

MESA COUNTY
CLERK & RECORDER

Hon. Janet Rowland

Board of County Commissioners

544 Rood Ave. Grand Junction, CO

March 1, 2022

RE: Forensic Report No. 2 on EMS Server Images

Dear Commissioner Rowland:

Enclosed is the second report, in electronic and hard copy form, from the cybersecurity experts who have continued to analyze the forensic images of the drive of the DVS Democracy Suite Election Management System in my office which we used for the management of the 2020 general election and the 2021 City Council Election. As you know, I had these images taken to preserve election records and help determine whether the county should continue to utilize the equipment from this vendor. Because the enclosed report reveals shocking vulnerabilities and defects in the current system, placing my office and other county clerks in legal jeopardy, I am forwarding this to the county attorney and to you so that the county may assess its legal position appropriately. Then, the public must know that its voting systems are fundamentally flawed, illegal, and inherently unreliable.

From my initial review of the report, it appears that our county's voting system was illegally certified and illegally configured in such a way that "vote totals can be easily changed." We have been assured for years that external intrusions are impossible because these systems are "air gapped," contain no modems, and cannot be accessed over the internet. It turns out that these assurances were false. In fact, the Mesa County voting system alone was found to contain thirty-six (36) wireless devices, and the system was configured to allow "any computer in the world" to connect to our EMS server. For this and other reasons—for example, the experts found uncertified software that had been illegally installed on the EMS server—our system violates the federal Voting System Standards that are mandated by Colorado law.

As the county officer elected to manage our elections in accordance with the law, I cannot hide behind the Secretary of State's certification of the Democracy Suite system and ignore the numerous and profound deficiencies revealed in this report. As the experts point out, the Secretary of State's certification itself was unlawful, based as it was on testing performed by an unaccredited lab, a lab that missed 100% of the security issues that render the system unusable, uncertifiable, and illegal. The county must reassess its recently-renewed lease agreement and consider its legal options immediately. We cannot continue to use this equipment. Please respond once you have read the enclosed report.

Very truly yours

Tina M. Peters

Tina M. Peters

Mesa County Clerk & Recorder

200 S. Spruce Street | Grand Junction, CO 81501

Tina.Peters@MesaCounty.US Office (970) 244-1714 Cell (970) 812-2610

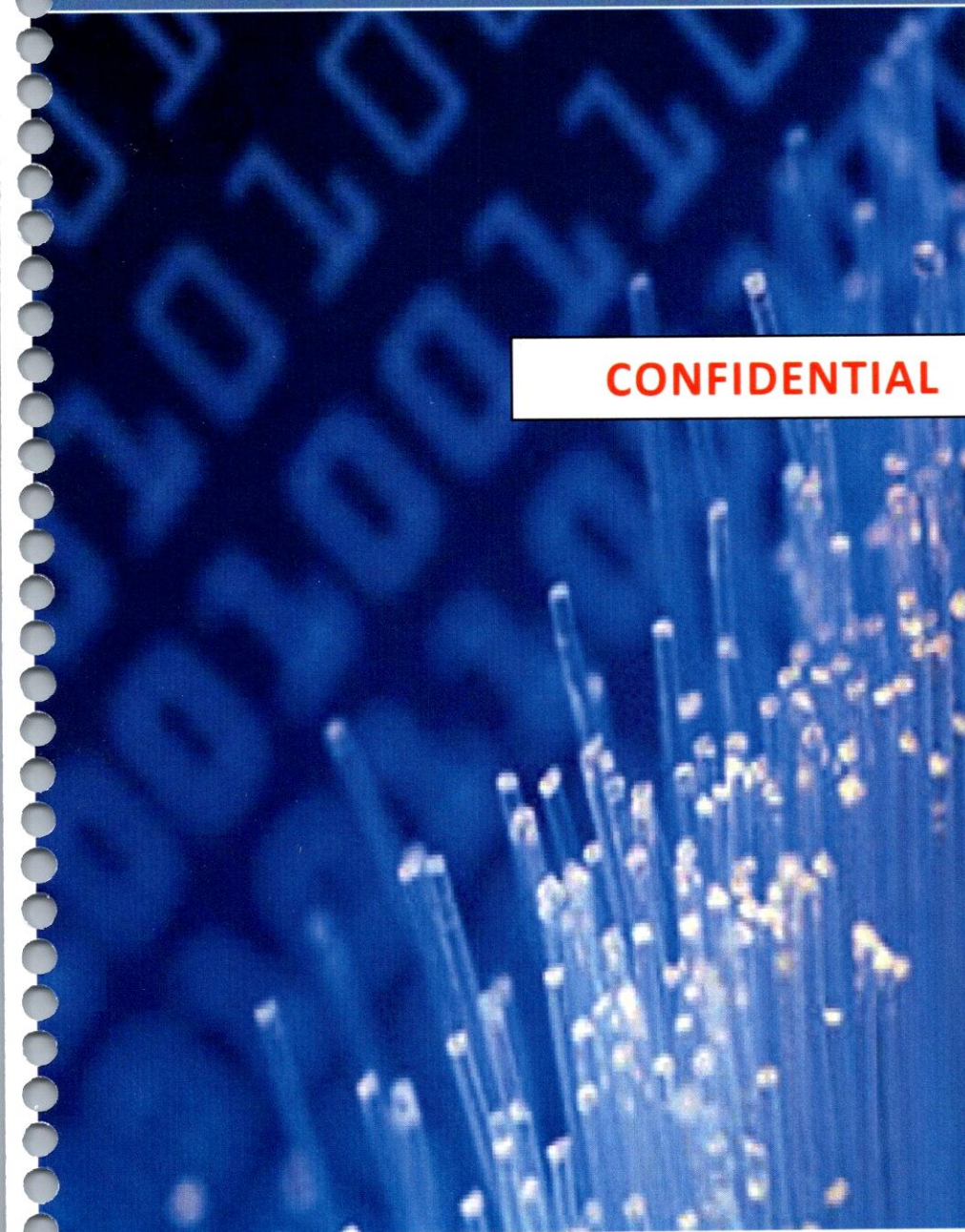


**Mesa County
Colorado
Voting System**

Report #2

Forensic Examination and Analysis Report

CONFIDENTIAL



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.....	127
Bypassing a password	127
Exploitation of Services.....	127
Intel Active Management Technology (AMT) and Management Engine (ME)	128
Dell Integrated Remote Access Controller (iDRAC)	129
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 - "internalMachinelid" 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 unauditable "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

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

⁸ https://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.

CONFIDENTIAL

can perform such an intrusion. It is not possible to reconcile these massive security failures with the obvious 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, foreseeably, 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

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.

CONFIDENTIAL

(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.

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/8CCR1505-1/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>

CONFIDENTIAL

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).

CONFIDENTIAL

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.

CONFIDENTIAL

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

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.

CONFIDENTIAL

highly likely to have occurred across Colorado and possibly other jurisdictions. The configuration of the 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.

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.

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, 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, 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.

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/>

CONFIDENTIAL

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 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.

CONFIDENTIAL

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

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.

CONFIDENTