suite system

SSMS shows the same table in the same format as it did on the EMS server.

In Figure 45 the top 200 rows of the election database are available for editing using SSMS running on the Test Workstation to access the Mesa County EMS server across the network. The internalMachineld for Biden is still '2' and for Trump it is still '1' from the previous alteration in Examination Objective 1 (Figure 26).

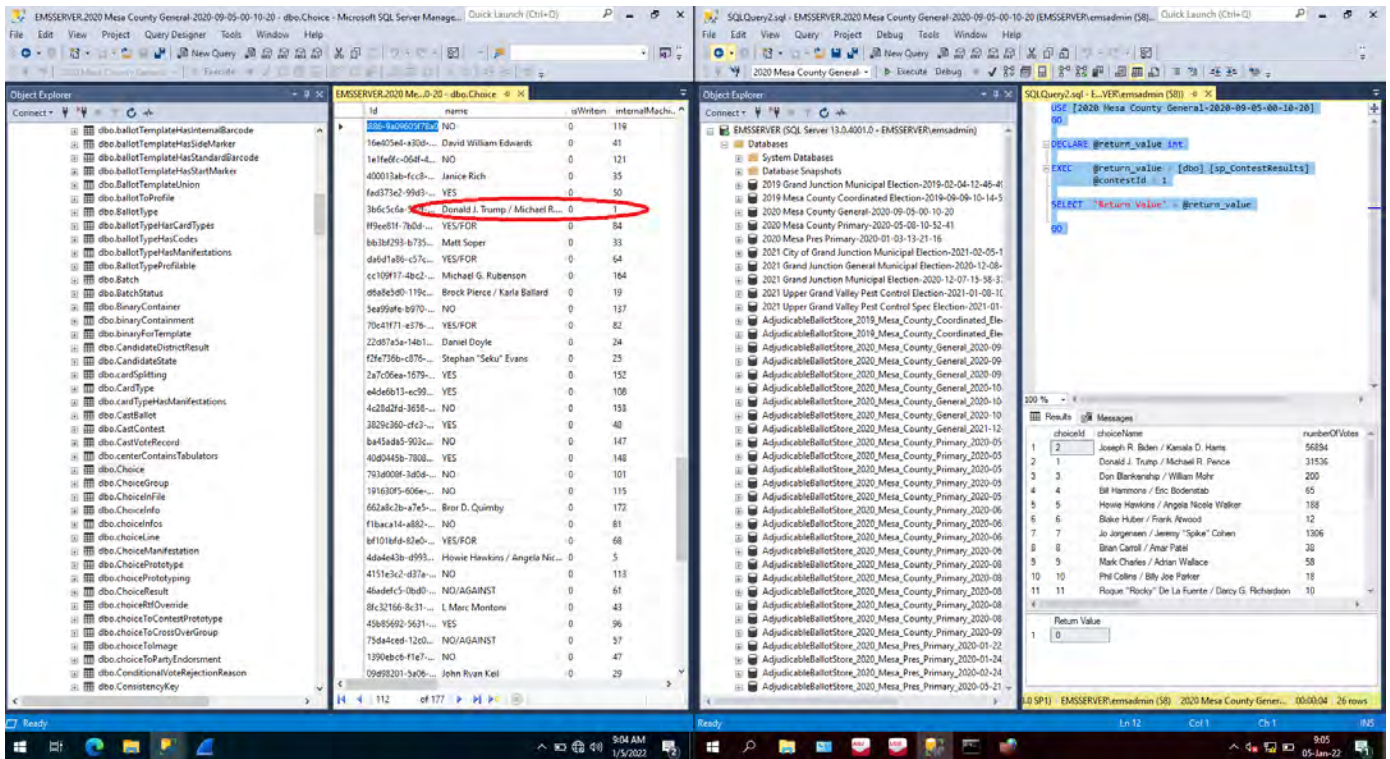


Figure 46 - SSMS permits us to edit the databases

A successful attempt to edit the election database on the EMS server, from the Test Workstation, is made to reverse the changes made earlier, thereby altering them back to the original results. Note the current setting of internalMachined for Trump is '1.'

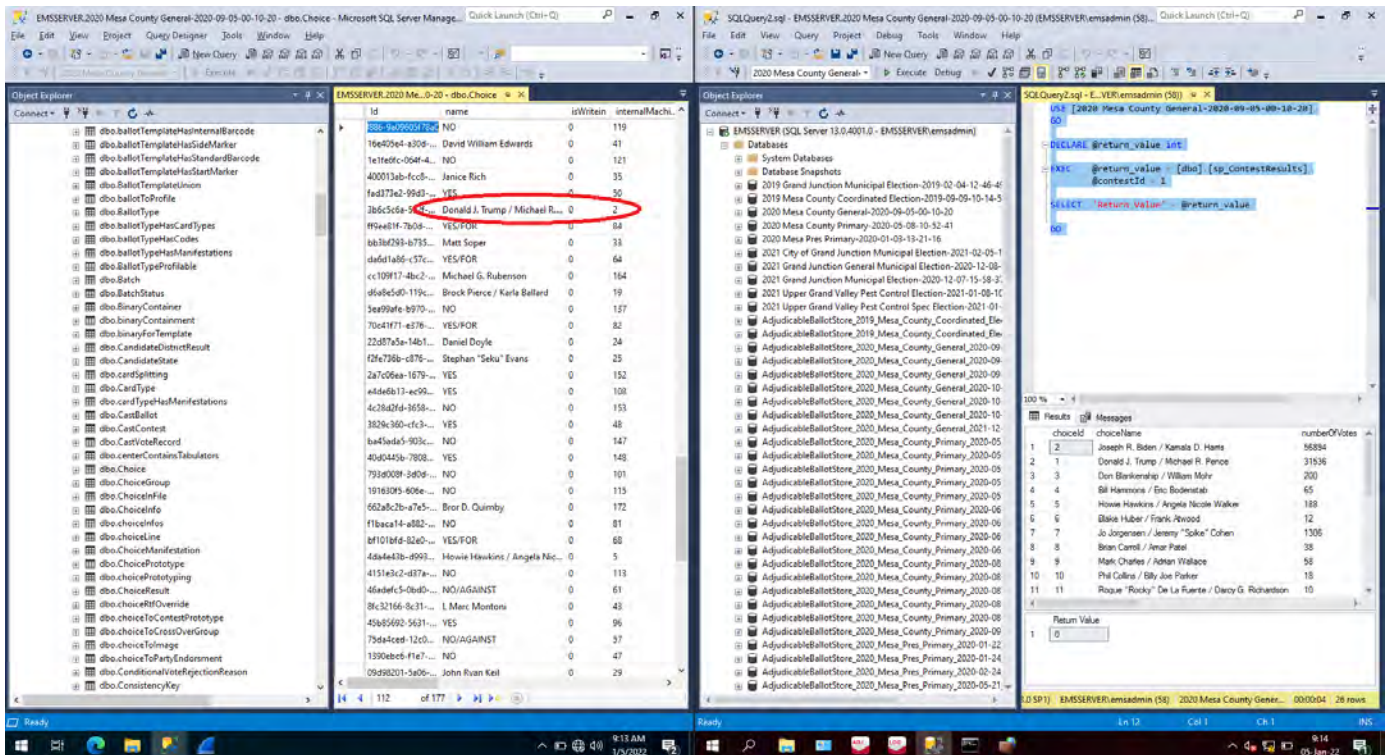


Figure 47 - “internalMachineId” for Trump is now changed back to a 2.

The “internalMachineId” for Trump is changed back to “2.” The database server allows this alteration from the Test Workstation without any error or warning.

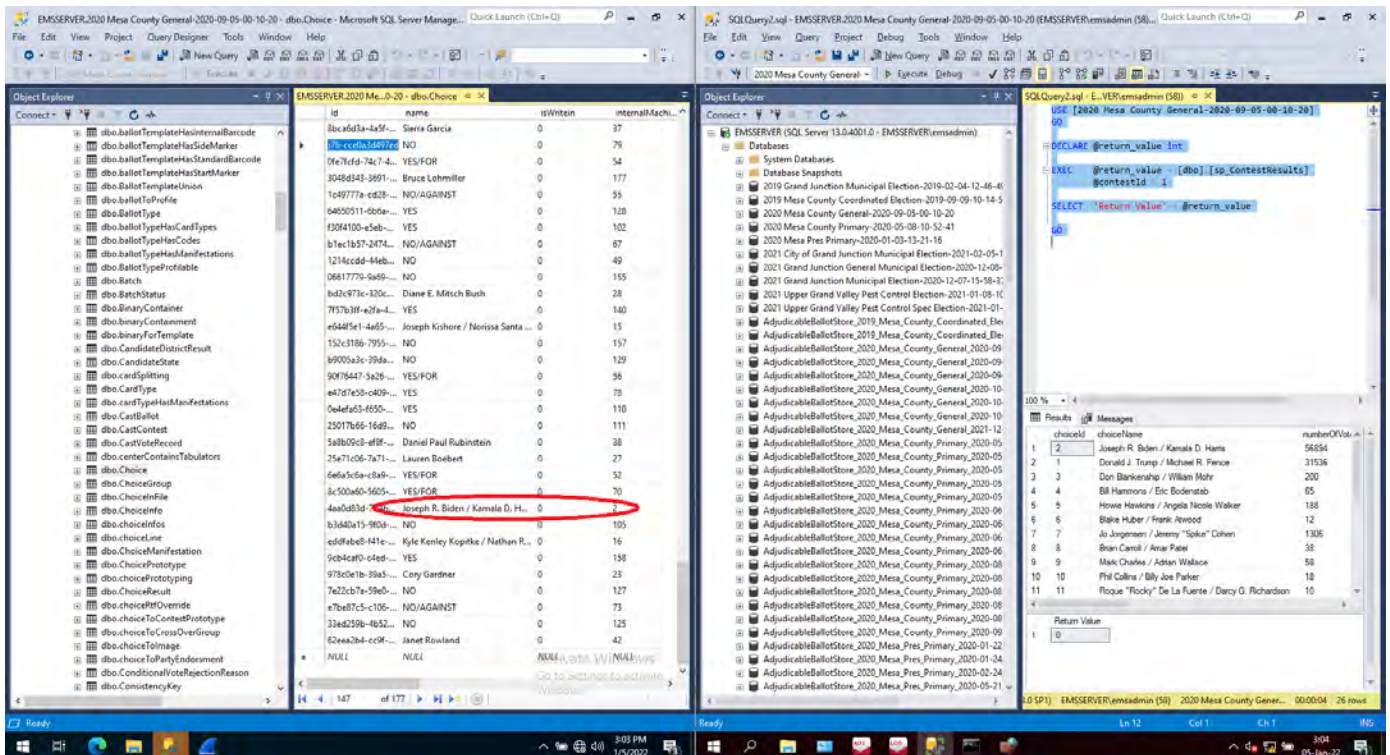


Figure 48 - Candidate data for Biden from previous change

The current “internalMachinel” for Biden is still “2”, in the election database on the EMS server, as changed earlier from the EMS server.

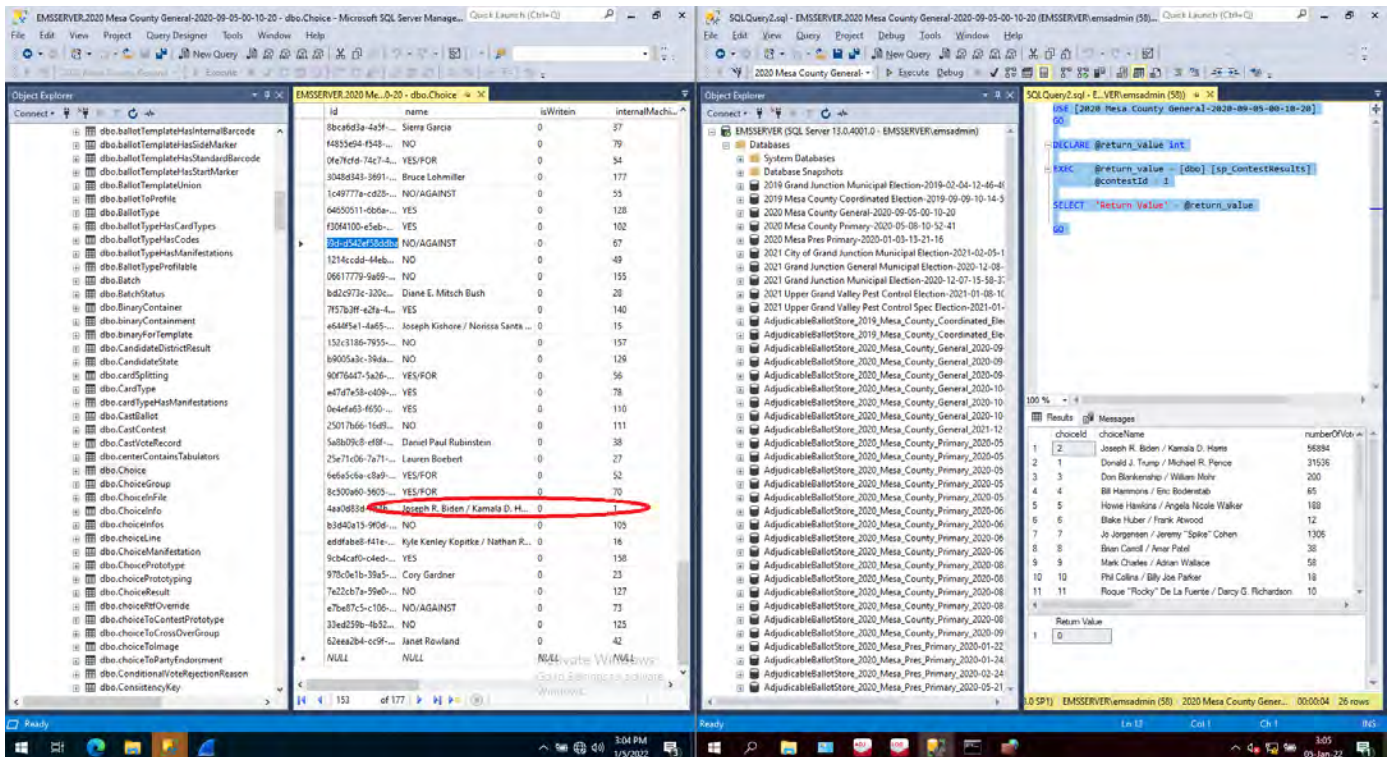


Figure 49 - Candidate data for Biden changed back to original

I next change, from the Test Workstation, the “internalMachineId” for Biden in the election database on the EMS server back to “1”, its original value. There is again no error or warning given.

As one can see, this alteration of the voting database was also successful. The system has been restored to the state in which it was found prior to making the first alteration of the voting system database.

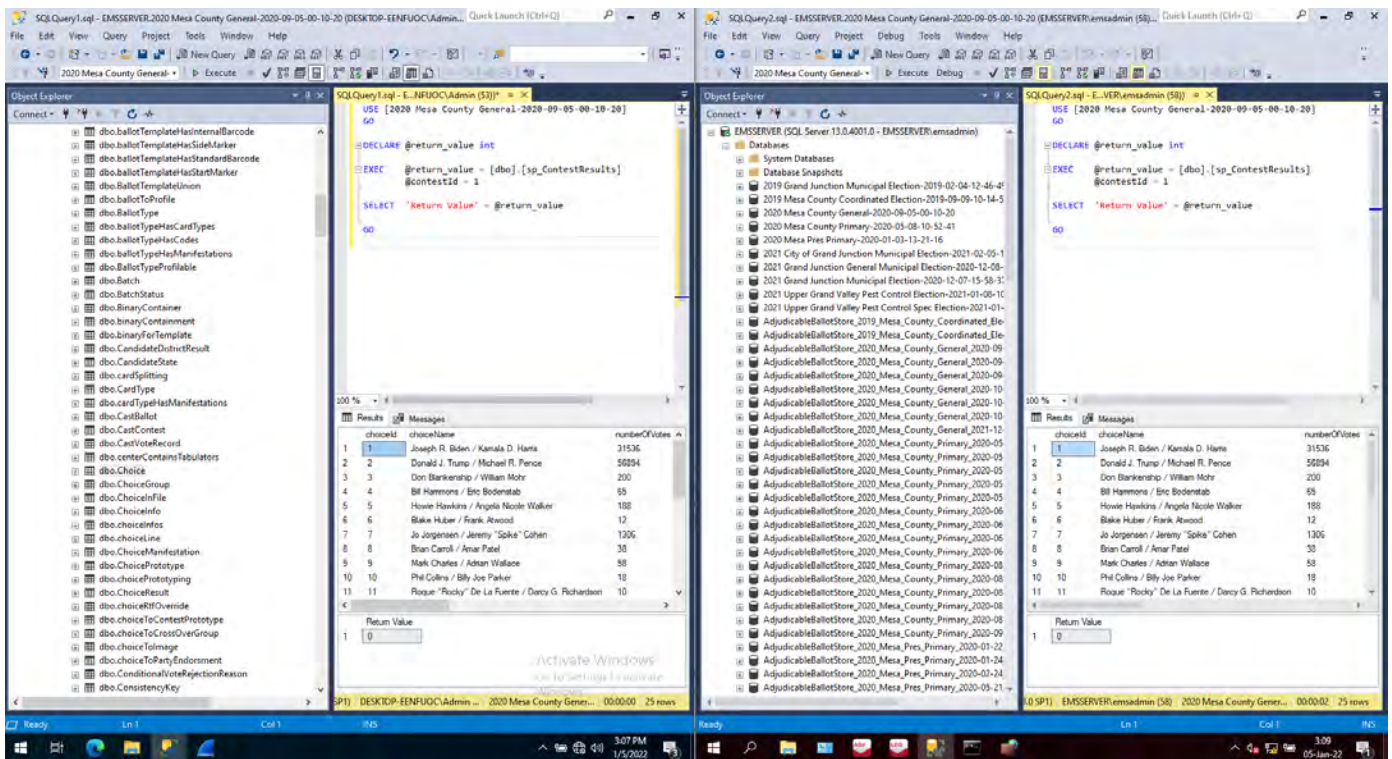


Figure 50 - The vote choice was remotely changed back to its original state

The alterations of the vote totals in the election database on the EMS server also succeeded from a separate computer not part of the DVS D-Suite system. Queries were executed both from the Test Workstation and on the EMS server, and both results again show that it is possible by anyone with physical access to a Dominion Computer or any part of the voting system network to alter the entire election result on the EMS server by changing only two values, with knowledge nearly anyone could attain by using Google and watching one or more YouTube videos.

The query is run on both systems to show that the database results have changed back.

Finding 6: The Mesa County EMS server containing the 2020 General Election vote results has been shown to be insecure and grossly misconfigured such that it allows unrestricted access to the election database and enables changing calculated vote totals from a separate computer not part of the DVS D-Suite system with nothing more than the knowledge of a password. It was possible to access the EMS server and, by changing only 2 numbers in the database, completely alter the election results in Mesa County for the 2020 Presidential election.

EXAMINATION RESULT 2:

The election results database CAN be altered by any person using a non-DVS D-Suite computer directly or indirectly connected to the EMS server network.

EXAMINATION OBJECTIVE 3:

Determine whether the calculated vote totals of an election can be altered by any person using a cell phone or mobile device wirelessly connected to the EMS server network.

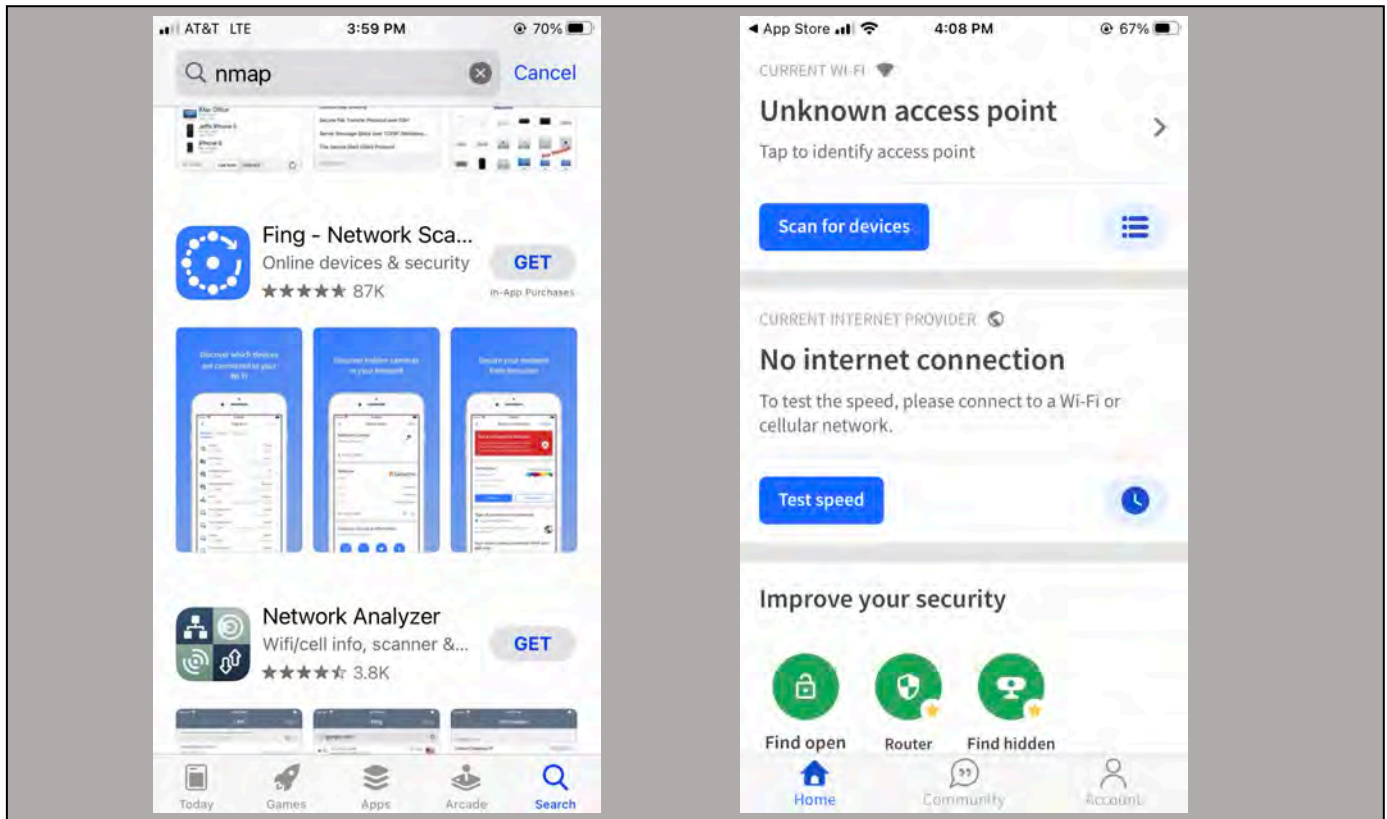


Figure 51 - Network scanner installed on cellphone

An iPhone was connected to the same network, wirelessly, using a common wireless router purchased at a retail store. A router such as this could be plugged in and hidden anywhere on the DVS D-Suite network, or the same functionality could be inserted electronically via common hacking into any device on the network with a wireless card, including network printers and network scanners. As discussed earlier, thirty-five (35) devices of the existing DVS-supplied equipment already had a built-in wireless card or device installed, as well as a wireless-capable printer, so this could have easily been done without attaching any devices outside the system components. The Apple App Store was searched and a common network scanner 'Fing' was easily found. As one can see, 'Fing' has already been downloaded over 87,000 times. In the image on the right, 'Fing' was run and the option 'Scan for Devices' was selected.

Previously an Island-Hopping attack was described. For such an attack to occur, a connection to a different network is used.

This part of the examination was carried out to determine whether the system could have been accessed wirelessly using the more limited capabilities of a mobile device (a cell phone in this test). Thirty-five (35) wireless devices were identified within the Mesa County DVS D-Suite system. In order to perform this part

of the examination it was necessary to mimic the actual MESA hardware, so a wireless access point was connected to the VirtualBox test system that was running the actual software of the Mesa County EMS server via a host-based network interface card.

If any wireless device gains access to any device connected to the EMS infrastructure (as was demonstrated here), including the inadvertent enabling of even a laptop wireless interface (typically performed by a single button press on the keyboard of a laptop, or by preprogrammed, triggered activation of internal code on the device, or by remote command from an actor with access to the device), such an attack could easily occur.

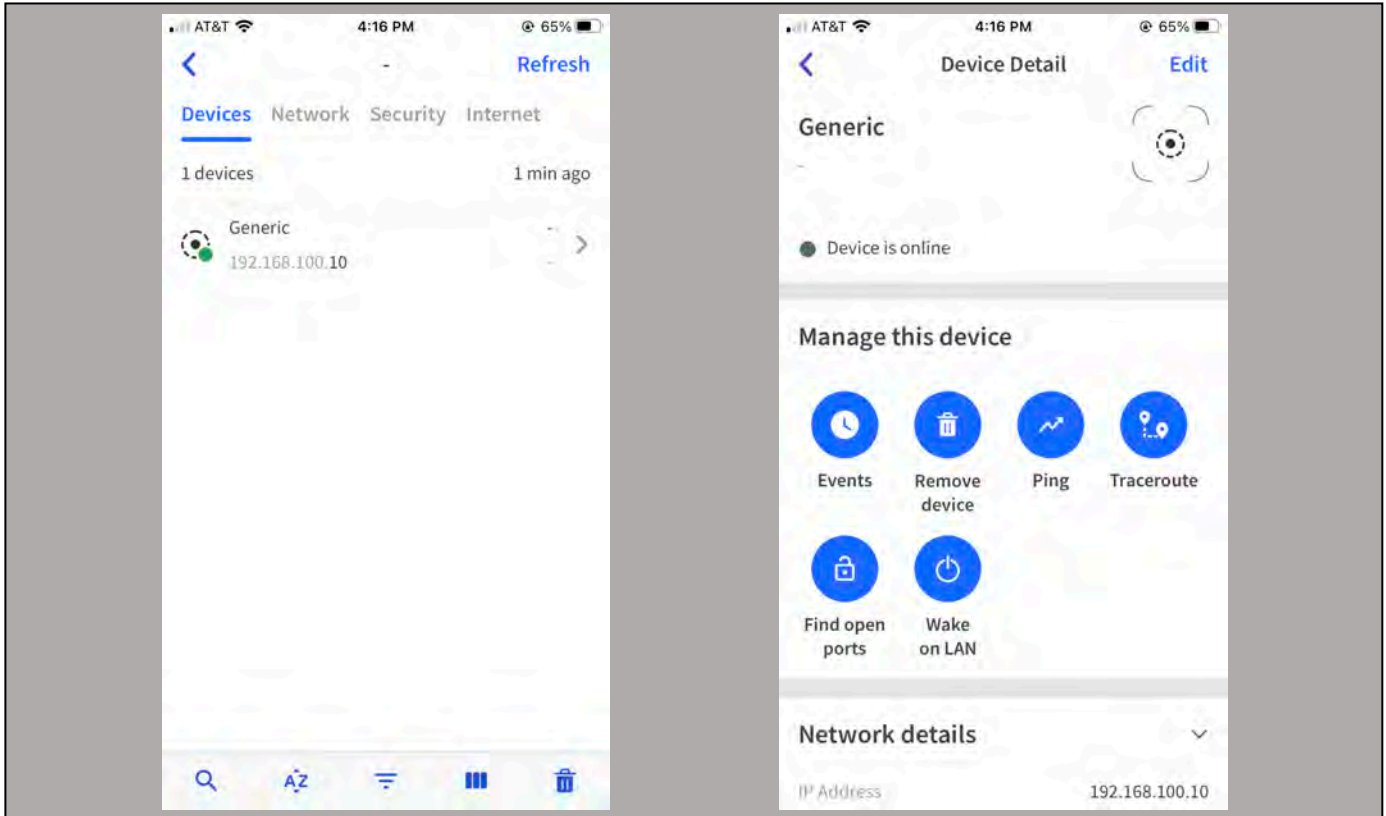


Figure 52 - IP address for the EMS server found via wireless connection and iPhone app

On the left, the network scanner immediately finds the IP address for the EMS Server and displays the IP address (192.168.100.10). The device is selected, and on the right, the phone app presents more options. I then selected "Find open ports."

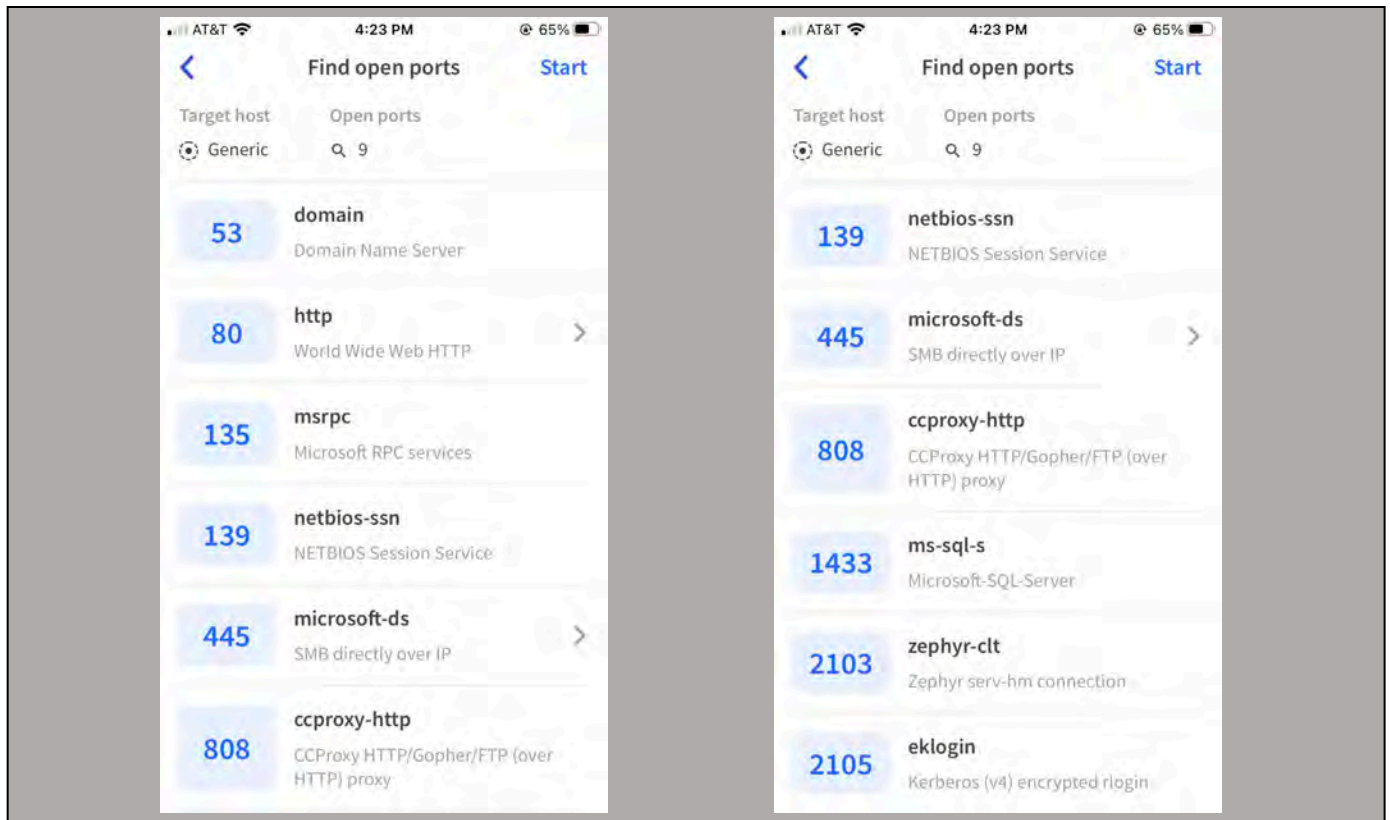


Figure 53 - Scanner Results

The iPhone app lists all the ports that it sees open on the EMS server. Port “1433”, which the app indicates is associated with “Microsoft-SQL-Server,” is immediately detected.

In Figure 53, left, one can see the first 6 of the 9 open ports on the EMS server with a wireless access point connected. On the right, scrolling down the screen reveals the remainder of the 9 open ports identified. The SQL service port, 1433, has been identified as operating and configured on this device.

Using the method recommended by CIS (Nmap⁷¹), a device that offers the Microsoft SQL Service has been identified. This uses standard networking software that many IT professionals and most IT Security professionals are very familiar with.

Whether such an exploitation of technology is performed with the single-response ping command or by using a more powerful tool like Nmap, the discovery of a network connected device on the same network segment has been accomplished.

⁷¹ Network Mapper (Nmap) is a tool for network exploration or security auditing, frequently used by cybersecurity penetration testers to find live / operating devices and hosts on networks, perform port scanning, detect operating systems and versions in use, and ping networks and subnetworks to diagram potential and available communication paths.

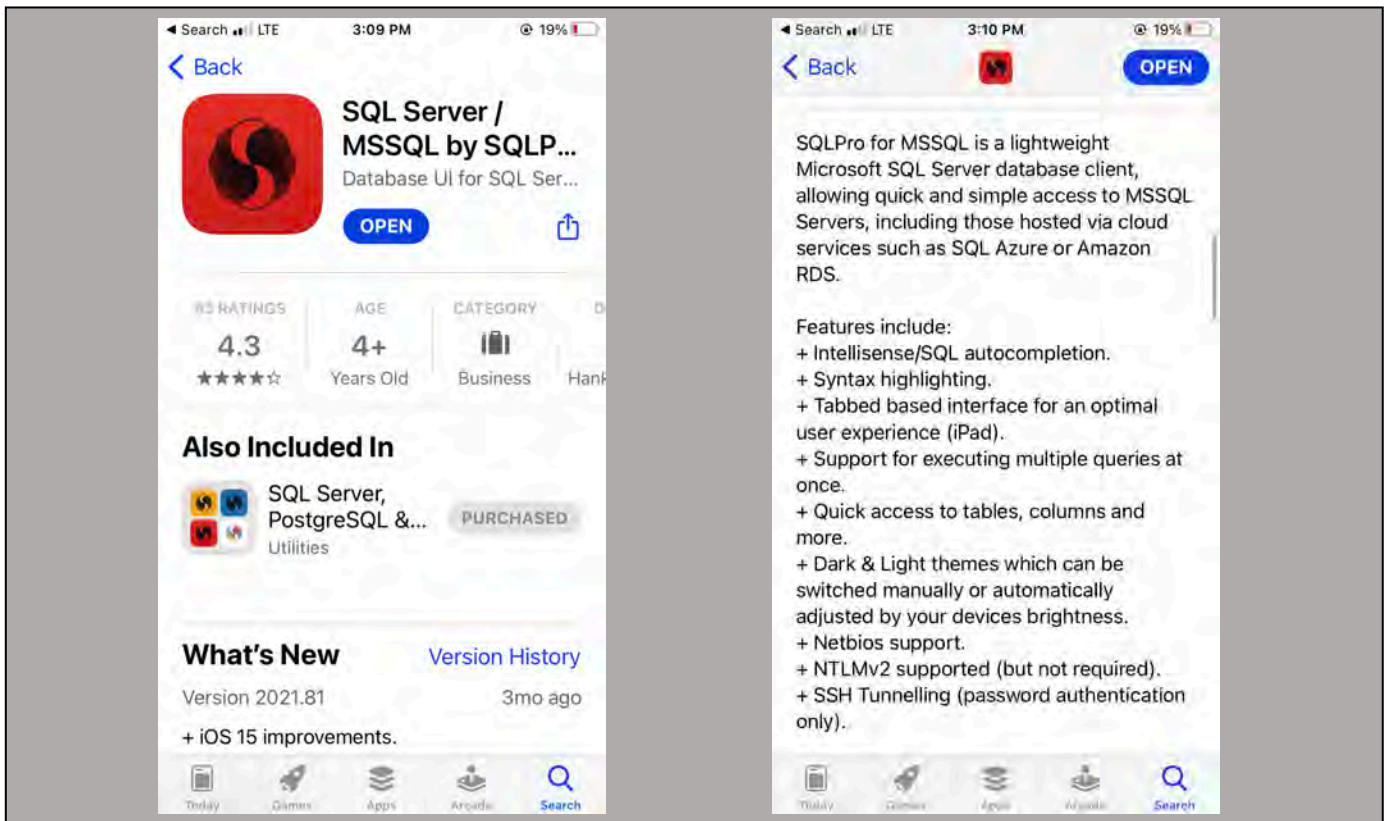


Figure 54 - SQL Access Functionality

Returning to the Apple App Store, a search for 'SQL Server' finds another app, 'SQL Server by SQLPro'. The description shows that it is a Microsoft SQL Server database client.

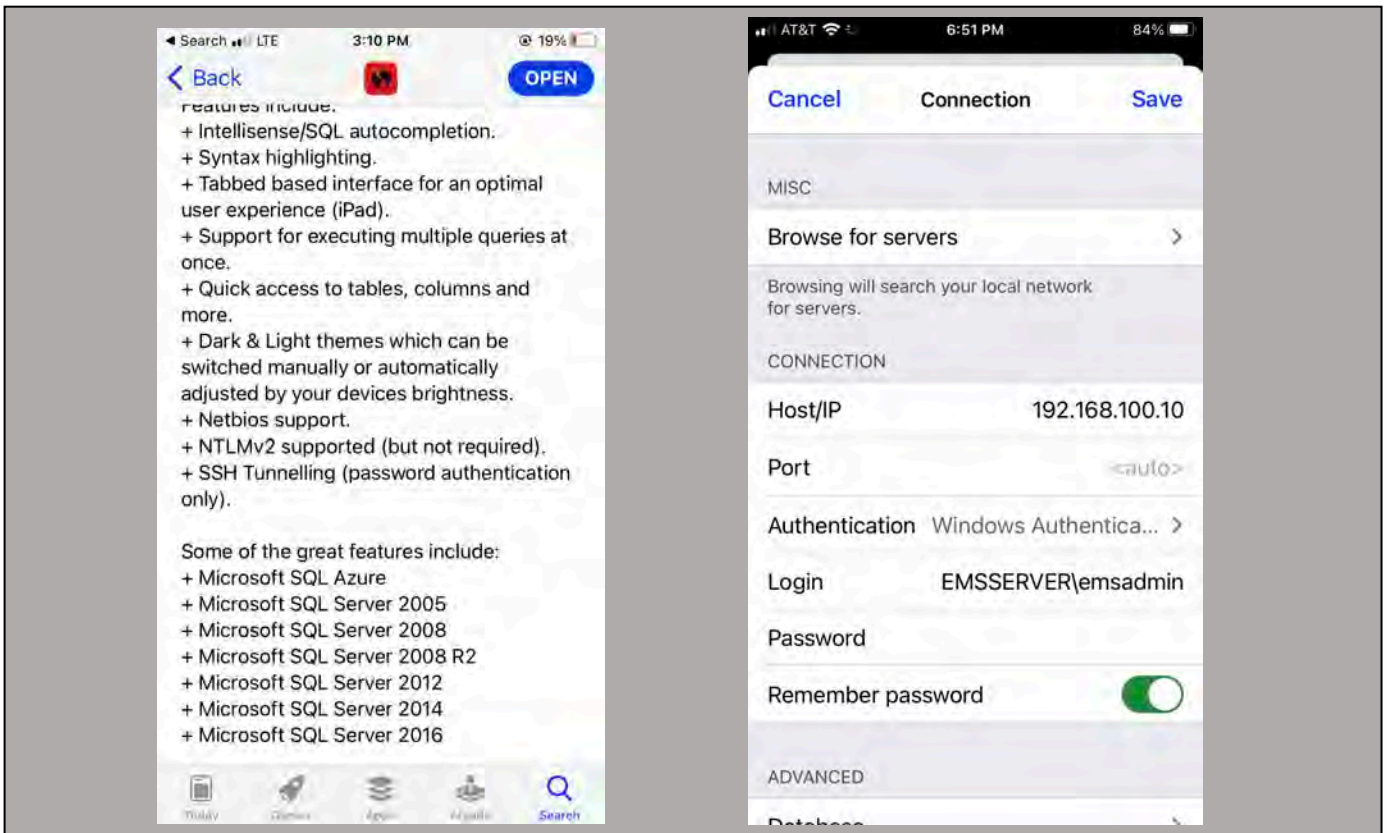


Figure 55 - SQL Pro Capabilities

On the left, the app description shows that it supports Microsoft SQL Server 2016, which is the exact version used by the EMS server. On the right, we use the same IP address, username, and password applied from the iPhone app as previously used to access the EMS server, physically sitting in front of its screen.

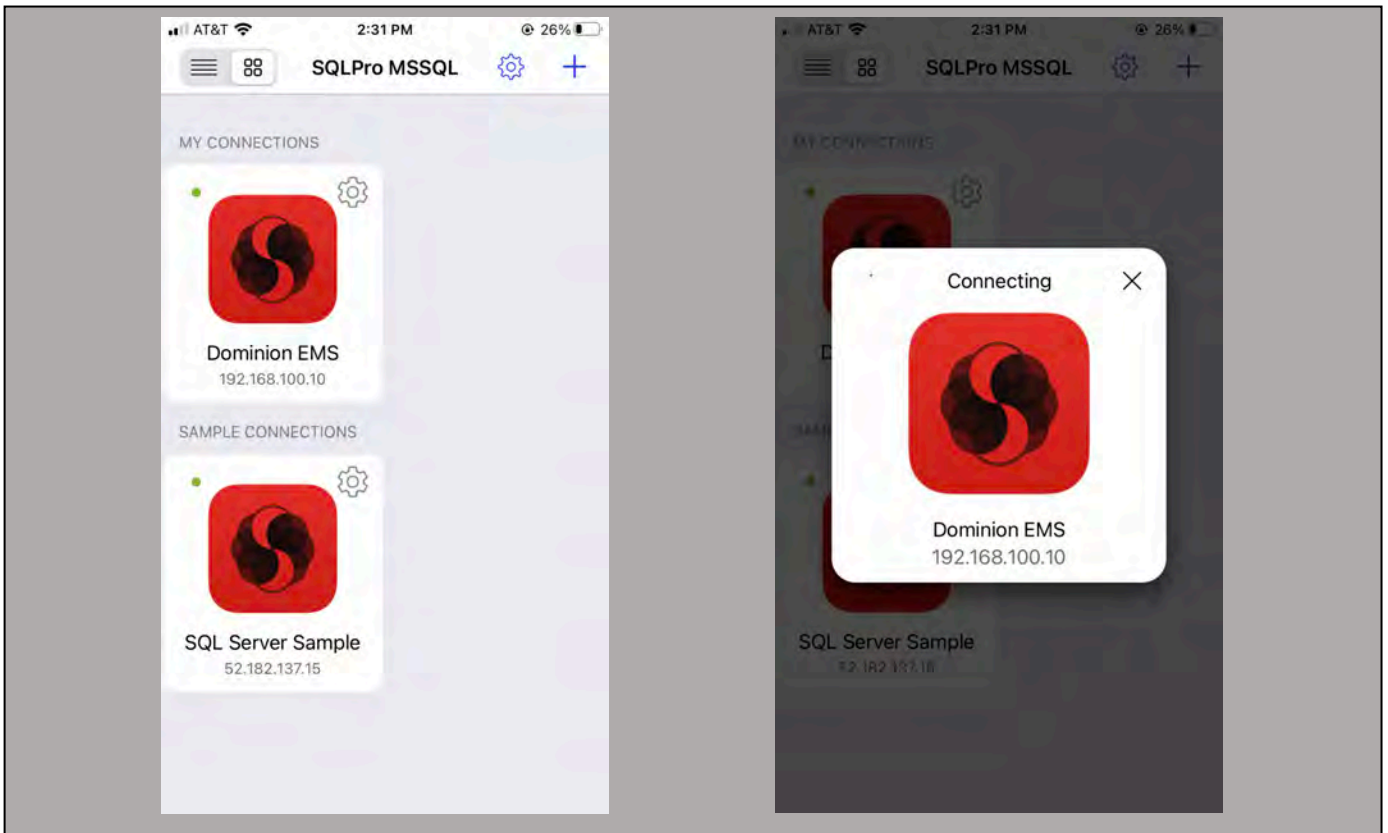


Figure 56 - Making an SQL Connection

The left image shows the configured connection to the EMS server. The right image shows the iPhone connecting directly to the database on the EMS server.

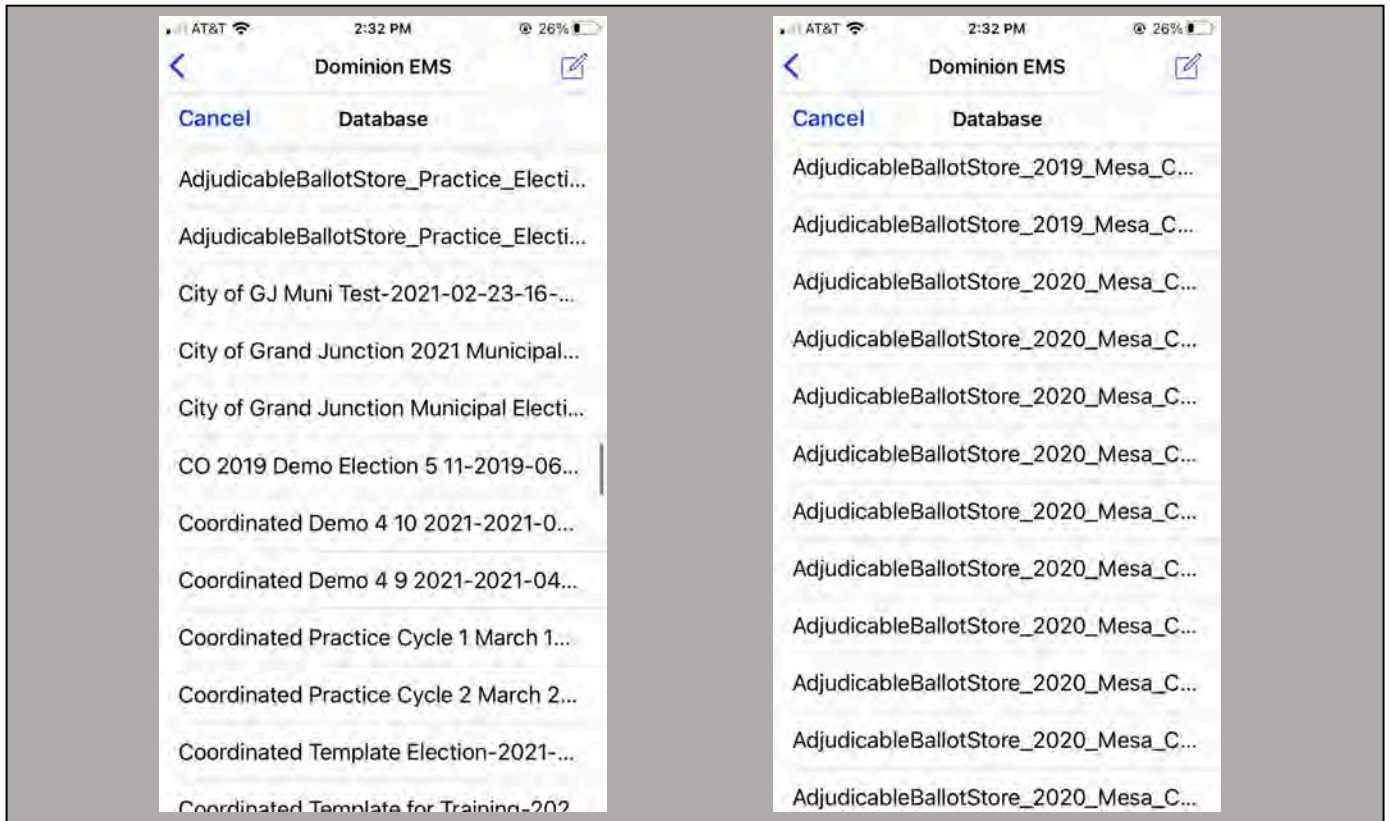


Figure 57 - iPhone Connection to Dominion EMS Database

After a second, the app lists all the voting system databases, just like it did on both the EMS server and on the Test Workstation.

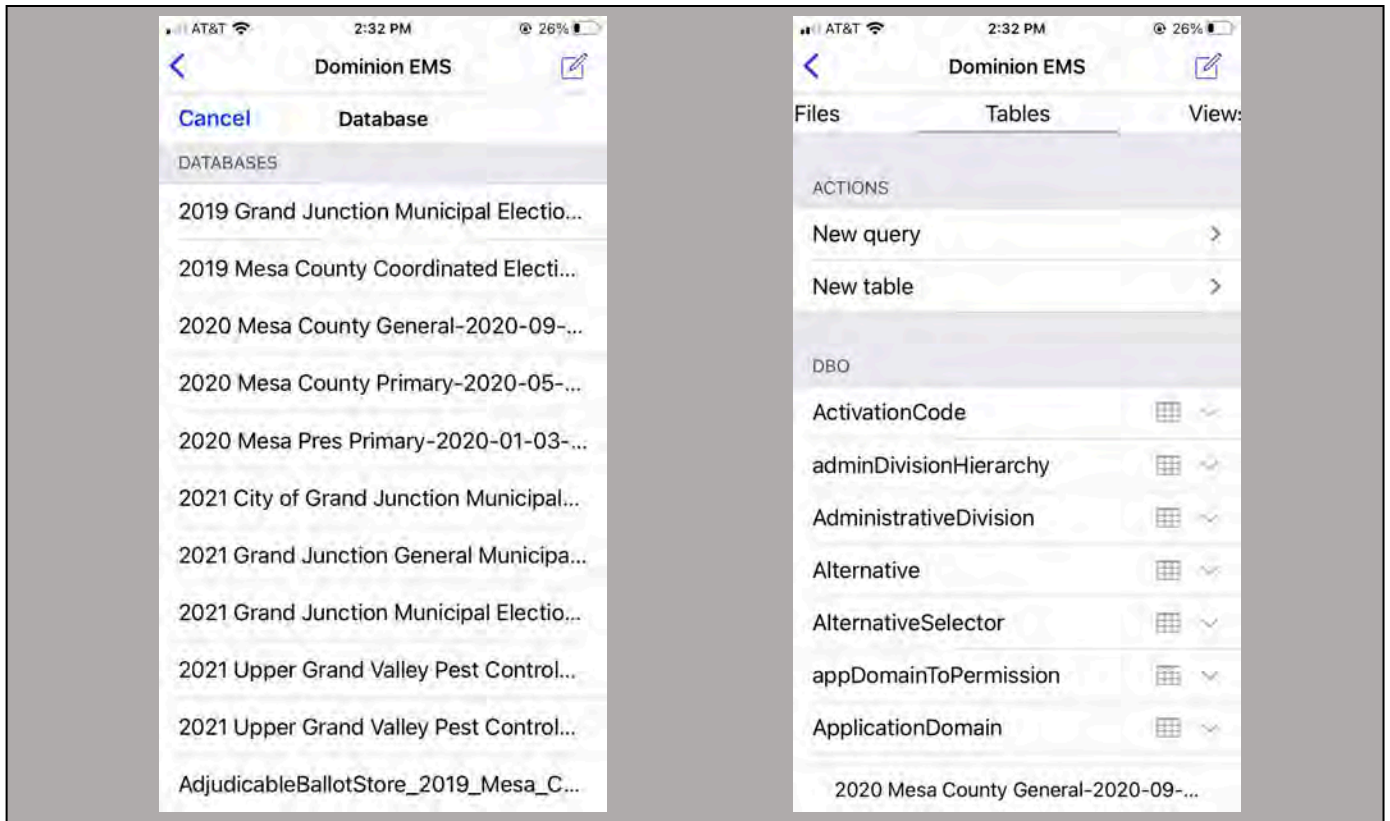


Figure 58 - Databases listing, Continued

Multiple Tabulation Store databases are shown on the left. Next, the 2020 Mesa County General election was chosen from the top of the list, and the image on the right shows the resulting screen, listing the tables in that particular database. So far, the examiner has not been denied access or even experienced a warning of any kind.

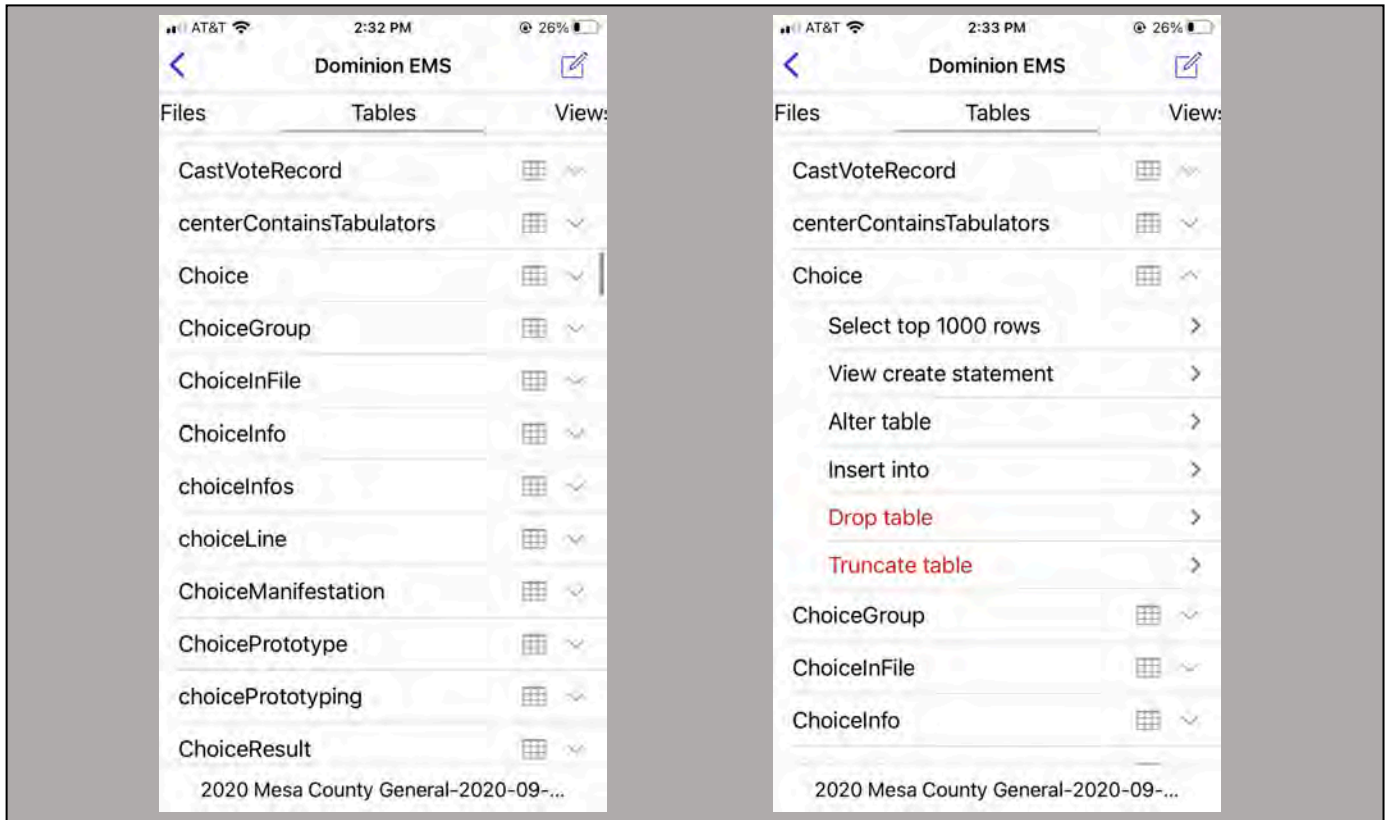


Figure 59 - Database Table Listing

On the left, one sees the same 'Choice' table as was seen on the EMS server and Test Workstation (where it was called 'dbo.Choice'). On the right, 'Choice' table is selected resulting in the options as shown. I selected 'Select top 1000 rows'.

Note that the "drop table" command would delete the table entirely, while the "truncate table" command would shorten the table, and if applied to a table containing actual vote data, would delete some of those votes.

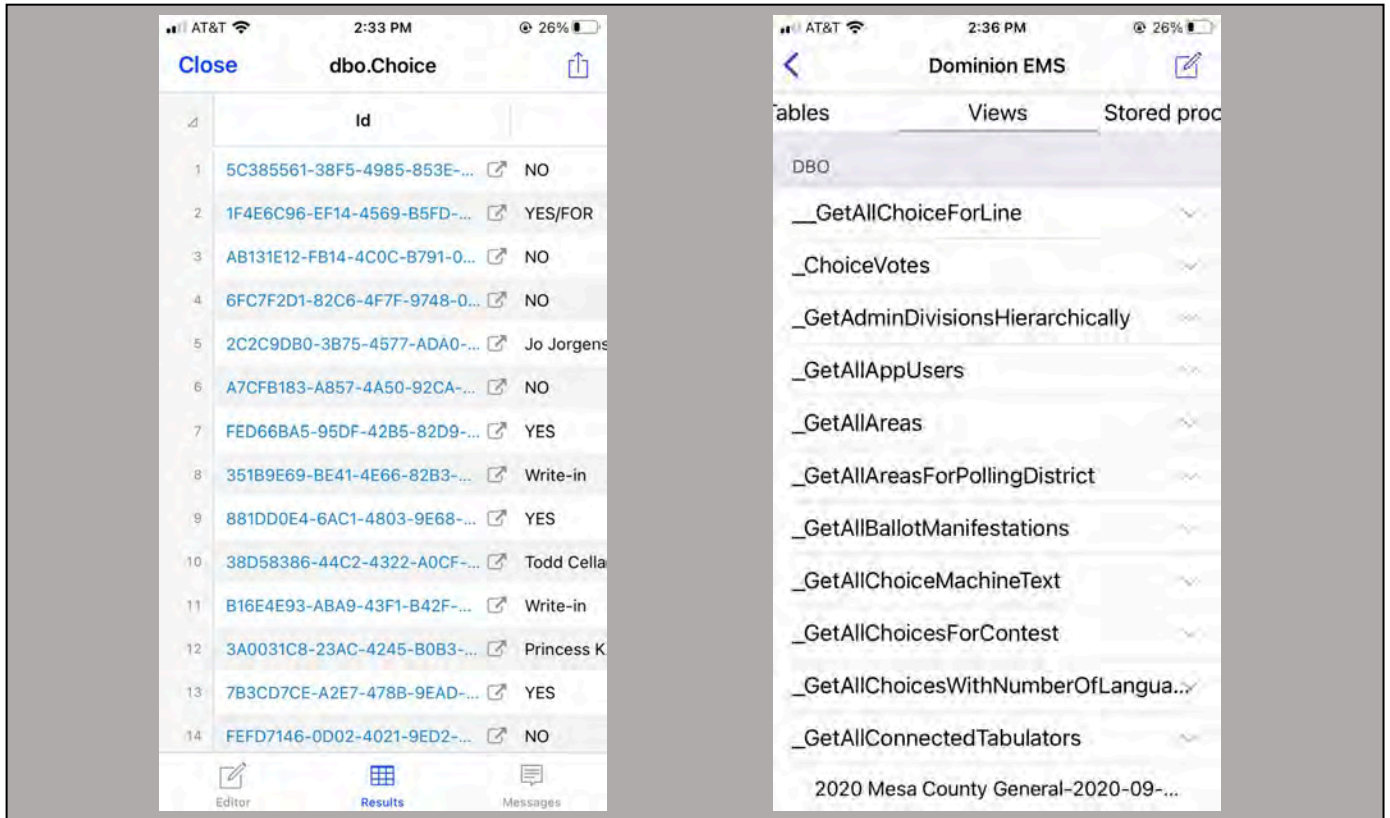


Figure 60 - Database Access

On the left, one sees the top 177 rows in the 2020 Mesa County General database, along with the choices listed as shown by both the EMS server and the Test Workstation. One the right, 'Views' at the top menu was then selected to pull up the database views from the EMS server.

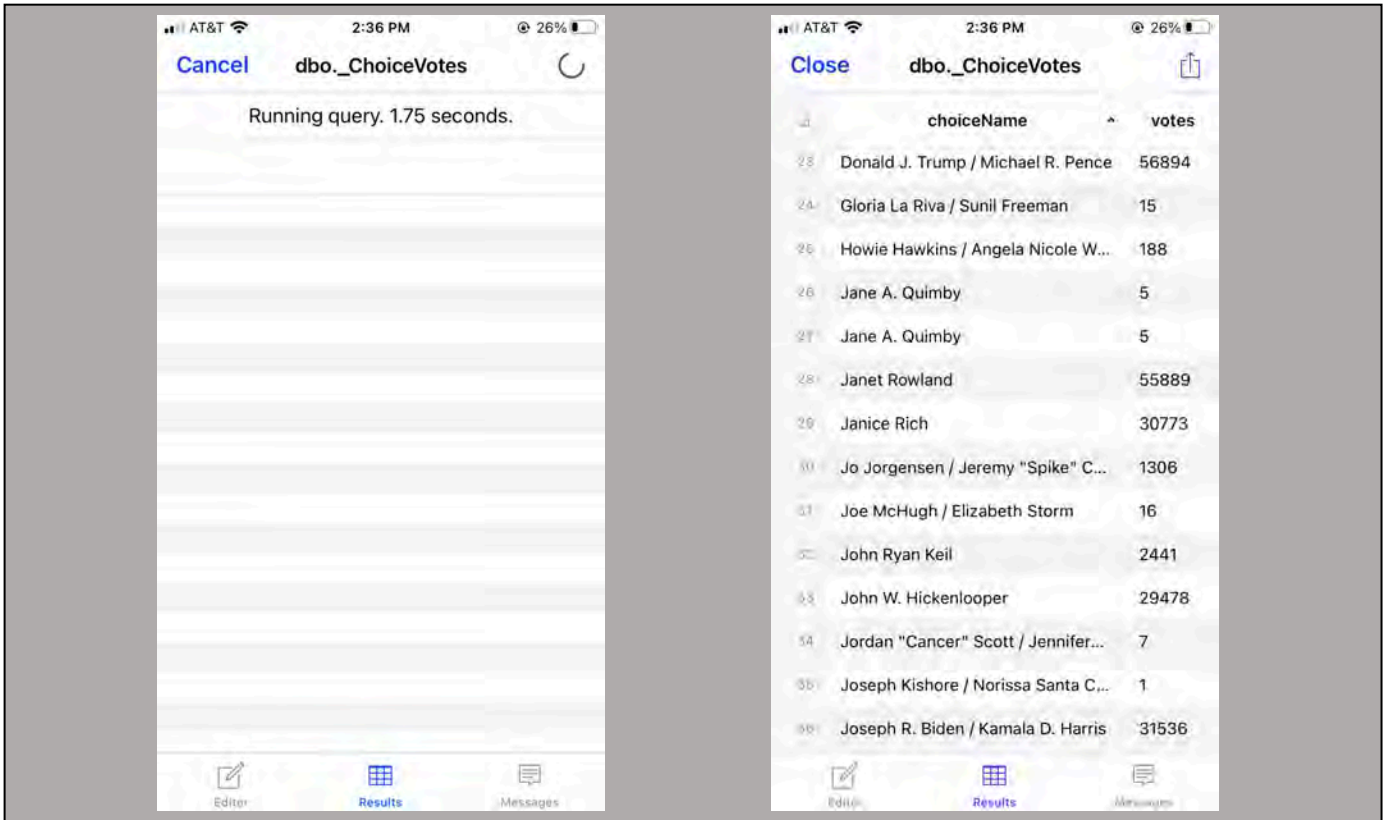


Figure 61 - Executing a Database Query

The `_ChoiceVotes` view was selected. On the left, one sees that it took 1.75 seconds to pull up all the votes for each choice in the election. The result of that query is shown on the right.

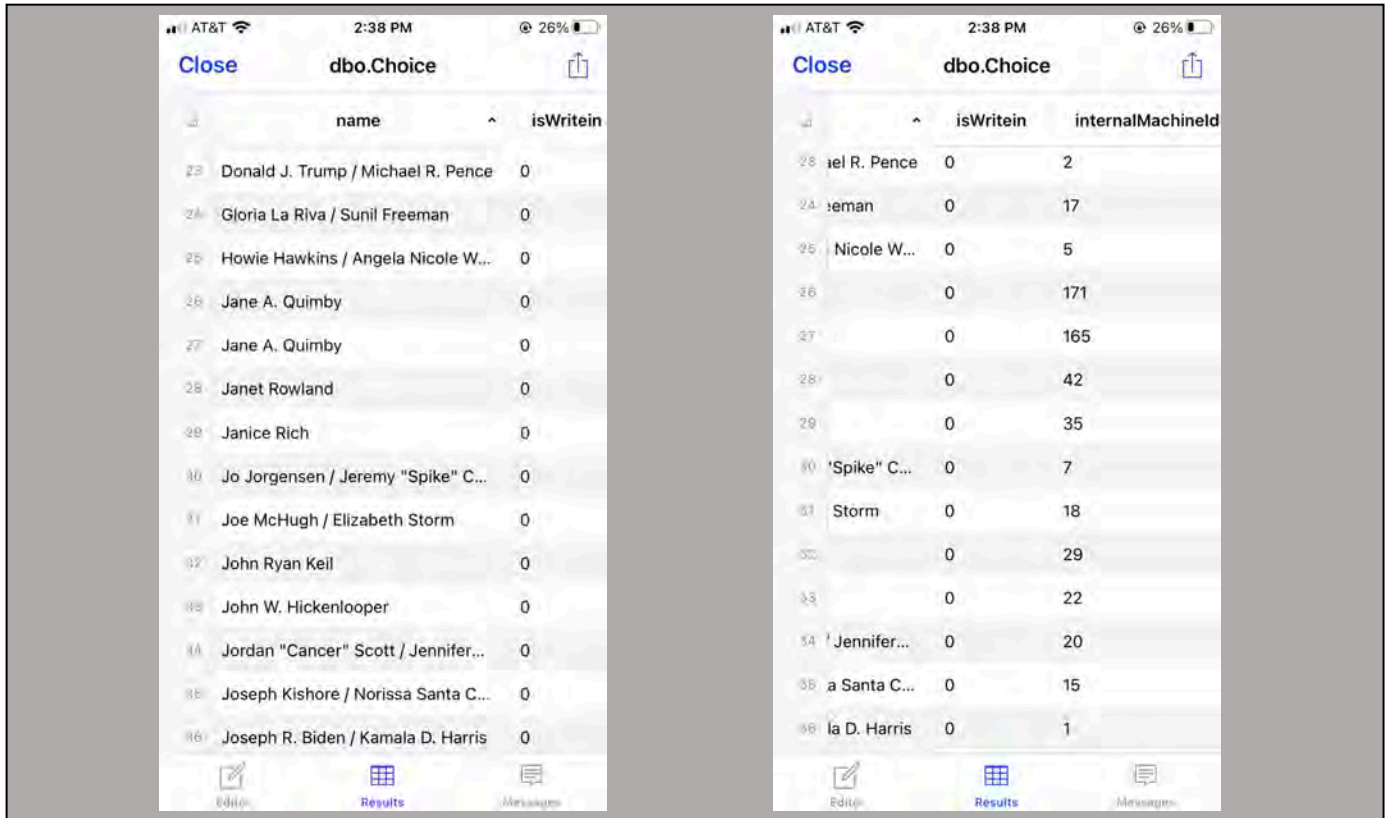


Figure 62 - Table Data

The left and right images demonstrate the effect of scrolling to the right, to display all the columns. All the columns in this table can be viewed without being denied or without any type of warning.



Figure 63 - A script to change the vote data

The left image shows the default query that asks for the SQL Server to send the top 1000 rows from the `dbo.Choice` table. The instructions on the image on the right were then typed in. What they do is very simple: They update the `Choice` table by setting the `internalMachineId` to '1' for 'Donald J. Trump / Michael R. Pence,' and setting the `internalMachineId` to '2' for the entry with 'Joseph R. Biden / Kamala D. Harris' in it. This is the same type of change that was made by hand on both the EMS server and the Test Workstation earlier in this report.

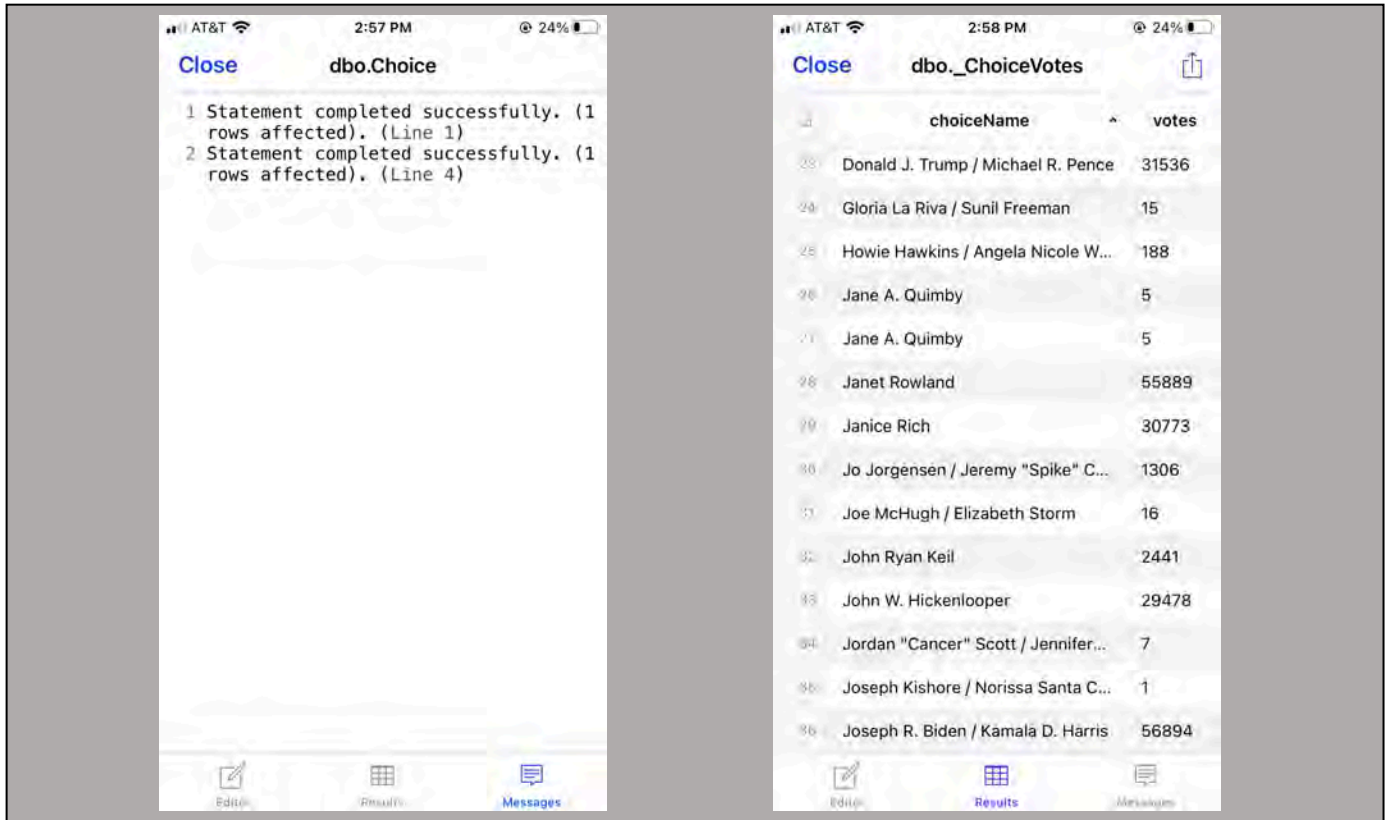


Figure 64 - Script Results

The image on the left shows the typed instructions were executed and the EMS server reported that each instruction was completed successfully, affecting one row each. On the right, the `_ChoiceVotes` view is run again to see that once again the election results were flipped from Trump to Biden, using a basic iPhone with an app downloaded from the App Store that anyone could install and use.

EXAMINATION RESULT 3:

The calculated vote totals in an EMS server database can be altered by any person using the more limited capabilities of a mobile device wirelessly connected to the EMS server network.

For the iPhone test, while a wireless device was added to the network to allow this demonstration to occur, it's alarming that's all it took to accomplish this, especially since thirty-six devices in the Mesa DVS hardware had wireless cards installed. Anyone could purchase a wireless device like this online or at most computer or office supply stores, attach it inside the voting center, and use one of the easy to guess or well-known passwords on the system (or obtain it from the Darkweb,⁷² or access the iDRAC remote control server, or use DVS-published default passwords, etc.), could sit out in the parking lot and change any part of the database before, during, or after an election. More dangerous, since thirty-six devices in the DVS D-Suite System were configured with a wireless card, the same abuse could be committed by someone with basic computer networking skills,⁷³ given wireless access to the EMS server is completely insecure, exposed to access, protected by only a Windows password, despite many additional protections being available. As an example, a Dell Wireless 1560 internal wireless adapter was identified in the specified configuration on the DVS D-Suite ImageCast Voter Activation (ICVA) computer that is part of the Mesa County DVS D-Suite system. A skilled individual could easily get away with this same unauthorized access and much more with almost any modern cell Phone, iPhone or Android, Mac, or PC. Wireless capability is very small today, easily fitting inside a small USB device, which could even be inserted in an internal port, invisible to County officials, allowing for the surreptitious connection of the capability in such a manner that only highly trained specialists would be able to find it. Figure 65 depicts such a miniaturized wireless USB device, which could be installed without notice on a motherboard of the type used by D-Suite EMS servers (shown).

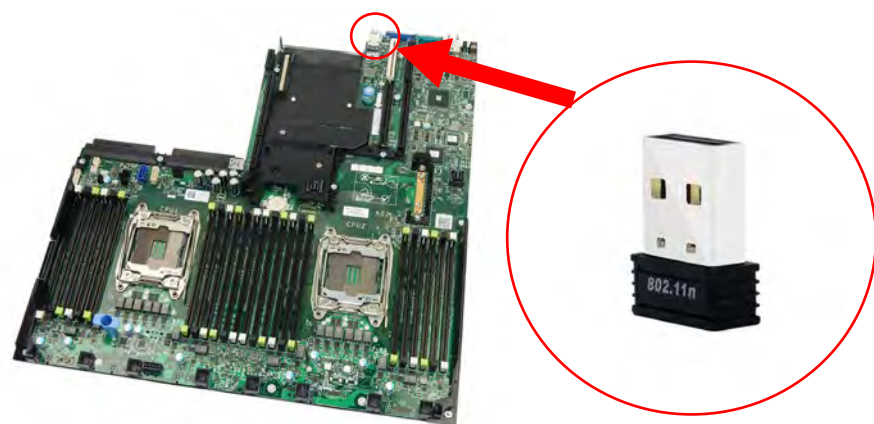


Figure 65 - Small Wireless Device Surreptitiously Installed (internally) on a Computer Motherboard

The result of this examination demonstrates that an attack is possible using a wireless device connected in any one of a multitude of ways. It was possible to perform network scanning using industry standard tools on a common Apple iPhone.

It must be noted that the methods used here are well described in publicly-available, commonly-known literature. Cybersecurity industry guides⁷⁴ describe the Nmap application specifically to identify

⁷² The Darkweb is a clandestine, encrypted, anonymized webserver infrastructure characterized by extensive criminal activity including trafficking in computer access credentials (passwords) as well as many other criminal activities. Access to the Darkweb is only available through use of The Onion Router (TOR) which hides and renders untraceable (to most searches and searchers) the IP address and location of its users. Content on the Darkweb is hidden from the general Internet to facilitate criminal activity.

⁷³ <https://papers.mathyvanhoef.com/ccs2017.pdf>, <http://www.krackattacks.org/>

⁷⁴ <https://attack.mitre.org/techniques/T1046/>

connections to the network. Nmap uses the ICMP 'echo request' command, just as our previous check did using the 'ping' command. Nmap is capable of executing many echo requests in parallel to more rapidly identify the devices connected to a network than the single-request ping program can, and Nmap tests all of the port numbers configured to be tested, for each IP address being tested.

The report in this examination does not reveal any secret tradecraft, or compromise election security; the techniques used in this examination are common among IT professionals. Unfortunately, there is very little security in this voting system, to begin with.

This examination demonstrates how the use of wireless networking can be easily exploited and documents the risk presented using one example. Given the ease with which it can be implemented if wireless devices are enabled (e.g., by an accidental button press on a laptop), it is important to acknowledge the risk so that future elections can be properly protected. To assure integrity of the infrastructure, computing devices with wireless network capability must not be used because wireless networking can be easily enabled by accident (or maliciously). Additionally, certification under VSS absolutely required steps to have been taken within the voting system design and implementation that secure the system from accidental or malicious connections to other networks. The fact that these steps were not taken casts doubt on the credibility and competence of the vendor, the certification authority, the certification testing lab, and the institutions responsible for the testing lab accreditation program.

Making use of the broadband modem inside the cell phone, it may be possible to create a connection from the internet directly into the electronic voting system, bypassing all County firewalls and security, allowing someone to command and control it from anywhere in the world.

This would be completely undetectable by election officials, and most, if not all forensic experts.

While critics may assert that it has not yet been proven that any wireless device was connected to the Mesa County systems and operating prior, during, or after the election, the fact is that wireless devices were installed in Mesa County DVS systems, and critics cannot prove those devices were not operating and exploited. The required compliance standards were created explicitly to provide such proof, yet the features that enable compliance were disabled. Due to the illegal disabling of logging mechanisms, configured overwriting of logs, and the failure to preserve the log data (in violation of the law) that would either show tampering and fraud or support claims of the integrity of the election, it cannot be proven that the election was free of intrusion and tampering (See Report #1).

CONCLUSION

An ongoing forensic examination of the Mesa County EMS server, version 5.11-CO, provided by DVS revealed the overwriting of critical log data and election records, the misconfiguration of logging functions, and the failure to preserve required election records in Report #1.

In this Report #2, the examination has conclusively shown and demonstrated the ability to access election records from a separate computer, not part of the DVS D-Suite system, the ability to edit the election database, and the ability to change calculated vote totals to alter the election results on the Mesa County EMS server entirely, “flipping” the winner of an election contest in the jurisdiction from one candidate to another.

The Key Objectives for this report were answered by this examination:

1. To determine whether D-Suite-implemented security requirements comply with the 2002 Voting System Standards (VSS)
 - a. Uncertified software was used on the system rendering the certification of the entire system and all elections conducted with it, Invalid.
 - b. Security protections required by law were almost completely absent
 - i. Other than a userID and an easily guessed or bypassed password, no authentication was required
 - ii. The firewall rule for access to the election database, ballots and results was unrestricted to any IP address in the world
 - iii. Together with the firewall rule, Microsoft SQL Server Management Studio (SSMS) enabled complete access to the entire election databases – not just to the 2020 election but to the elections of June 2019 through May 25, 2021.
 - iv. A self-signed encryption certificate was used introducing the potential for a man-in-the-middle attack
 - v. Thirty-five wireless devices (802.11, Wi-Fi) were installed inside election equipment and an additional wireless device was identified in a connected printer
 - vi. Any or all of these wireless devices could have connected to the Internet via the building wireless facilities
 - vii. “Purging” (deletion) of critical Audit Log data, as specified by DVS and directed by the Secretary of State⁷⁵, destroyed all records of connection to the Internet or elsewhere, all record of user activity, including programs run by these users, errors, and any record of the addition or deletion of votes and the alteration of election results.
 - c. **EACH of the compliance failures identified in 1.a. and 1.b. above are clear violations of the law.**

⁷⁵ The TDP associated with the “trusted build” process is promulgated by the Secretary of State. CRS 1-5-620 States that the vendor provides manuals and documentation and that any information not on file with and approved by the Secretary of State shall not be used in an election.

2. To determine whether the results of an election, stored on the EMS server, can be altered by any person with physical access to the logged-in EMS server,
 - a. **Any person with physical access to the logged-in EMS server can change the calculated vote totals on the EMS server.**
3. To determine whether the results of an election stored on the EMS server, can be altered by any person using even a non-Dominion computer directly or indirectly connected to the EMS server network.
 - a. **Any person using even a non-DVS computer directly or indirectly connected to the EMS server network can change the calculated vote totals on the EMS server.**
4. To determine whether the results of an election stored on the EMS server, can be altered by any person using a device such as a cell phone wirelessly connected to the EMS server network.
 - a. **Any person using a device such as a cell phone wirelessly connected to the EMS server network can change the calculated vote totals on the EMS server.**

Examination of wireless vulnerability required that a wireless device be connected to the EMS server network and demonstrated that such a device when connected is capable of allowing uncontrolled access to and alteration of an election database on the EMS server.

The purpose and the finding of Key Objective 4 demonstrates that if such a wireless device were connected to the EMS server network, the election results can be accessed and altered surreptitiously. The ease with which wireless technology can be enabled, even by accident, presents an unacceptable risk to critical infrastructure voting systems, especially when combined with the egregious violations of the VSS and the multiple security failures found in this examination. **Wireless encryption is easy to break,⁷⁶ has been broken, documented and demonstrated online.⁷⁷**

The disabling and mis-configuration of numerous security measures as found in this Examination renders this EMS election system unsafe and utterly insecure. Unauthorized software, multiple violations of VSS and consequently Colorado law and the use of an un-accredited testing laboratory made the certification of this system, and its subsequent use in elections, illegal.

The on-going examination found that security provisions on the election equipment were not restricted by IP address but rather the firewall configuration was programmed to allow any IP address from anywhere in the entire World to access the election records with no more than a single and relatively simple password to protect it.

There is nothing secret or novel about the techniques used to demonstrate direct access, access by a non-DVS computer or iPhone access to the election databases. Software accessible to hundreds of millions of people and openly advertised for free download and use was used to demonstrate the extreme insecurity of the voting system.

⁷⁶ <http://cve.mitre.org/>, supra note 18

⁷⁷ <https://papers.mathyvanhoef.com/ccs2017.pdf>, <http://www.krackattacks.org/>

The reason for the insecure configuration of these critical infrastructure-designated voting systems, in contradiction to the vendor's claims⁷⁸ and the Secretary of State's certification, should be determined through appropriate investigation.

The law requires the retention of election records including system logs but this election system is grossly out of compliance with the law. Combined with the overwriting of log files, the systematic disabling of critical logging and numerous security elements disabled or bypassed, creating a "back-door" for malicious actors, this configuration of the Mesa County, Colorado voting system assures that may not be possible to prove the integrity of any election in which this equipment was used. This voting system is not compliant with the law, should never have been used in an election, and cannot be trusted to provide authenticated, reliable election data in any election.

Nearly every point of examination has revealed the most serious deficiencies in both security and configuration.

The claim that "election systems were not connected to the Internet" has been made, however the use of removable media devices, presence of wireless networking components within DVS components, use of the internet for election results reporting and other functions, and the destruction of and non-retention of critical logs prevent the verification that the system was not connected to the internet. The configuration of logging to ensure overwriting of log data resulted in operating system logs not being retained that may have shown any improper activity, had it occurred. Because of this it is not possible, on the basis of election systems log files (that are required to be retained), to prove election tampering or election integrity.

This failure of the voting system to retain log files that could prove election integrity is a most serious violation of certification requirements. The voting system, having not met election certification requirements, could not have been legally authorized for use in an election.

This report has detailed the following critical discoveries in Mesa County's voting system:

- **Uncertified software installed, rendering the voting system unlawful for use in elections.**
- **Does not meet statutorily mandated Voting System Standards (VSS) and could not have been lawfully certified for purchase or use.**
- **Suffered systematic deletion of election records (audit log files required by Federal and State law to be generated and maintained), which, in combination with other issues revealed in this report, creates an unauditible "back door" into the election system.**
- **Violates Voting Systems Standards ("VSS") which expressly mandate prevention of the ability to "change calculated vote totals." This report documents this non-compliance from the logged-in EMS server, from a non-DVS computer with network access, and from a cell phone (which may be possible if any of the 36 internal wireless devices in voting system components are deliberately or accidentally enabled and a password is obtained).**
- **Mandatory VSS "System auditability" required features are disabled.**
- **Is configured with 36 wireless devices, which represent an extreme and unnecessary vulnerability, and which may be exploited to obtain unauthorized access from external devices, networks, and the Internet.**

⁷⁸ See Appendix A. Compliance Requirements.

- **Is configured through firewall settings to allow any computer in the world to connect to the EMS server.**
- **Uses only a Windows password with generic userIDs to restrict and control access.**
- **contains user accounts with administrative access that share passwords, subverting VSS-required user accountability and action traceability controls.**
- **Uses a self-signed encryption certificate which exposes the system to the risk of undetected compromise or alteration.**

This report does not compromise state secrets or election integrity – that has already been done by these multiple violations of law, multiple failures of the vendor, the Voting System Testing Lab and the Secretary of State’s improper certification. Nation-state adversaries already know these vulnerabilities exist; it is only the American people that are unaware. No new vulnerabilities are discovered or disclosed in this report; all of them are previously well known in the industry and to professionals.

Immediately pending elections and the complete lack of election integrity presented by this voting system present an extreme danger to our constitutional republic. With elections beginning on a large scale very soon, with the massive security vulnerabilities, the weakness presented by this uncertifiable Voting System, the abject failure of the Voting System Testing Laboratory with expired accreditation and lack of proper oversight by authorities, remediation of these issues before pending elections is not possible.

This DVS election system has been shown non-compliant with the law and has been shown to be uncertifiable. The use of this system in an election was itself a breach of law, and more importantly a breach of public trust with reckless disregard for the right of a free people to choose their government.

APPENDIX A. COMPLIANCE REQUIREMENTS

Standards for election systems are provided by the Federal Election Commission Voting Systems Standards (VSS) and in Colorado, compliance is required with this standard.

The VSS requires access control to prevent or detect access to election systems, ensure that system functions are executable only in the intended manner and order, provide safeguards to prevent tampering, record and report the date and time of normal and abnormal events, maintain a permanent record of all audit data that cannot be modified or overridden, detect and record every event including an error condition that the system cannot overcome, time-dependent or programmed events that occur without the intervention of the voter or a polling place operator, and to protect the system from intentional manipulation and fraud, among many other requirements.

Federal Election Commission 2002 Voting Systems Standards (VSS)

Specific compliance requirements from the 2002 Voting Systems Standards (VSS) documentation are excerpted in this section. The Standards are contained in 2 volumes which together are several hundred pages long, and are published on the Federal Election Commission website as two PDF documents.

Excerpts in this Appendix are cited by VSS Volume, Section and Page number for reference in the first line of each box, followed by text of the VSS. Discussion of these standards follows outside each text box as appropriate.

APPLICABILITY

VSS V1, 1.6, page 1-13:

The Standards apply to all system hardware, software, telecommunications, and documentation intended for use to:

- Prepare the voting system for use in an election;
- Produce the appropriate ballot formats;
- Test that the voting system and ballot materials have been properly prepared and are ready for use;
- Record and count votes;
- Consolidate and report votes;
- Display results on-site or remotely; and
- Maintain and produce all audit information.

In general, the Standards define functional requirements and performance characteristics that can be assessed by a series of defined tests. Standards are mandatory requirements and are designated by use of the term “shall”.

All of these functional requirements are important. In this report we focus on aspects of recording and counting votes. Determination of whether the election management system performed with the accuracy and integrity required by these standards requires the audit information be maintained and preserved in accordance with law. The VSS is applicable the DVS D-Suite systems examined and reported upon in this document and in Report #1.

VSS V1, 2.1, page 2-19:

This section contains standards detailing the functional capabilities required of a voting system.

[...]

- Overall Capabilities: These functional capabilities apply throughout the election process. They include Security, accuracy, integrity, system auditability, election management system, vote tabulation, ballot counters, telecommunication and data retention.

The VSS is written specifying capabilities required at a high level. Detailed implementation methods are not specified but it is clear, for example, that these topics are not to be ignored.

VSS V1, 2.2, page 2-20:

This section defines required functional capabilities that are system-wide in nature and not unique to pre-voting, voting, and post-voting operations. All voting systems shall provide the following functional capabilities:

- Security;
- Accuracy;
- Error Recovery;
- Integrity;
- System auditability;
- Election management system;
- Accessibility;
- Vote tabulating;

The emphasis on all of these functional capabilities together indicates the serious nature of the requirement in this standard. The declaration by the U.S. Government that these systems are part of the national critical infrastructure further reinforces the importance of these capabilities. “Shall provide” indicates the mandatory nature of the requirement. The implementation of a functional security capability does not mean to apply the weakest possible implementation of security, for example.

DATA RETENTION

VSS V1, 2.2.11, page 2-34:

United States Code Title 42, Sections 1974 through 1974e, states that election administrators shall preserve for 22 months “all records and paper that come into (their) possession relating to an application, registration, payment of poll tax, or other act requisite to voting.” This retention requirement applies to systems that will be used at anytime for voting of candidates for Federal offices (e.g., Member of Congress, United States Senator, and/or Presidential Elector). Therefore, all systems shall provide for maintaining the integrity of voting and audit data during an election and for a period of 22 months thereafter.

[...]

The appropriate state or local authority must preserve all records that may be relevant to the detection and prosecution of federal civil rights or election crimes for the 22-month federal retention period, if the records were generated in connection with an election that was held in whole or in part to select federal candidates.

This requirement is clear. In discussion of retention of “all records that come into their possession” the burden of understanding what a record is, falls on election administrators. In particular this standard specifies that state or local authority must perform the preservation of all records.

Election Record Definition, Scope and Content

VSS V1, 4.4.3, page 4-84:

In-process audit records document system operations during diagnostic routines and the casting and tallying of ballots. At a minimum, the in-process audit records shall contain:

- a. Machine generated error and exception messages to demonstrate successful recovery. Examples include, but are not necessarily limited to:
 - 1) The source and disposition of system interrupts resulting in entry into exception handling routines;
 - 2) All messages generated by exception handlers;
 - 3) The identification code and number of occurrences for each hardware and software error or failure;
 - 4) Notification of system login or access errors, file access errors, and physical violations of security as they occur, and a summary record of these events after processing.

Other exception events such as power failures, failure of critical hardware component, data transmission errors, or other type of operating anomaly;

Documenting computer interrupts is a very detailed requirement, from a computer science perspective it is considered extreme. In normal operation, logs of computer activity typically do not include this level of detail unless the generation of records (logging) is set to the most verbose level for software debugging, because the volume of log data generated can be extreme. The specification that these records are

generated during diagnostic routines as well as during the counting and tallying of the vote, in the same sentence, is illuminating and indicates that the intention of the VSS is that this most extreme level of record be generated especially in the 4th example listed in this standard.

It is instructive to note that this standard specifically enumerates these requirements within the definition of a record, rather than in the section that specifically addresses security:

- System login;
- System access errors;
- File access errors; and
- Physical violations of security as they occur,

One reason that file access errors are included in this definition is that programming and operational errors can result in the creation of errors in stored data (that manifest in file access errors). Another reason is that intruders were well known at the time this standard was written and before, to attempt to destroy evidence of their activities by deleting audit trail records that might tend to incriminate them. Title 18, Sec. 1030 makes unauthorized access to such a computer system a felony.

In other election cases such as the Antrim, Michigan case it is notable that while records of previous elections were preserved and still on the election system, the audit records from the 2020 election were missing; the fact that records were generated and preserved previously but suddenly stopped during a specific event where malfeasance is suspected is significant and indicative of the practice by intruders to delete any record of their activity.

Astronomer Cliff Stoll became famous as an early computer crime investigator and published a book entitled “The Cuckoo’s Egg” in which he recognized that computers don’t make mistakes – programmers do. As a consequence, he looked at the very records regarding exception handling and errors that are required in this standard, because accounting software on the computer he managed as a grad student reported a 25-cent error in accounting data. Cliff’s curiosity and persistence resulted in the discovery of a computer attack where the intruder tried to delete audit records that resulted in the error. The investigation ultimately revealed international espionage and attacks against the US Government that would have gone unnoticed without his analytical search for what he initially assumed was a programming error. As a pattern of evidentiary finding, this history is very useful in understanding computer crime and criminal behavior.

This inclusion of these security-specific requirements in this basic but over-arching definition indicates their importance and that the intent of the standard is for great detail in the generation of these specific security audit records.

Security Requirements for Voting Systems

VSS V1, 6.1, page 6-93:

[...]

Ultimately, the objectives of the security standards for voting systems are:

- To establish and maintain controls that can ensure that accidents, inadvertent mistakes, and errors are minimized;
- To protect the system from intentional manipulation and fraud, and from malicious mischief;
- To identify fraudulent or erroneous changes to the system; and
- To protect secrecy in the voting process.

The Standards are intended to address a broad range of risks to the integrity of a voting system. While it is not possible to identify all potential risks, the Standards identify several types of risk that must be addressed by a voting system. These include:

- Unauthorized changes to system capabilities for:
 - Defining ballot formats;
 - Casting and recording votes;
 - Calculating vote totals consistent with defined ballot formats; and
 - Reporting vote totals;
- Alteration of voting system audit trails;
- Changing, or preventing the recording of, a vote;
- Introducing data for a vote not cast by a registered voter;
- Changing calculated vote totals;
- Preventing access to vote data, including individual votes and vote totals, to unauthorized individuals; and
- Preventing access to voter identification data and data for votes cast by the voter such that an individual can determine the content of specific votes cast by the voter.

This standard is also clear. The first three bullets in the list of objectives are related as previously explained, because intentional manipulation, fraud, malicious mischief and fraudulent or erroneous changes to the system often manifest in records that appear initially to have been accidents, inadvertent mistakes and errors.

The failure of security identified in this report specifically permitted unauthorized changes to the recording of votes in a database, as components of the database that should have been protected were allowed to be altered. A more difficult to find alteration might involve the changing of ballot formats so that a vote for one candidate appeared as a vote for a different candidate, but the access granted by the failure of security access controls allowed full administrative access to the database. The changing of calculated vote totals was specifically demonstrated by the tests in this examination. The data values changed essentially mean "Trump's votes are stored here -> X" and "Biden's votes are here -> Y" and the test switched X and Y.

As presented in Report #1, audit trails were altered (deleted) because the specifically enumerated risk was not addressed as required by this standard.

VSS V1, 6.2, page 6-96:

Access controls are procedures and system capabilities that detect or limit access to system components in order to guard against loss of system integrity, availability confidentiality and accountability. Access controls provide reasonable assurance that system resources such as data files, application programs, and computer-related facilities and equipment are protected against unauthorized operation, modification, disclosure, loss, or impairment. Unauthorized operations include modification of compiled or interpreted code, run-time alteration of flow control logic or of data, and abstraction of raw or processed voting data in any form other than a standard output report by an authorized operator.

Access control capability was built into the EMS server operating system and into the SQL DBMS but not programmed to be secure and one most egregious finding was that the EMS server was specifically configured to be insecure in defiance to the requirements in this standard and every known industry, government and security best practice, the standards of the National Institute of Standards and Technology (which chaired the committee that produced the VSS), and the DoD Security Technology Implementation Guides.

VSS V1, 6.2.2, page 6-97:

Vendors shall provide a detailed description of all access control measures designed to permit authorized access to the system and prevent unauthorized access. Examples include:

- a. Use of data and user authorization;
- b. Program unit ownership and other regional boundaries;
- c. One-end or two-end port protection devices;
- d. Security kernels;
- e. Computer-generated password keys;
- f. Special protocols;
- g. Message encryption; and
- h. Controlled access security.

Vendors shall also define and provide a detailed description of the methods used to prevent unauthorized access to the access control capabilities of the system itself.

This standard requires a detailed description to be provided by the voting system vendor, but clearly expects these functional protections to be implemented if the measures are to be documented.

DVS stated on their website⁷⁹ that they are compliant with voting systems standards, including the Voluntary Voting Systems Guidelines (VVSG) as shown in Figure 66. A review of the VSTL test-related documents reveals that the standards tested against were the VVSG standards. By comparing the test plans and reports to the requirements in the VVSG, this is easily assessed.



Figure 66 - DVS Compliance Statement

The Voluntary Voting Systems Guidelines (VVSG) contain even more explicit and precise definitions of the logging required than do the VSS, and although these are Guidelines that are not explicitly required under Colorado law, DVS makes the claim on their website that they are compliant with them. The 2005 VVSG were a defacto standard for the security of election systems and have been revised several times. The 2005 VVSG specifically requires in section 2.1.5.1 that a number of safeguards and operational requirements be applied. The VVSG excerpt below is *only a small partial list of those requirements*, but for this examination, the finding of key compliance issues is noted in Red following each requirement:

- a. Voting system equipment shall record activities through an event logging mechanism.
FAIL. Log mechanism does exist and records some, but not all activities, even though it overwrites and destroys those records frequently. Logging is not only incomplete but is wholly inadequate.
- b. Voting system equipment shall enable file integrity protection for stored log files as part of the default configuration.
FAIL. Not only have log files not been preserved, but they have been overwritten as indicated in Report #1. Further, the log file size has been set to a very small limit such that the log data is NOT preserved and cannot be recovered historically. Integrity Protection for these log files is not implemented.
- c. The voting system equipment logs shall not contain information that, if published, would violate ballot secrecy or voter privacy or that would compromise voting system security in any way.
FAIL. The log files that remain contain very little information of value in determining the integrity of the election at all; no information was found in the logs that can violate the secrecy of ballots or voter privacy, or that would compromise voting system security, but critical Audit Log data has been deleted (overwritten and in some cases its collection disabled) that is required for an Audit of the system's security, integrity, accuracy, that would identify errors, malicious actions, illegal tampering with ballots and vote totals, intrusions, what programs

⁷⁹ This statement was present on Dominion Voting Systems' website in September, 2020 and has since been removed, however the claim that they comply with voluntary VVSG standards brings this into relevance.

were run, by whom, and their results. **Contrary to the law, this is not in compliance – it is just the opposite: voting system security is compromised by the inability to detect malicious activity.**

- d. The voting system equipment shall log at a minimum the following data characteristics for each type of event: 1) system ID; 2) unique event ID and/or type; 3) timestamp; 4) success or failure of event, if applicable; 5) User ID trigger the event, if applicable; 6) Resources requested, if applicable.

FAIL. The EMS system does not record this information and in most cases has been configured by the Manufacturer to not log this information.

- e. Voting system equipment shall log all events, including abnormal events.

FAIL. The disabling of logging and the overwriting of log files above a certain size prevent the logging of all events.

- f. Voting system equipment shall ensure that event logging cannot be disabled. Voting system equipment shall implement default settings for secure log management activities, including log generation, transmission, storage, analysis and disposal.

FAIL. The design and configuration of this voting system provides exactly the opposite. Logging has been disabled by design and by the misconfiguration of the operating system such that the required and necessary records are NOT stored.

- g. Voting system equipment shall log clearing of logs and log rotation.

FAIL. The EMS system does not log the clearing of logs or log rotation, nor the overwriting of files (an act of “clearing the logs”). No record of log rotation could be found. In Report #1, the vendor DVS not only overwrote the operating systems and all log data with its “Trusted Build” installation, it designed the installation process to re-format and re-partition the hard disk ensuring that this occurred.

Of particular importance are sections b, d, e, f and g above. Had they been implemented properly and in accordance with the standards as Dominion claims and Customers expect, these log data would have supported conclusions regarding the integrity or the lack of integrity of the election. In both Antrim and Maricopa investigations, the DVS software did not log each modification to each record. Per the VSS, this detail of logging should be not only performed, but retained for 22 months (25 months in Colorado).

Even the Center for Internet Security (CIS) recognizes the need for these controls, among many others, in their Handbook for Election Infrastructure Security.⁸⁰

Given the failure to implement these required and recommended controls, the DVS Democracy Suite version 5.11-CO as provided to the State of Colorado **does not possess the required integrity controls as claimed by DVS and required by law. From the evidence presented in this report, this failure of integrity safeguards means that elections held in Colorado using this equipment do not possess the integrity to protect the vote from tampering, or to record access to or modification of the vote.**

⁸⁰ <https://www.cisecurity.org/wp-content/uploads/2018/02/CIS-Elections-eBook-15-Feb.pdf>

APPENDIX B. DATABASE FUNDAMENTALS

This report addresses computerized databases. This Appendix provides a basic understanding of the terms and technology involved to support the reader's understanding of findings in this report.

The voting systems used in Mesa County, Colorado are made by DVS. Many of these voting systems are comprised of an industry-standard computer that uses a Microsoft operating system and Dominion application software that provides a foundation for election related functions including capturing and storing the election data in a database management system, tabulating and counting the vote.

The Mesa County Election Management System (EMS) server runs on the Microsoft Windows Server 2016 operating system, and it employs a database management system known as Microsoft SQL Server. The security of the system depends largely upon the proper configuration of the Operating System and the SQL Server.

There are several types of databases, including relational, non-relational, and object-oriented databases. This discussion will be limited to relational databases because this is the type of database used in the Dominion voting system that is the subject of this forensic examination.

Microsoft SQL Server is a Database Management System (DBMS). A DBMS can contain many databases. Within this Mesa County, Colorado EMS server DBMS are many databases from prior elections, in addition to the 2020 General Election. Each database consists of many tables that can have different purposes. Some are administrative (access permissions for example), some are necessary for the DBMS to function (such as the database of databases, necessary because a DBMS can have multiple databases), and some have operational content related to the purpose of the database. This information is contained in multiple Tables consisting of multiple columns (and multiple rows if not empty). The database of databases (referred to as the DBDB) identifies the users, access permissions, the identity of each table that is contained within each respective database, among other items.

The fundamental components of a relational database are Tables, Rows and Columns. Data are organized in tables. Columns within a table contain specific data types, for example, first name, last name, street address, city, state, etc. Rows within a table each contain an instance of the data, referred to in database science as a tuple. The database is called a relational database because the various tables are *Related* by what is known as a KEY value. The Key value exists in multiple tables and is the item that links or *relates* the data in one table to the data in another table. For example, in a voter database, one reasonable KEY value might be Ballot Number – it would exist in all the associated tables and it becomes possible to retrieve ALL the data about a particular ballot by searching for every row where ballot number equals, for example, 300.

One primary purpose of a database is to return data in response to a request for that data, called a Query. One of the most common computer languages used in modern relational databases is the Structured Query Language (SQL). Structured query language is intended to be readable and understood easily.

An example of an SQL-like query might be to find the address of a person in a database table called "Addresses". Such a query might look like:

```
RETRIEVE(Addresses) address.street.address, address.city, address.state where first.name="John"  
and last.name="Smith"
```

IF the database table has an entry for John Smith, the above query would return the Street Address, City and State for him, *provided that* the user of this database had permission to read this specific Addresses table. While there is a specific order (syntax) for the components of the database command (e.g., a format), the commands are not difficult to understand, and the example here, while similar, is simplified to make it very understandable.

A DBMS implemented in software known as *Microsoft SQL Server* is addressed in this document because it is the DBMS installed and used in the Mesa County Colorado Election Management System server. The function of a DBMS is to organize its tables and rows, to provide a very granular set of permissions to the users of the database, to provide the integrity of the data – specifically to ensure that data cannot be inappropriately altered or deleted, and to control the four basic functions of the database. Four basic functions are implemented in relational databases, with respect to the data contained in its table-rows. Those basic functions are read, write, modify, and delete. The DBMS also supports various types of calculations based on the data in its tables.

One of the features of a DBMS is to very granularly control the permissions within a database. For example, a user might have permission to change the street address within a row, but not be allowed to change the city or state. Normal computer system permissions *without* a DBMS give the user permission to access the entire data set (for example, within a spreadsheet). Thus, the permission settings (e.g., configuration) of a DBMS are critical to its proper functioning and the ability to maintain integrity of the data within the database. These permission settings control who can perform which transactions.

Permissions within a well-controlled database specify which users can read which tables, which users can add data to the table, which users can modify (or update) data in the table, and which users can delete data in a table. Most commonly only the DBMS administrator has all four permissions for any table. It is common for an average user to be able to read and perhaps add data to a table, while changing or deleting data requires a supervisor to perform the task. A computer program (or task) can be assigned permission in the same manner that a user can be, sometimes by creating a user-id that is used only by the program.

There are special tables within a database that are highly restricted. These special tables include the DBDB within the DBMS, the User table within each database, the permissions for each user to each database and database table, and in some cases, the permissions for each user to the columns within each table. These special tables define how the DBMS operates.

It is required that a particular user within a DBMS only be able to alter the data with good reason. One example might be the case of a changed vote. Let's consider, for example, a hand-marked ballot, for simplicity, identified as ballot #300. The identity of the voter is not associated with the ballot number so it is accessed only by its number. The ballot contains circles or squares to be marked to indicate a vote. However, if the ballot marking is not within the lines (within limits), the ballot is marked for adjudication so that a human can then take steps to determine the voter's intent and then store that entry in the database. In this example, the original vote (and the photographic image of the ballot) might be stored in a database table called PendingAdjudication (the table name is an example to illustrate the technology). The Adjudication user should be able to read the data in the PendingAdjudication table, but not change or delete it. The user looks at the ballot image and makes their determination of voter intent and the results are written to a separate table called AdjudicatedVote. The user then has permission to change the value of ONE COLUMN within the PendingAdjudication table (for the specific data row) to indicate Adjudicated or NotAdjudicated. The point of the example is that even in this case, the original data is not deleted, and a

separate database table is used to compile the data. The Adjudication user in this example NEVER changes the original data, but the vote that is counted is in the AdjudicatedVote table. Thus, an audit of the complete voter database should show that there is one, and only one, entry for ballot #300, and the decision of the auditor should be available for review and the actions taken should be traceable. A more complex design may even use a separate table all-together to track which items are adjudicated or not.

The design of the database must make sense. In the example above, if the Adjudicator were to be permitted to change the original vote in the PendingAdjudication table, the ability to review their decision would be lost and there would be no way to audit the change, without seeing the before- and after- results. Thus, not only must the configuration of permissions enable those necessary changes but it must protect the integrity of the data and support the ability of the system to be auditable.

There is much not discussed here. For example, the DBMS in a voting application would be expected to check the PendingAdjudication table to make sure that every ballot that was sent to be adjudicated HAD BEEN processed, and that there were no rows with NotAdjudicated remaining, before the tabulation and count of votes had been finalized.

The design of the database and its permissions are only part of the logic required to make such a system work properly. As with the check above to ensure that all votes were adjudicated, there is much additional logic, which should be found within the database processing workflow, to ensure the proper calculations and integrity are maintained throughout the entire voting process.

APPENDIX C. IP ADDRESSING FUNDAMENTALS

There are two versions of Internet Protocol addressing seen in this data. The legacy version of addressing is expressed by four one- to three-digit numbers separated by periods – “X.X.X.X,” where X is an 8-bit number (e.g., has a value of 0-255). Because industry and users throughout the world have exceeded the number of available address numbers, a new address scheme was developed. The legacy address scheme is known as IP version 4 (IPv4) and is 32 binary bits long, while the new scheme is known as IP version 6 (IPv6) and is 128 binary bits long, represented as 8 groups of 4 hexadecimal values (0-9 and A-F) separated by periods (A.B.C.D.E.F.G.H). This solves the problem of running out of IPv4 addresses and provides, by one estimate, more than 1,500 IP addresses for every square meter of Earth’s surface. This explanation is provided because both types of addresses are present in this forensic analysis and it is necessary for the reader to understand the data being presented.

In Figure 8, IP2 shows the IPv4 address 192.168.100.10, the address assigned to be used by the Mesa County EMS server. IP1 shows the IPv6 address FE80::792B:3E74:DF1B:C565%5. This translates to FE80:0000:0000:792B:3E74:DF1B:C565 (the double colon stands for repeated 0 address values), and “zone” 5 (%5) which is essentially the identifier that indicates which IP Network Interface Card (NIC) the address is tied to. While these data reflect the interface capability of the Oracle VirtualBox environment, the IP Address 192.168.100.10 is configured in the stored operating system and when launched here, automatically assumed the same IP address. IPv6 is addressed here for completeness.

The IPv4 address used (192.168.x.x) is a “Private Network” address per Internet Standard RFC-1918 and is NOT directly routable across the Internet. However, firewalls, routers and other network devices use a service called Network Address Translation (NAT) or Port Address Translation (PAT) to convert these private addresses to publicly routable addresses and allow them to be transmitted over the larger Internet. Thus, the use of a private network address assigned to a particular Ethernet interface does not in itself, prevent the computer from accessing the Internet – it becomes necessary to examine all routers, firewalls and other networking equipment to determine whether the computer is capable of *direct* connection to the Internet via a translation mechanism such as NAT or PAT.

For every IPv4 address, the number is split into two parts – the first part of the number is the Network Address and the second part of the number is the Device Address. This is defined by the number of bits assigned to the network address and follows the IP address and a slash “/.” “192.168.100.0/24” indicates the first 24 bits of this binary number constitutes the Network Address and the remaining 8 bits constitute the Device Address. This set of Device Addresses is referred to as a Subnet. For data to leave a subnet, the subnet must have a Default Gateway assigned. When a computing device sends data to an address that is outside the Subnet group of addresses, it sends that data to the Default Gateway address which then *routes* the data onward to its destination.

There are two special Device Addresses: the first value in the Device Address is used to specify the Network Address while the last address in the subnet range is defined as a Broadcast Address and is used to send data to every device in the Subnet. In the address example “192.168.100.0/24,” the first address is 0 and is the Network Address is 255; a broadcast to all 254 device addresses possible on this subnet would be sent to “192.168.100.255.” The first usable address of this subnet is “192.168.100.1,” which is typically used for the Default Gateway address.

The IPv6 address used (FE80:x:x:x:x:x:x) is a *link-local* address, which means that it is also not routable across the Internet. The concept of NAT and PAT are not used in IPv6, *with the single exception of using it to translate IPv6 addresses to IPv4 addresses and vice versa* because not all network equipment is capable of using IPv6 (yet). Some legacy network equipment widely in use today is not capable of transporting IPv6.

This link-local (FE80) address is not routable and is not supposed to be translatable from IPv6 to IPv4 and vice versa, however this depends on whether a particular network device vendor has followed the standard when implementing their software. While most vendors have designed their devices properly (network devices would not work properly otherwise), from a scientific and evidentiary perspective, it still remains necessary to forensically examine all connected network devices to ensure that these addresses cannot reach the Internet.

APPENDIX D. NATION-STATE CYBER ATTACK CAPABILITIES

Introduction

The mere idea of advanced Nation-State cyberwarfare capabilities at first blush seems like fantasy straight out of a James Bond film. Yet these attack capabilities are the most sophisticated on the planet. Most countries, including the USA, consider their defensive and offensive cyberwar capabilities to be highly classified. In the USA these are implemented by the National Security Agency, specifically in its Tailored Access Operations (TAO) group according to numerous reports, and in the UK, by the CGHQ. In this appendix, a short synopsis (and bibliography) of several of the more sophisticated cyberattacks are presented, *in particular in support of statements made elsewhere in this document*—specifically, that attacks occur *extremely quickly*, that a USB Thumb Drive can be infected with malicious software which can then infect other computer systems, and that cyberattacks can cause considerable damage. This is a very small sampling of some of the more sophisticated attacks but is illustrative of the advanced sophistication and the pervasive nature of vulnerabilities.

Security experts in the USA also understand and have documented issues with Voting Systems security, in *this report* <https://archive.org/details/6432002-Voting-Village-Report-defcon27/page/n15/mode/2up>. This security conference (Defcon 2019) is often billed as a “hacker” conference, however some of the most renowned security professionals in the world attend it, and the “Voting Village” at Defcon, in the referenced report, is co-chaired by Matt Blaze, Professor of Law and McDevitt Chair for the Department of Computer Science, Georgetown University (and author of many books on the subject). Christopher Krebs, Director of the US Critical Infrastructure Security Agency (CISA) also attended.

In 1984, while working at Bell Telephone Laboratories, I witnessed one of the very first destructive computer viruses. In that era, computer monitors used standard NTSC television signals to present video on a large cathode ray tube “tv screen”. The monitor used a very high voltage (tens of thousands of volts) to cause the electron beam to display a picture. To generate the high voltage, the monitor used a “flyback” transformer, a specific type of high-frequency transformer commonly found in televisions, that took advantage of the 15,575 hertz horizontal scan signal that is part of the NTSC standard video signal. This signal was amplified and fed the primary winding of the transformer. It was found that the video driver circuit card in primitive ‘PCs’ of that era allowed the frequency of the horizontal scan signal to be programmed. When that frequency was programmed to 0 hertz, the electric current through the primary winding of the transformer changed from a rapidly varying signal to a constant “on” state. Since this state exceeded the capability of the transformer, it burned the transformer out, destroying the monitor.

In 2007, DHS and the Idaho National Laboratory ran the Aurora Generator Test to demonstrate vulnerabilities in the electric power grid in the USA.⁸¹ A leaked video⁸² of the attack is widely available on the Internet and shows the complete destruction of a 27 ton, 2.25MW generator by a cyberattack. In this attack, the attackers (part of the US Military) opened the relays of the generator (by remote computer control) long enough for the generator to slip out of synchronization with the power grid, and then reconnected the relays, causing a catastrophic mechanical jolt to the generator. This is the equivalent of driving your car at 70 mph, and while moving at that speed, placing your car into reverse gear. They did this three times, as is apparent from the video. The third time was “the charm” as the generator’s diesel

⁸¹ https://en.wikipedia.org/wiki/Aurora_Generator_Test

⁸² <https://youtu.be/LM8kLaJ2NDU>

engine self-destructs and the room as well as the external exhaust pipe fill with black smoke. The article cited⁸³ includes both the video of the test showing destruction of the generator as well as the original DHS report, released under FOIA.

Adversaries constantly scan and probe every computer on the internet to identify weakness well in advance of the need for an attack. A commercial (i.e., unclassified) example of this scanning is demonstrated by the company Lumeta. During the first Gulf War, noted security expert Bill Cheswick, co-founder of Lumeta, used a common troubleshooting tool (ping) and was able to perform real-time battle-damage assessment by detecting computers that went offline due to active bombing campaigns. Adversaries have discovered their targets well in advance and have pre-programmed attacks ready to launch.

Moonlight Maze

“Moonlight Maze was a 1999 US government investigation into a massive data breach of classified information. It started in 1996 and affected NASA, the Pentagon, military contractors, civilian academics, the DOE, and numerous other American government agencies. By the end of 1999, the Moonlight Maze task force was composed of forty specialists from law enforcement, military, and government. The investigators claimed that if all the information stolen was printed out and stacked, it would be three times the height of the Washington Monument, which is 555 ft (169 m) tall. The Russian government was blamed for the attacks, although there was initially little hard evidence to back up the US accusations besides a Russian IP address that was traced to the hack. Moonlight Maze represents one of the first widely known cyber espionage campaigns in world history. It was even classified as an Advanced Persistent Threat (a very serious designation for stealthy computer network threat actors, typically a nation state or state-sponsored group) after two years of constant assault. Although Moonlight Maze was regarded as an isolated attack for many years, unrelated investigations revealed that the threat actor involved in the attack continued to be active and employ similar methods until as recently as 2016.”⁸⁴

Stuxnet

Stuxnet was an offensive operation, believed to be conducted by the USA and Israel,⁸⁵ to destroy nuclear enrichment centrifuges at Iran’s Natanz enrichment facility,⁸⁶ About 1,000 centrifuges were involved in the enrichment of ‘yellow cake’ uranium from “fuel grade” for commercial power reactors to “weapons grade” to create nuclear weapons (bombs/missiles).

“Stuxnet was a 500-kilobyte computer worm that infected the software of at least 14 industrial sites in Iran. This worm was an unprecedentedly masterful and malicious piece of code that attacked in three phases. First, it targeted Microsoft Windows machines and networks, repeatedly replicating itself. Then it sought out Siemens Step7 software, which is also Windows-based and used to program industrial control systems that operate equipment, such as centrifuges. Finally, it compromised the programmable logic controllers. The worm's authors could thus spy on the industrial systems and even cause the fast-spinning centrifuges to tear themselves apart, unbeknownst to the human operators at the plant.”

⁸³ <https://www.muckrock.com/news/archives/2016/nov/14/aurora-generator-test-homeland-security/>

⁸⁴ https://en.wikipedia.org/wiki/Moonlight_Maze

⁸⁵ <https://www.jpost.com/International/Snowden-US-Israel-created-virus-to-destroy-Iran-nukes-319226>

⁸⁶ <https://www.wired.com/2010/11/stuxnet-sabotage-centrifuges/>

“Stuxnet could spread stealthily between computers running Windows—even those not connected to the Internet. If a worker stuck a USB thumb drive into an infected machine, Stuxnet could “worm” its way onto it, then spread onto the next machine that read that USB drive. Because someone could unsuspectingly infect a machine this way, letting the worm proliferate over local area networks, experts feared that the malware had perhaps gone wild across the world.”

“In October 2012, U.S. defense secretary Leon Panetta warned that the United States was vulnerable to a “cyber–Pearl Harbor” that could derail trains, poison water supplies, and cripple power grids. The next month, Chevron confirmed the speculation by becoming the first U.S. corporation to admit that Stuxnet had spread across its machines.”⁸⁷

Operation Titan-Rain

Titan Rain was a series of coordinated computer attacks⁸⁸ on the United States that began in 2003 and originated from Guangdong, China. The attacks are believed to have come from the People’s Liberation Army unit 61398, located at the Lingshui Signals Intelligence Unit on Hainan Island, one of China’s largest military facilities in the South China Sea. This is the same unit responsible for the attack on the Wall Street Journal, which cyber forensics company Mandiant identified as APT-1 (Advanced Persistent Threat–1)⁸⁹.

“An **advanced persistent threat (APT)** is a stealthy threat actor, typically a nation state or state-sponsored group, which gains unauthorized access to a computer network and remains undetected for an extended period. In recent times, the term may also refer to non-state-sponsored groups conducting large-scale targeted intrusions for specific goals.”⁹⁰

Titan Rain is rumored to have stolen as much as 40 Terabytes of US Government secrets. This attack persisted for many years.

Operation Aurora

Operation Aurora was conducted by the People’s Liberation Army of China from mid-2009 through December, 2009.⁹¹

It was a very large scale attack that affected numerous commercial entities including Google, Morgan-Stanley, Adobe Systems, Akamai Technologies, Juniper Networks, and Rackspace who have publicly confirmed that they were targeted. According to reports, Yahoo, Symantec, Northrop Grumman, Morgan Stanley, and Dow Chemical were also among the targets. The unit which conducted the attack has been named APT-17.

“The attack was named ‘Operation Aurora’ by Dmitri Alperovitch, Vice President of Threat Research at cybersecurity company McAfee. Research by McAfee Labs discovered that ‘Aurora’ was part of the file path on the attacker’s machine that was included in two of the malware binaries McAfee said were associated

⁸⁷ <https://spectrum.ieee.org/the-real-story-of-stuxnet>

⁸⁸ https://en.wikipedia.org/wiki/Titan_Rain

⁸⁹ <https://www.lawfareblog.com/mandiant-report-apt1>

⁹⁰ https://en.wikipedia.org/wiki/Advanced_persistent_threat

⁹¹ https://en.wikipedia.org/wiki/Operation_Aurora

with the attack. "We believe the name was the internal name the attacker(s) gave to this operation," McAfee Chief Technology Officer George Kurtz said in a blog post."

"According to McAfee, the primary goal of the attack was to gain access to and potentially modify source code repositories at these high-tech, security, and defense contractor companies. '[The software configuration management systems] were wide open,' says Alperovitch. 'No one ever thought about securing them, yet these were the crown jewels of most of these companies in many ways—much more valuable than any financial or personally identifiable data that they may have and spend so much time and effort protecting.' "

2020 US Government Attack

In 2020, a massive nation-state attack against many companies and US Government organizations took place.⁹² Initially only the Treasury department and the NTIA were thought to have been attacked. But it turned out that many of the US Government operations including the IRS and even the US Administrative Office of the Courts (which relies heavily on the software SolarWinds) were compromised.

This attack was a supply-chain attack. SolarWinds, a network management system, as many software firms do, periodically releases updates to its software. SolarWinds was broken into and one of its update programs was infected with malware. Because SolarWinds was inappropriately assigned too much trust by its customers, their software updates were white-listed (allowed through the firewall, unchallenged). The attack was in the update.

This is widely regarded as one of the worst attacks in US history for the length of time it lasted (9 months) before detection as well as the impact it had upon affected organizations.

Summary

Nation-States including Russia, China, North Korea, Malaysia, Iran and many others seek to attack the USA's national security, economic, industrial, communications, and financial systems. These attackers are extremely sophisticated and well trained. For example, North Korea has an institute in Pyongyang that teaches cyberwarfare and has been turning out more than 100 graduates every month for well over 15 years. Other Nation-States, including Iran, have sent students to North Korea's school.

This brief history has documented the sophistication of advanced cybersecurity attacks.

Multiple references show that sophisticated attacks can occur by transfer through USB drives, without being detected by the end user.

This history shows how unprotected system configurations have enabled advanced cyberattacks, and how software updates can infiltrate a company's IT operations and take control.

⁹² https://en.wikipedia.org/wiki/2020_United_States_federal_government_data_breach.

APPENDIX E. SECURITY CONSIDERATIONS FOR SQL SERVER INSTALLATIONS

The following information was taken directly from Microsoft documentation and is provided here to be a reference to basic security considerations related to installations of Microsoft SQL Server. This is relevant as Microsoft SQL Server is the product used in the Dominion EMS.

From Microsoft SQL Server Documentation:

Security is important for every product and every business. By following simple best practices, many security vulnerabilities can be avoided. Below are some security best practices that should be considered both before installing SQL Server and after SQL Server has been installed. Security guidance for specific features is included in Microsoft reference articles for those features.

Before Installing SQL Server:

- Follow these best practices when setting up the server environment:
- Enhance physical security
- Use firewalls
- Isolate services
- Configure a secure file system
- Disable NetBIOS and server message block

Details about these items are provided below.

Enhance Physical Security

Physical and logical isolation make up the foundation of SQL Server security. To enhance the physical security of the SQL Server installation, do the following tasks:

- Place the server in a room accessible only to authorized persons.
- Place computers that host a database in a physically protected location, ideally a locked computer room with monitored flood detection and fire detection or suppression systems.
- Install databases in the secure zone of the corporate intranet and do not connect your SQL Servers directly to the Internet.
- Back up all data regularly and secure the backups in an off-site location.

Use Firewalls

Firewalls are important to help secure the SQL Server installation. Firewalls will be most effective by following these guidelines:

- Put a firewall between the server and the Internet. Enable your firewall. If your firewall is turned off, turn it on. If your firewall is turned on, do not turn it off.
- Divide the network into security zones separated by firewalls. Block all traffic, and then selectively admit only what is required.
- In a multi-tier environment, use multiple firewalls to create screened subnets.
- When you are installing the server inside a Windows domain, configure interior firewalls to allow Windows Authentication.

Isolate Services

Isolating services reduces the risk that one compromised service could be used to compromise others. To isolate services, consider the following guidelines:

- Run separate SQL Server services under separate Windows accounts. Whenever possible, use separate, low-rights Windows or Local user accounts for each SQL Server service.

Configure a Secure File System

Using the correct file system increases security. For SQL Server installations, you should do the following tasks:

- Use the NTFS file system (NTFS). NTFS is the preferred file system for installations of SQL Server because it is more stable and recoverable than FAT file systems. NTFS also enables security options like file and directory access control lists (ACLs) and Encrypting File System (EFS) file encryption. During installation, SQL Server will set appropriate ACLs on registry keys and files if it detects NTFS. These permissions should not be changed. Future releases of SQL Server might not support installation on computers with FAT file systems.
- Use a redundant array of independent disks (RAID) for critical data files.

Disable NetBIOS and Server Message Block

Servers in the perimeter network should have all unnecessary protocols disabled, including NetBIOS and server message block (SMB).

NetBIOS uses the following ports:

- UDP/137 (NetBIOS name service)
- UDP/138 (NetBIOS datagram service)
- TCP/139 (NetBIOS session service)

SMB uses the following ports:

- TCP/139
- TCP/445

During or After Installation of SQL Server

After installation, you can enhance the security of the SQL Server installation by following these best practices regarding accounts and authentication modes:

Service accounts

- Run SQL Server services by using the lowest possible permissions.
- Associate SQL Server services with low privileged Windows local user accounts, or domain user accounts.

Authentication mode

- Require Windows Authentication for connections to SQL Server.
- Use Kerberos authentication.

Strong passwords

- Always assign a strong password to the sa [system administrator] account.
- Always enable password policy checking for password strength and expiration.
- Always use strong passwords for all SQL Server logins.

References:

<https://docs.microsoft.com/en-us/sql/sql-server/install/security-considerations-for-a-sql-server-installation?view=sql-server-ver15>

<https://docs.microsoft.com/en-us/sql/sql-server/install/security-considerations-for-a-sql-server-installation?view=sql-server-2016>

APPENDIX F. C.R.S. 1-5-608.5

1-5-608.5. Electronic and electromechanical voting systems - testing by federally accredited labs - certification and approval of purchasing of electronic and electromechanical voting systems by secretary of state - conditions of use by secretary of state - testing.

(1) A federally accredited laboratory may test, approve, and qualify electronic and electromechanical voting systems for sale and use in the state of Colorado.

(2) (Deleted by amendment, L. 2009, (HB 09-1335), ch. 260, p. 1190, § 4, effective May 15, 2009.)

(3)

(a) If the electronic and electromechanical voting systems tested pursuant to this section satisfy the requirements of this part 6, the secretary of state shall certify such systems and approve the purchase, installation, and use of such systems by political subdivisions and establish standards for certification.

(b) The secretary of state may promulgate conditions of use in connection with the use by political subdivisions of electronic and electromechanical voting systems as may be appropriate to mitigate deficiencies identified in the certification process.

(c) In undertaking the certification required by this section, the secretary of state may consider either procedures used or adopted by county clerk and recorders or best practices recommended by equipment vendors.

(3.5)

(a) [Editor's note: Subsection (3.5) is effective July 1, 2022.] On and after December 31, 2022, if an electronic and electromechanical voting system tested pursuant to this section satisfies the requirements of this part 6 related to the use of the system in an election using instant runoff voting and the rules established by the secretary of state pursuant to section 1-5-616 (1.5), the secretary of state shall certify such system and approve the purchase, installation, and use of such system by political subdivisions in an election using instant runoff voting.

(b) The secretary of state may promulgate conditions of use in connection with the use by political subdivisions of an electronic and electromechanical voting system in an election using instant runoff voting as may be appropriate to mitigate deficiencies identified in the certification process.

(c) In undertaking the certification required by this section, the secretary of state may consider procedures used or adopted by county clerk and recorders or best practices recommended by equipment vendors.

(4) In undertaking the certification required by this section, the secretary of state may request a federally accredited laboratory to undertake the testing of an electronic or electromechanical voting system or may use and rely upon the testing of an electronic or electromechanical voting system already performed by another state or a federally accredited laboratory upon satisfaction of the following conditions:

(a) The secretary of state has complete access to any documentation, data, reports, or similar information on which the other state or laboratory relied in performing its testing and will make such information available to the public subject to any redaction required by law; and

(b) The secretary of state makes written findings and certifies that he or she reviewed the information specified in paragraph (a) of this subsection (4) and determines that the testing:

(I) Was conducted in accordance with appropriate engineering standards in use as of the time the testing is undertaken; and

(II) Satisfies the requirements of sections 1-5-615 and 1-5-616 and all rules promulgated thereunder.

(5) In undertaking the certification required by this section, the secretary of state may conduct joint testing with an agency of another state or with a federally accredited laboratory.

History

Source: L. 93:Entire section added, p. 1414, § 57, effective July 1. L. 2004:Entire section amended, p. 1346, § 13, effective May 28. L. 2009:Entire section amended,(HB 09-1335), ch. 260, p. 1190, § 4, effective May 15. L. 2021:(3.5) added,(HB 21-1071), ch. 367, p. 2416, § 3, effective July 1, 2022.

Research References & Practice Aids

Hierarchy Notes:

C.R.S. Title 1

C.R.S. Title 1, Art. 5

State Notes

Research References & Practice Aids

Cross references:

For the legislative declaration contained in the 2004 act amending this section, see section 1 of chapter 334, Session Laws of Colorado 2004.

Colorado Revised Statutes Annotated

Copyright © 2022 COLORADO REVISED STATUTES All rights reserved.

APPENDIX G. C.R.S. 1-5-615

1-5-615. Electronic and electromechanical voting systems - requirements.

(1) The secretary of state shall not certify any electronic or electromechanical voting system unless such system:

(a) Provides for voting in secrecy;

(b) Permits each elector to vote for all offices for which the elector is lawfully entitled to vote and no others, to vote for as many candidates for an office as the elector is entitled to vote for, and to vote for or against any ballot question or ballot issue on which the elector is entitled to vote;

(c) Permits each elector to verify his or her votes privately and independently before the ballot is cast;

(d) Permits each elector privately and independently to change the ballot or correct any error before the ballot is cast, including by voting a replacement ballot if the elector is otherwise unable to change the ballot or correct an error;

(e) If the elector overvotes:

(I) Notifies the elector before the ballot is cast that the elector has overvoted;

(II) Notifies the elector before the vote is cast that an overvote for any office, ballot question, or ballot issue will not be counted; and

(III) Gives the elector the opportunity to correct the ballot before the ballot is cast;

(f) Does not record a vote for any office, ballot question, or ballot issue that is overvoted on a ballot cast by an elector;

(g) For electronic and electromechanical voting systems using ballot cards, accepts an overvoted or undervoted ballot if the elector chooses to cast the ballot, but it does not record a vote for any office, ballot question, or ballot issue that has been overvoted;

(h) In a primary election, permits each elector to vote only for a candidate seeking nomination by the political party with which the elector is affiliated;

(i) In a presidential election, permits each elector to vote by a single operation for all presidential electors of a pair of candidates for president and vice president;

(j) Does not use a device for the piercing of ballots by the elector;

(k) Provides a method for write-in voting;

(l) Counts votes correctly;

(m) Can tabulate the total number of votes for each candidate for each office and the total number of votes for and against each ballot question and ballot issue for the polling location;

(n) Can tabulate votes from ballots of different political parties at the same voter service and polling center in a primary election;

(o) Can automatically produce vote totals for the polling location in printed form; and

(p) Saves and produces the records necessary to audit the operation of the electronic or electromechanical voting system, including a permanent paper record with a manual audit capacity.

(1.5) [Editor’s note: Subsection (1.5) is effective July 1, 2022.] The secretary of state shall not certify any electronic or electromechanical voting system for use in an election using instant runoff voting unless, in addition to meeting the requirements of subsection (1) of this section, the system meets the requirements and performs the functions required by section 1-7-1003.

(2) The permanent paper record produced by the electronic or electromechanical voting system shall be available as an official record for any recount conducted for any election in which the system was used.

History

Source: L. 2004:Entire section added, p. 1347, § 14, effective May 28. L. 2013:IP(1), (1)(m), (1)(n), and (1)(o) amended,(HB 13-1303), ch. 185, p. 713, § 49, effective May 10. L. 2021:(1.5) added,(HB 21-1071), ch. 367, p. 2417, § 6, effective July 1, 2022.

Research References & Practice Aids

Hierarchy Notes:

C.R.S. Title 1

C.R.S. Title 1, Art. 5

State Notes

Research References & Practice Aids

Cross references:

(1) For the legislative declaration contained in the 2004 act enacting this section, see section 1 of chapter 334, Session Laws of Colorado 2004.

(2) In 2013, the introductory portion to subsection (1) and subsections (1)(m), (1)(n), and (1)(o) were amended by the “Voter Access and Modernized Elections Act”. For the short title and the legislative declaration, see sections 1 and 2 of chapter 185, Session Laws of Colorado 2013.

Colorado Revised Statutes Annotated

Copyright © 2022 COLORADO REVISED STATUTES All rights reserved.

APPENDIX H. MAN IN THE MIDDLE ATTACK

In Figure 10, an encryption certificate is not visible. This is due to the fact that an encryption certificate had not been created and assigned. This alone does not indicate the lack of a security encryption certificate, because SQL Server will create a self-signed certificate automatically, as it has done in this case. However, self-signed certificates are known to be insecure and susceptible to common man-in-the-middle attacks. On a voting system, where security should be paramount, this is wholly irresponsible at best.

Despite the direct connection to the back-end of the SQL server is set to be encrypted even in this sub-par fashion, any device with Microsoft SQL Server Management Studio or any other SQL Server client installed that supports the Windows Authentication method can connect to the server provided they have some type of connection (directly or indirectly) to any part of the voting system network, can find the server IP address, a userID and a password. Microsoft SQL Server Management Studio is a free download from Microsoft and does not require any special licensing – anyone can obtain it and use it without restriction. There are also many other SQL Clients that exist for Windows, OS X, iPhone, Android, and others, many that are free to download and use.

The SQL Server Management Studio (SSMS) software used on the Expert's client computer was downloaded directly from Microsoft, and that Expert's client computer had no prior encryption configuration, encryption keys or certificates containing encryption keys – the only things supplied to make the connection to the EMS server were a userID, password, and the IP address of the server.

Detail:

A “Man-In-The-Middle” attack (MITM) is an attack where an eavesdropper intercepts a communication between two parties, and makes each party believe he (or she) is the person they intended to communicate with by impersonating them.

In Figure 67 below, Person A would normally communicate with Person B directly. The attack involves intercepting the communication and impersonating the other party as illustrated by the red arrows and Person C.

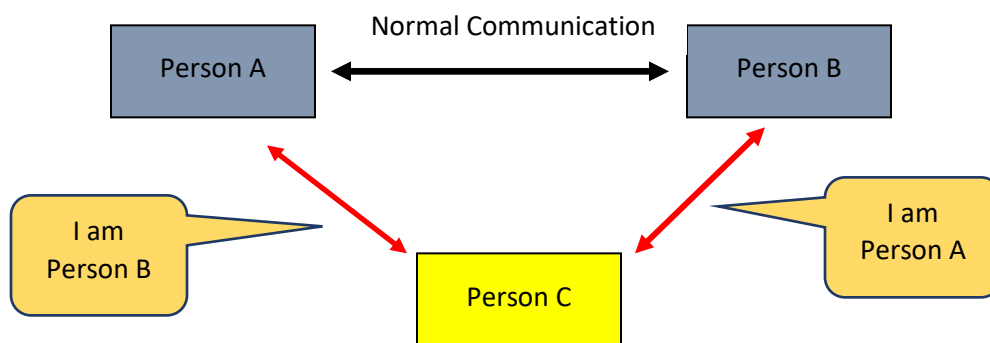


Figure 67 - Man In The Middle Attack

In the MITM attack, Person C can eavesdrop undetected, and can also alter or insert data that the other parties are unaware of. This is often used to steal passwords as well as change information, when the communication is unencrypted.

When the communication is encrypted with an encryption certificate, the certificate must be checked to be sure it is authentic and valid. If these checks are not properly performed, the MITM attack becomes possible.

A public Certificate Authority (a commercial service that can be purchased) usually guides the user through the proper certificate checking process when setting up the service. Alternatively, encryption may be setup using a Self-Signed Certificate, however the user is dependent upon their own knowledge and experience, thus Self-Signed Certificates are more prone to human error, oversight, or lack of knowledge of the proper process. If the checks are not properly setup, either method may be subject to this attack method.

While this seems complicated to setup for the average user, devices that perform MITM attacks are commonly available (see the Wi-Fi Pineapple, <https://shop.hak5.org/products/Wi-Fi-pineapple>). Tools such as these are used by cybersecurity professionals to check for the kind of misconfiguration that would allow an MITM attack, with the goal of helping the client fix those security problems, once identified. However, the devices are available for purchase by anyone.

APPENDIX J. FORENSIC IMAGING TECHNOLOGY

In the forensic community, forensic imaging is often referred to as producing a bit-for-bit image of a data storage medium, most of which historically have been hard disk drives. The statement is not quite so simple – as this Appendix explains.

In the figure below, internal components of a hard disk drive are illustrated. The blue disks are the actual 'disk platters', each of which have an upper magnetic media surface and a lower magnetic media surface. Each disk platter is mounted on a center shaft, called a 'spindle' which is connected to a motor that rotates the disks. For each media surface (i.e., where data can be stored) there is an armature (illustrated in black on the right) with a read/write head (in red, at the end of the armature). In this illustration, there are 4 platters with 2 media surfaces each, for a total of 8 surfaces where data can be stored.

As the disk spins, the read/write heads (similar to the heads in a magnetic tape recorder) move over the data and can read and write new data by magnetizing the disk media. These heads actually aerodynamically fly, a micron or so above the disk platter.

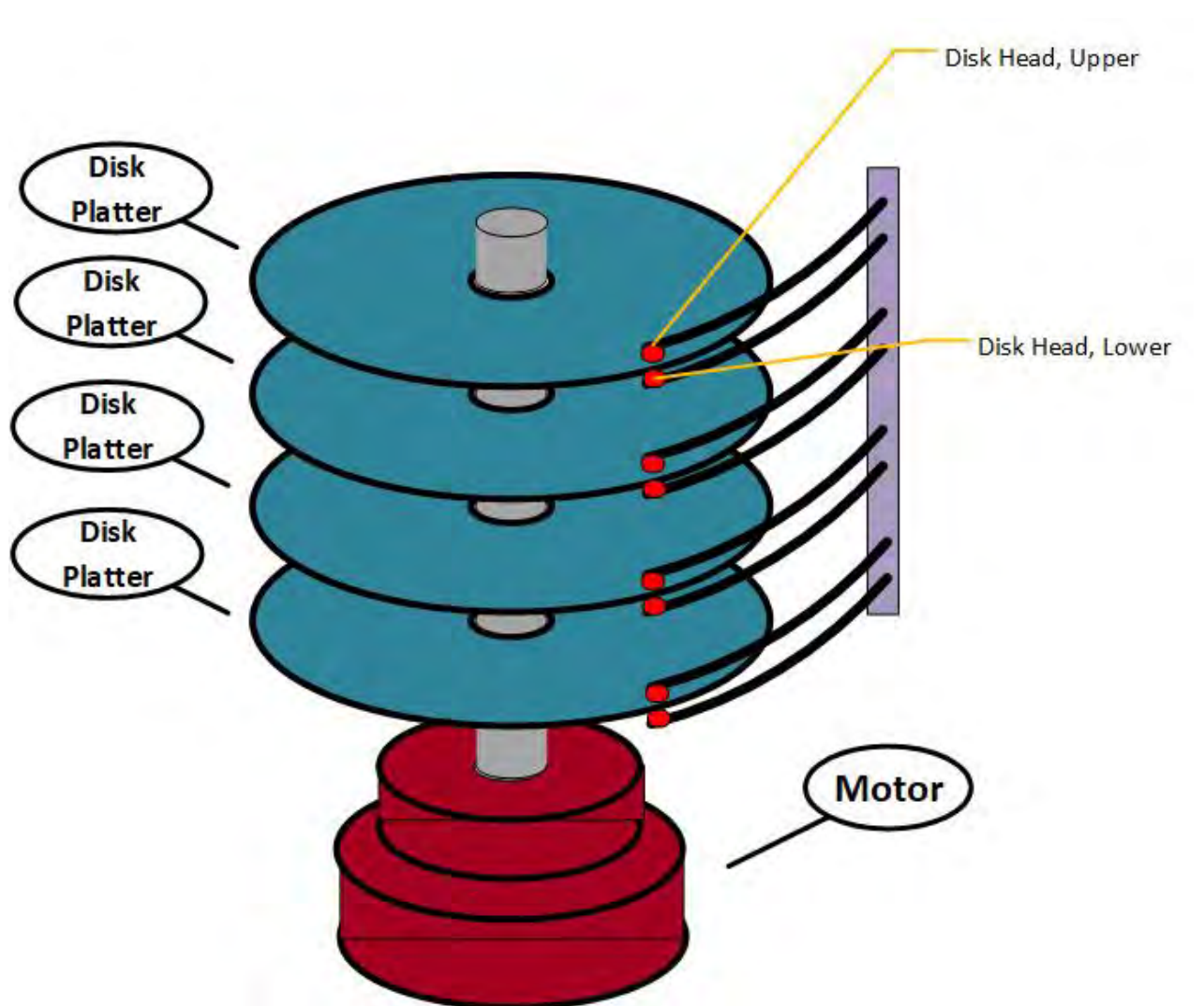


Figure 68 - Illustrative Hard Disk Components

Much like a pizza, each platter surface is divided into sectors (nearly triangular, just as pizza slices are). The surface is further divided into tracks – concentric rings that are smaller and smaller as they move toward the center of the disk. This organization is illustrated in a highly simplified illustration in Figure 67.

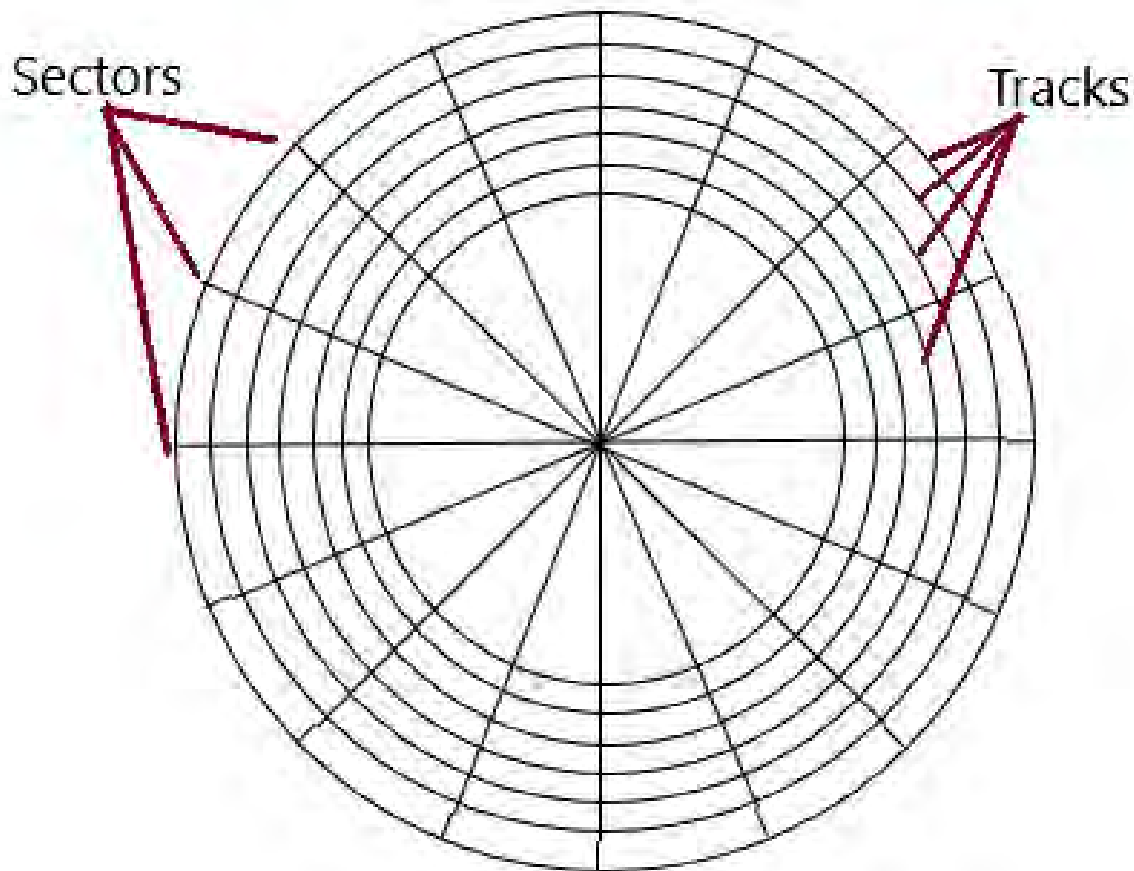


Figure 69 - Disk Track and Sector illustration

In the 1970's, magnetic media was manufactured to have a defect-free surface, but this was prohibitively expensive. Winchester disk technology provided a solution to the high expense. Rather than manufacture a disk media surface that was 100% usable, the manufacture of disk media with a 98% usable surface provided the ability to reduce cost very significantly. This allowed for defective areas on the disk – sectors in which data could not be reliably stored. But this required a scheme to identify these bad areas and ignore them. A map of the disk was developed, from the first sector to the last. As the disk was manufactured, the surface was tested for defects and those sectors with defects were added to the Permanent Defect list, today referred to as the p-list. When the disk is formatted, the disk controller (contained in the disk itself, on its circuit card) will access each physical sector on the disk that is not contained in the p-list, and label that sector with a sequential sector number known as a Logical Block Address (LBA). Obviously the LBA will skip over those sectors in the Defect list. To accommodate the growth of future defects, a list of new bad sectors (to be discovered later in the life of the device) would be added to a Growth List, known as a G-list.

Disk drives are manufactured with more capacity than the end user can access. For example, a 500Gb disk may actually have 580Gb of media storage available. This extra area is known as the Service Area of the disk, and is inaccessible except to the physical disk controller (circuit card that is part of the disk drive itself).

The p-list may be stored in a read-only memory (ROM) on the physical disk controller, or it may be stored in the service area. The g-list is empty at manufacture time and cannot be stored in a ROM but is rather stored in the service area of the disk. The remainder of the service area consists of spare sectors – unused sectors. When a new bad sector is discovered (i.e., a new disk failure) special disk access commands in the disk driver software instruct the disk that a specific logical block is bad and that block is added to the g-list, together with the identity of a spare sector used to replace that sector. The physical disk controller may have replaced physical sector 3921 (LBA 3921) with spare sector 616416, but the new physical storage sector is still addressed by the host computer controller as LBA 3921 because of this mapping. This permits the disk to continue to be used without the computer (and consequently its software) being aware of the replacement sector. If data was unreadable from the damaged sector, the data (file) stored in that location may be damaged and have to be replaced but the disk device still appears, to the computer, to work normally.

Because the sectors in the p-list were defective and never used after manufacture at all, and the g-list sectors were determined after manufacture to be defective, they cannot be read at all. The physical disk controller (built into the drive) has made these p-list and g-list sectors no longer accessible. Spare sectors are also not accessible in the service area of the disk as they are intended to be used as future replacements for active data storage. Finally some physical disk controllers store disk firmware in the service area of the disk but this is neither accessible nor usable to the end user or to the host computer system, but ONLY to the physical disk controller itself.

Thus, there exist data storage areas on a hard drive that have a list of bad sectors, the actual bad sectors themselves that cannot be read, and spare sectors used to repair the drive (and sometimes disk controller firmware). These data storage areas are protected from access to ensure that the drive can be used even though some defects are present from manufacture and others may develop during the lifetime of the drive.

This detail is provided to explain from a scientific perspective that the statement that “every physical bit on a hard drive is accessible and preserved in a forensic image” is true because the logical hard drive, i.e., the total user accessible data area, is what the computer itself and the user are able to access and every bit of data is preserved exactly as it existed at the time of imaging the data. These data in the service area of the data storage system are not accessible to the computer or any user, are not able to be read by forensic software, and they are not copied as part of a forensic image, but they are also not relevant to a forensic analysis of the computer system as none of the data in this service area can be read, written or manipulated without special equipment used by the manufacturer to create the storage device.

The unreadable service area on the drive is not accessible by the computer and does not contain any user accessible data. Even when a bad sector is added to the g-list, the computer does not access the protected service area; it sends a command to the physical disk controller which adds the sector to the g-list and remaps a spare sector in its place.

The remainder of the disk is known as ‘user accessible data area’ and is accessible by the computer system. This user accessible data area is formatted by the computer operating system, Microsoft Windows Server 2016 standard in the case of the Mesa County EMS server, and the data components necessary to create a file system are added to the drive (Master Boot Record, Partition Table, list of free data blocks / sectors, directories and ultimately files containing program and user data). Data in the user accessible data area can be created, modified, or overwritten. When a file is “deleted” by the operating system, the directory

entry is marked indicating that the directory slot is now available to be reused and the sector numbers previously occupied by the file are added back to the list of free data blocks (the free list). The data is not physically deleted from the drive – the drive area is simply marked as available for reuse. When the sectors previously occupied (by for example, data from a photographic image, 1 megabyte in size) are reused by a smaller file, for example, 10,000 bytes of data, the remainder of the original file is still present on the drive and these 990,000 bytes of the photo image in this example can be recovered. Forensic practitioners call this “carving” data from the unallocated disk data, because the boundaries of the previous data are no longer defined and must be discovered by the practitioner to successfully recover the data. These data are fragments of previous files, and while recoverable, are incomplete and sometimes present the forensic analyst with difficulty even determining what kind of data it previously was. Data that has been partially overwritten is not likely recoverable, but the remainder of the data that was not overwritten is able to be recovered. Absent context it may not be possible to draw a conclusion from the data so recovered, however sometimes enough information persists that it supports a conclusion alone or in combination with other data recovered.

All data, and every bit stored in the user accessible data area on the disk drive are captured by a forensic image of the entire disk system and are accessible to the forensic analyst in the forensic image. Thus, for all practical purposes, every possible bit and byte of data on the storage device that is accessible is captured and its integrity preserved such that any modification or alteration of the forensic image is detectable.

The data storage device may be a spinning magnetic disk storage device (hard drive), or it may include Solid State Disks (SSD) or other storage devices and may be in a Redundant Array of Independent Disk (RAID) configuration, in which case the data captured in a forensic image will include every bit of data in the logical hard drive exactly as presented to the computer by the data mass storage subsystem. From an evidentiary point of view, the forensic image captures and preserves every bit and byte of data in the logical view of the physical disk. The forensic imaging software copies all the data that can be accessed by the computer system regardless of whether it is partitioned and formatted or not.

Data that has been completely overwritten is not likely recoverable. “Completely overwritten” means that a sector containing 512 bytes of data is overwritten with 512 bytes of new data (random data in the case of “drive wiping” software). The US Department of Defense considers a file containing classified information (up to the Secret classification) to be adequately destroyed and unrecoverable when overwritten with random data 7 times.

In this examination, the term “hard drive image” refers to this exact data set presented to and operated upon by the computer system. It is a complete set of all data accessible to the computer or computer operator and is an accurate reproduction of ALL of the data on the disk system that can be accessed by the computer under examination.

The original data in the integrity-protected forensic archive cannot be altered, and preserves forensic chain of custody, because this examination used an exact copy of from the original preserved in the forensic archive.

In this Appendix the capability of a forensic image has been explained, with the technical detail of hard drive technology to aid in the understanding that the statement that “every bit and byte of data in the hard drive is captured and preserved”, made with reference to the logical view of the data storage medium is technically accurate, and that “every bit and byte of data that can be accessed by a human or a computer

operating system IS captured and preserved”, integrity controlled and evidentially a complete set of all possible data is preserved and presented in the examination.

APPENDIX K. ACCESSING A COMPUTER WITHOUT A PASSWORD

It is a common belief that a password provides safety as a security mechanism.

In this Appendix I discuss some of the many methods by which password can be bypassed, at a high level. Step-by-step instruction is not provided here. Many books have been published⁹³ and many professional instruction courses and certifications⁹⁴ exist for those in the field who need or desire it and it is not my purpose to repeat that content here.

Finding a password

Many resources exist on the Darkweb⁹⁵ to obtain passwords that have been broken by criminals and are either offered for free or for sale. The article cited discusses 1.4 billion passwords available for free on the Darkweb. US Title 18, section 1029 makes trafficking in passwords or access devices a crime. I did not search the Darkweb for these passwords because trafficking in passwords is a crime, the Darkweb is also full of criminal content, some of which the mere possession of without any intent, is a crime, as well as malware and ransomware, often disguised in innocent-looking webpages. Venturing onto the Darkweb is a good way to lose all your computer data as a consequence of encountering these subversive “traps”.

Method #1 is simply looking up the password. Despite the risk of computer infection or damage, many people do use the Darkweb and this content is available in many cases for free. This risk is so prolific that many services monitor this for you, Norton LifeLock and Identity Force among them, by searching for your credentials on the Darkweb and providing notification if your access has been compromised.

Cracking a password

Passwords, when entered, are encrypted and only the encrypted form of the password is stored. When a person enters a password to login, it is again encrypted and the result is compared to the stored encrypted password. The two encrypted passwords are compared and if they match, access is granted. The encrypted, stored password is *never* decrypted in the process of granting access.

It is possible, once the encrypted stored passwords are obtained, to run various “password cracking” software that tries all conceivable combinations of letters, numbers and symbols until a match between the encrypted stored password and the result under test. The password “cracker” outputs the unencrypted password, once found.

Rainbow Tables

Encrypting every possible password (called a “brute force” method) requires an extensive amount of computing power and is remarkably slow. To speed this process up, “rainbow tables” have been created.

⁹³ <https://www.goodreads.com/shelf/show/penetration-testing>

<https://computingforgeeks.com/best-penetration-testing-books-to-buy>

⁹⁴ [Certified Ethical Hacker \(CEH\) Certification](#), [GPEN](#), [Certified Penetration Tester \(CPT\)](#), [PenTest+](#), [ECSA- EC Council Certified Security Analyst](#), [Certified Expert Penetration Tester \(CEPT\)](#), [Licensed Penetration Tester \(LPT\)](#), [OSCP – Offensive Security Certified Professional](#), [OSCE – Offensive Security Certified Expert](#)

<https://alpinesecurity.com/blog/top-penetration-testing-certifications/>

⁹⁵ <https://www.csoonline.com/article/3266607/1-4b-stolen-passwords-are-free-for-the-taking-what-we-know-now.html>

These are tables of encrypted passwords and the corresponding plaintext password allowing the application to simply search the list for a matching entry rather than encrypting every possible combination until a match is found.

Many sources of rainbow tables and the software that uses them exist on the Internet and are readily available.

Bypassing a password

It is possible to bypass a password requirement altogether by using special software on a CD, USB thumb drive or other media or installed by one of many access methods. Security professionals use capabilities like password bypass when a password is forgotten and must be recovered. Microsoft operating systems even include the option to create such a bypass mechanism when the operating system is installed (a password recovery disk). There are many password recovery methods identified on the Internet that perform this function across many different operating systems and are readily available on demand including, specifically, for Microsoft Windows Server 2016 Standard.⁹⁶

Exploitation of Services

Often, in the programming of a computer service, for example, a web server, mistakes and oversights are made in the programming process that leave opportunities for a malicious person to obtain unauthorized access. One such example is the inclusion of “non-printable” characters in an input value (meaning that the included data does not show on a screen). This technique fools the receiving computer into accepting part of the input value as a command that it should execute (a command that means “send me your password file,” for example). There are many different ways to do this, each with their own deep technical explanation (buffer overflow, cross-site scripting, code injection, manipulation of software timing, etc.). There are many penetration testing textbooks that explain the deep technical process and teach how to do this.

These types of mistakes and oversights account for nearly 170,000 identified weaknesses that allow a computer to be attacked. The CVE⁹⁷ system operated by Mitre Corp. has identified 169,169 publicly disclosed vulnerabilities to date. The National Vulnerability Database (NVD⁹⁸) is provided by the National Institute of Technology and Standards (NIST) and contains 808 vulnerabilities that provide full administrative access (between 2005 and the time of this writing). Computer vulnerabilities (weaknesses) are identified nearly daily, and are reported and validated before being published in the CVE or NVD repositories. There exist more vulnerabilities than are publicly known; many are under investigation, not yet validated, while others are known to the US military and intelligence communities and are classified. From these 808 publicly known vulnerabilities, many could be applied to the Mesa County EMS server to grant the type of access demonstrated in this report.

There are entire suites of software that simplify and automate the capability. Manually performing an exploitation may be a difficult process that requires deep technical knowledge but these automated suites simplify the task making it accessible to a larger population of people. For example, Metasploit can obtain access to a system and return to the user a fully logged-in session with administrative access, allowing the

⁹⁶ <https://www.top-password.com/blog/reset-forgotten-windows-server-2016-password/>

⁹⁷ <https://www.cve.org/>

⁹⁸ https://nvd.nist.gov/vuln/search/results?form_type=Basic&results_type=overview&query=administrative+access&search_type=all&isCpeNameSearch=false

malicious user to do whatever they want to with the system, including stealing or altering data. Kali Linux is an operating system (intended for security professionals to test the security of systems) that contains Metasploit and many dozens of other security tools that can be used to exploit a computer system.

Even passwords (and encryption keys) specific to Dominion Voting Systems have been revealed on the Internet, by no less than the U.S. Election Assistance Commission, and are available online at the time of this writing. One such report with the actual system passwords and encryption keys was published more than 10 years ago and is still available online.

Intel Active Management Technology (AMT) and Management Engine (ME)

Every processor made by Intel since 2008, as well as processors made by AMD and others, incorporate a form of this Management Engine (ME) technology.⁹⁹ This has not been popularized broadly but is a serious concern for all computer systems.

Embedded in the silicon of microprocessors is an independent processor with its own operating system. This processor runs even when the power is off (as long as there is power to the motherboard), and is accessible via the computer's network interface. It provides its own IP address and MAC address and is capable of bypassing the operating system.

Vulnerabilities identified in 2017 were identified as critical.¹⁰⁰ Researchers indicated that it was possible to read passwords from memory (among other things) and completely bypass the Operating System of today's computers. While no exploitation of this capability has been identified that we know of, Nation-States (including our own) would consider the ability to be highly classified – to the point – we would not know about it.

The vulnerabilities are known as Meltdown and Spectre. They are side-channel attacks against systems.¹⁰¹

These vulnerabilities if exploited could provide complete access, undetectably, to a system, even with the computer in a “shutdown” state, as long as the system is plugged in (i.e., power is supplied to the motherboard). This continuous power to the motherboard has long been a feature in modern computer systems and is how the “Wake on LAN” feature is able to function ... it is not that the computer has no power, it just has very low power applied.

Dell Integrated Remote Access Controller (iDRAC)

Dell offers a capability known as iDRAC on its servers.¹⁰² It is a completely separate processor with its own Ethernet interface, IP and MAC addresses. It is intended to be used on a highly restricted network for “out of band” management of the server, and allows an administrator (or anyone with access¹⁰³) to reboot the system, access and change the BIOS, and alter the system without the motherboard's processor being able

⁹⁹ https://en.wikipedia.org/wiki/Intel_Management_Engine

¹⁰⁰ <https://www.intel.com/content/www/us/en/support/articles/000025619/software.html>

¹⁰¹ <https://www.intel.com/content/www/us/en/architecture-and-technology/side-channel-variants-1-2-3.html>

<https://www.intel.com/content/www/us/en/architecture-and-technology/side-channel-variants-3a-4.html>

<https://www.intel.com/content/www/us/en/architecture-and-technology/l1tf.html>

<https://www.intel.com/content/www/us/en/architecture-and-technology/mds.html>

¹⁰² <https://www.dell.com/support/kbdoc/en-us/000179517/dell-poweredge-how-to-configure-the-idrac-system-management-options-on-servers>

¹⁰³ Note that this document identifies the default iDRAC userID and password as “root” and “calvin”.

to detect this activity. If you have a server in a data center 30 miles (or more) from your office that needs to be rebooted, and you don't have staff at this remote location, driving an hour or more just to reboot the system is an impediment to productivity – the iDRAC is intended to provide remote control for just this reason.

The primary computer has no way to detect the use of the iDRAC; if used the primary computer's audit and system logs would not record it. An iDRAC is intended to permit access to the core computer and its files.

Strengthening Access Security

One technique for strengthening access security is multi-factor authentication. This is an industry-standard practice and recommended by the National Institute of Standards and Technology (NIST) among many other technical and professional organizations.

Many readers will recognize this multi-factor authentication as something you have already used, once you understand what it is. Multi-factor authentication requires identification be verified by techniques in two or more of the three categories:

1. Something you know (a password, special code, birthday, or other identifying number not related to the information you are accessing),
2. Something you have (an access token, a calculator that accepts an input number and returns an encrypted response, a cellphone where you receive a message to authorize the access, etc.), and
3. Something you are (biometric information, a fingerprint, retina scan, iris scan, face recognition, etc.).

Systems that send you a verification code via cell phone SMS message are a good example of the use of multi-factor authentication.

Best practice in access security is to apply the principle of "Defense in Depth," which is to apply multiple layers of security such that if one fails another serves to protect the system. A "hardened" system requires Defense in Depth, and the proper implementation of multiple security mechanisms, as specified in the DoD Security Technology Implementation Guides (STIGs).

The US Department of Defense employs thousands of military and contractor staff who work full-time on the problem of maintaining sufficient cybersecurity to (hopefully) stay ahead of the threat. Homeland Security maintains a significant cybersecurity division, as does the National Security Agency (NSA) and other parts of the US intelligence community; the Critical Infrastructure Security Agency (CISA) is dedicated to this mission; NIST maintains an entire division for cybersecurity; the DOJ maintains its own capability for the investigation and prosecution of these High-Tech crimes and the High-Tech Criminal Investigator's Association (HTCIA) provides a public private partnership with their law enforcement counterparts. This is a gross understatement of the problem and the resources allocated to address it. Part of the mission of the FBI InfraGard program is to maintain a public-private partnership with the civilian operators of US national critical infrastructure to thwart cybercrime and cyber threats against the USA. The US Secret Service maintains an Electronic Financial Crimes Task Force (EFCTF) to pursue financial cybercrimes. The budget for these efforts far exceeds several billion dollars annually.

Yet our election security depends on temporary workers with very minimal training and no requirement for cybersecurity knowledge, training or certification. DoD requires thousands of security professionals. Is our election infrastructure less important?

The ability to obtain access to a computer without a password is a persistent problem and will continue to be because computers are programmed by humans; and humans are not perfect, they make mistakes.

Unfortunately, there are enough nefarious people in the world exploiting these weaknesses for their own benefit, that this problem is not likely to ever end.

APPENDIX L. SUPPLY CHAIN SECURITY THREAT AND FOREIGN MANUFACTURING

The United States is a significant target of espionage from foreign adversaries. According to the US Director of National Intelligence in their Supply Chain Risk Management Best Practices¹⁰⁴ document,

“The U.S. is under systematic assault by Foreign Intelligence Entities (FIEs) who have augmented traditional intelligence operations with nontraditional methods, including economic espionage, supply chain exploitation, and the use of students, scientists, and corporate employees, to collect both classified and unclassified information. The scale of this effort has put entire industries at risk. Specifically, the globalization of supply chains presents a major attack vector, characterized by a complex web of contracts and subcontracts for component parts, services, and manufacturing. FIEs use this complexity to obfuscate efforts to penetrate sensitive research and development programs, steal vast amounts of personally identifiable information (PII) and intellectual property (IP), and insert malware into critical components. Supply chain exploitation, especially when executed in concert with cyber intrusions, malicious insiders, and economic espionage, threatens the integrity of key U.S. economic, critical infrastructure, and research/development sectors.”

With the growth of global competition, industry in the US is driven to source materials, components, and finished goods from other countries where costs are significantly lower. However, FIEs continue to insert operatives into these foreign supply chains to the USA where they might be strategically positioned to infiltrate supplies using espionage techniques, including inserting surveillance devices into manufactured goods.

This activity includes the contamination of manufactured electronic components with surveillance devices that record and retransmit audio, video and computer data to their foreign controllers.

Presidential Executive Orders 13959¹⁰⁵ signed by President Trump declared a National Emergency (Addressing the Threat From Securities Investments That Finance Communist Chinese Military Companies) and Presidential Executive Order 14032¹⁰⁶ signed by President Biden continued and expanded that National Emergency, banning investment in listed foreign companies. These include manufacturers like Huawei, China Telecom, cellphone manufacturers and electronics manufacturers that have conducted espionage against the US by means of installing covert surveillance devices in equipment during its manufacture.

Infiltration of the supply chain includes the use of hardware and software alterations to systems. The SolarWinds attack on the US Government involved a software infiltration of the supply chain.¹⁰⁷

¹⁰⁴ <https://www.dni.gov/files/NCSC/documents/supplychain/20190405-UpdatedSCRM-Best-Practices.pdf>

¹⁰⁵ <https://www.federalregister.gov/documents/2020/11/17/2020-25459/addressing-the-threat-from-securities-investments-that-finance-communist-chinese-military-companies>

¹⁰⁶ <https://www.federalregister.gov/documents/2021/06/07/2021-12019/addressing-the-threat-from-securities-investments-that-finance-certain-companies-of-the-peoples>

¹⁰⁷ <https://www.asisonline.org/security-management-magazine/articles/2021/03/spies-in-the-supply-chain/>

These alterations of hardware and software are incredibly sophisticated. The alteration of electronic computer chips to plant malicious circuitry¹⁰⁸ in the design of silicon integrated circuits has been demonstrated at the University of Michigan.¹⁰⁹

FBI Director Christopher Wray stated that Chinese spying in the U.S. is so widespread the FBI must launch two counterintelligence investigations a day to counter it.¹¹⁰ China is focused on stealing U.S. technology to increase its capabilities while shortening the research and development time. The FBI currently has over 2,000 active counterintelligence cases related to China.

Bloomberg reported about China's infiltration of the motherboards of Supermicro computers,¹¹¹ manufactured outside the United States and how the insertion of a small chip on the motherboard compromised dozens of companies in the US.

The use of components fabricated, assembled and, or manufactured outside the US, whether furnished as individual parts, assemblies or finished goods, exposes them to the risk of foreign exploitation.

As Bloomberg claimed about the exploitation of Supermicro computers, sourcing components from foreign suppliers presents a supply chain risk that can only be avoided by domestic sourcing.

¹⁰⁸ <https://www.wired.com/2016/06/demonically-clever-backdoor-hides-inside-computer-chip/>

¹⁰⁹ <https://web.eecs.umich.edu/~taustin/papers/OAKLAND16-a2attack.pdf>

¹¹⁰ <https://forwardobserver.com/dailysa-fbi-blown-away-by-chinese-spying/>

¹¹¹ <https://www.bloomberg.com/news/features/2018-10-04/the-big-hack-how-china-used-a-tiny-chip-to-infiltrate-america-s-top-companies>



News Release

Media contact

303-860-6903

Annie Orloff

annie.orloff@sos.state.co.us

Steve Hurlbert

steve.hurlbert@sos.state.co.us

State of Colorado Department of State

1700 Broadway

Suite 550

Denver, CO 80290

Jena Griswold

Secretary of State

Chris Beall

Deputy Secretary of State

Statement from Colorado Secretary of State's Office Regarding an Official Order to Appoint Sheila Reiner and an Advisory Committee to Supervise Mesa County Elections

Denver, August 17, 2021 - Today, the Colorado Secretary of State's office issued an [Order](#) to appoint Mesa County Treasurer Sheila Reiner to supervise all conduct of the Mesa County elections and establish a three-person advisory committee including Representative Janice Rich, Ouray Clerk and Recorder Michelle Nauer, and former Secretary of State Bernie Buescher to advise and assist Reiner in her duties.

"The people of Mesa County deserve safe and secure elections. I am confident that with these appointments, voters in Mesa will be able to exercise their constitutional right to have their voices heard in our democracy. As Secretary of State, my top priority is to ensure all election security protocols are followed and to safeguard Coloradans' right to vote and we will continue to conduct the business required of our office to provide oversight, to ensure the integrity of the state's elections," said Colorado Secretary of State Jena Griswold.

"In light of the ongoing investigation into the chain-of-custody and election security protocol breach in Mesa County, the Colorado County Clerks Association supports the Colorado Secretary of State's designation of an interim election official to conduct and oversee elections in Mesa County until the investigation is complete. While unusual, this important step of placing a top-notch election expert in the office will ensure a safe and secure election

is conducted for the citizens of Mesa County,” said Matt Crane, Executive Director of the Colorado County Clerks Association.

While Department of State staff is continuing to conduct analysis and awaiting additional information, as well as the outcome of a criminal investigation, several facts have prompted substantial concern regarding the ability of the Mesa County Clerk and Recorder’s office to execute an election in compliance with statute and rule. Of particular concern:

- Mesa County authorized a non-employee, Gerald Wood, to attend the May 25, 2021 trusted build, in clear violation of Election Rule 20.5.4. The Department has confirmed that this individual was present at the May 25, 2021 trusted build event. The Department has determined that Mesa County Clerk and Recorder employees Belinda Knisley and Sandra Brown participated in facilitating the improper presence of this non-employee during the trusted build event by misrepresenting the individual’s employment status and role.
- Footage, both video and photos, was posted online showing the BIOS passwords for Mesa County’s voting system. The Department knows from the timestamp on the video and from other evidence that it is likely this sensitive information was filmed and collected during the limited access trusted build installation in Mesa County on May 25, 2021. This meeting was limited only to a minimal number of Department of State staff, voting equipment vendor staff, and three individuals approved to attend by Mesa County: Clerk Tina Peters, Sandra Brown, and Gerald Wood.
- Video surveillance of the Mesa County voting equipment was not continuous and cannot confirm chain of custody of voting equipment. The evidence suggests that an individual in the Mesa County Clerk’s office directed Mesa County staff to turn off video surveillance of the voting equipment prior to the May 25, 2021 trusted build. The video surveillance cameras were not turned back on until well after the trusted build had been completed, which is inconsistent with the Department’s understanding of the normal course of business practice in Mesa County.
- Two hard drive images from Mesa County election servers were released on the internet during the week of August 9, 2021. Analysis confirms that these images belong to Mesa County hard drives and were created before and after the May 25, 2021 trusted build. The only method to make such copies is to physically access the machines.
- One of the hard drive images is believed to have been taken on Sunday, May 23, 2021. The Department has confirmed that Clerk Peters, Sandra Brown, and Gerald Wood accessed the area where election equipment was stored outside of normal work hours on May 23.

At this time, it is clear that the facts uncovered in the Mesa County Clerk and Recorder’s office require that the Secretary of State exercise her authority as Colorado’s chief election official pursuant to 1-1-107, C.R.S. to supervise all elections occurring under the authority of Title 1 of the Colorado Revised Statutes in order ensure compliance with all election statutes and rules.

Effective immediately and until revoked by the Secretary of State through subsequent order, Sheila Reiner the Mesa County Treasurer and former Mesa County Clerk will supervise all

conduct related to elections occurring under the authority of Title 1 of the Colorado Revised Statutes. The newly formed advisory committee will be responsible for advising and assisting Reiner and will include Representative Janice Rich, Ouray Clerk and Recorder Michelle Nauer, and former Secretary of State Bernie Buescher.

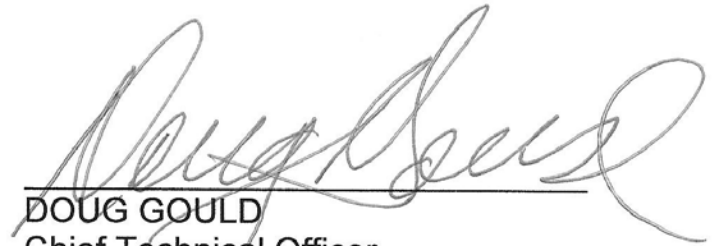
The committee will participate in weekly meetings with Ms. Reiner during the preparation for and execution of an election, unless Ms. Reiner and the committee decide upon another frequency. The committee shall also be permitted to participate in election functions as designated by Ms. Reiner. The Mesa County Clerk and Recorder and staff will take any and all lawful direction from Ms. Reiner and any other Secretary of State designee on any and all election matters.

Given the deadline to purchase, certify, and install trusted build on election equipment before August 31st, a swift appointment was required to ensure safe and secure elections in Mesa County.

###

The foregoing Forensic Examination and Report was prepared by me and I am responsible for its content.

This 28th day of February, 2022.



DOUG GOULD
Chief Technical Officer
CyberTeamUS

Doug Gould Biography

Doug Gould is an expert in Cyber Security with more than 40 years' experience in the field. Doug retired from AT&T after 31 years, where he served as Chief Cyber Security Strategist. He currently serves as Chief Technical Officer at CyberTeamUS.



Doug began at AT&T with Bell Laboratories, serving in the Semiconductor Laser Development department and later in the Bell Lab's Security Group, as a delegate to the Bell Labs' Unix Systems

Subcommittee, was an early pioneer in the field of Computer Forensics and won a Bell Labs Innovation Award. At AT&T he designed the security architecture for one of the largest states in the US, consulted with cabinets of the nations' largest corporations and designed the first healthcare network fully compliant with Healthcare Information Exchange standards. Outside AT&T, he has overseen security for a US Government Agency and has solved major cases for the FBI and Secret Service; he has served as an Officer of the Court as a forensic expert and has been an expert witness in landmark cybersecurity cases. He designed security architectures for DoD networks including some of the most sensitive areas of the Government. Doug has owned and led several professional services firms in the Information Security field. He served on the NC Council for Entrepreneurial Development and has consulted with many companies about the complex integration of business and technology.

Doug is the past president of Eastern North Carolina InfraGard, the public-private partnership between the nation's critical infrastructure operators and the US Intelligence community.

Doug's background is at the Master's level in Electrical Engineering, Computer Science, Computer Security and Business Administration.

He is a subject matter expert in:

- Strategic Enterprise Security
- Security Architecture & Design (including network Micro-Segmentation)
- Security Governance
- Risk Management

- Security Device Technologies (Firewalls, IDS/IPS, DLP, SIEMs, Encryption, VPNs, Unified Threat Management, etc., Enterprise, Remote and Cloud)
- Information Forensics (Computer & Network Forensics)
- Public Key Infrastructures
- Identity and Access Management
- Authentication, Authorization and Access Control (incl Biometrics)
- Regulatory Compliance
- Physical Security (Threat Assessment/Risk Analysis, TSCM, Access Control, Counterterrorism & Counterintelligence, facility and site protection)
- Business Continuity & Disaster Recovery Planning
- Response & Recovery Strategy
- Threat Intelligence
- Intelligence Analysis

Doug served as Chief Information Security Officer at the World Institute for Security Enhancement, has written advanced security courses, developed advanced security methodologies and has taught government, private sector professionals and law enforcement agents information security, computer forensics, advanced computer forensic sciences and Technical Surveillance Countermeasures (TSCM).

Doug holds numerous certifications in security including the CISSP and Certified Anti-Terrorism Specialist (CAS), as well as numerous instructor certifications in security.

Doug currently serves as Chief Technical Officer at CyberTeamUS.

He is a Vietnam-era US Navy Veteran where he worked in Electronic Warfare and Electronic Intelligence.

Doug is an invited conference speaker.

Doug Gould Forensic Addendum

Major Forensic Cases

- 1986 – Disclosure of National Security Information
Discovered a leak of highly classified information and was able to identify the perpetrator within a group of 15 people. The FBI and US Naval Investigative Service brought this to resolution.
- Early 1990's – US Secret Service investigation, "Mothers of Doom" hacker case
At USSS Evidence Lab, in response to a request for assistance from USS SA Jack Lewis, performed evidence recovery and identified 800 pages of evidence, invalidating immunity of a suspect's testimony in a proffer session.
- Late 1990's – Interpath, a North Carolina Internet Service Provider (ISP)
This ISP was a tier-1 (top level) provider infected with Stacheldraht malware. Investigated the live (running) server and identified that all evidence on disc had been deleted. The only remaining evidence was a running program in memory, which was recovered. This case changed the Best Practice in Forensics – no longer is the first step necessarily removing the power. Had that been done no evidence would remain in this case.
- Late 1990's – As senior security administrator for the US EPA, investigated a complaint from the White House of computer intrusions and discovered an international attack involving 4 countries. Wrote monitoring and tracking software to capture the perpetrator online, brought together the FBI, Royal Canadian Mounted Police (RCMP), Scotland Yard and Deutsche Bundespost in a live investigation tracking the intruder resulting in an arrest in Germany.
- South Carolina – A Public Works supervisor accused of violation of county policy was fired and brought countersuit. Forensic investigation recovered 4 3" thick binders of evidence showing sexual misconduct. Countersuit dismissed.
- Discovered Al Qaida attack plans targeting US Soil. Working with the FBI, the perpetrator, who was a foreign citizen in the US. Arrest made within 48 hours and the attack was thwarted.
- Mid-2000's – Florida vs. Rabinowicz – in a case where possession of contraband was the only element of proof, stipulated that the contraband was authentic and present. I proved forensically that the defendant was not technically in possession of the evidence and that evidence was planted. Qualified as an expert witness and provided expert testimony in this case.
- Mid-2000's – Identified a leak of national security from Oak Ridge National Laboratory involving chemical weapon information using forensic analysis and was able to identify the perpetrator. DSS responded and resolved the case.
- Mid-2000's – Investigated sabotage of a health industry contractor. The systems administrator had been fired and sabotaged the system. Solved the case and the administrator went to prison.

Instructor of Forensics

- Taught Forensics and Advance Forensic Techniques to State Law Enforcement, Military and major corporate customers at the World Institute for Security Enhancement.
- Taught Technical Surveillance Countermeasures (TSCM) course for government and industry at the World Institute for Security Enhancement.

Wrote the entire course and taught the entire CISSP curriculum at Able Information Systems.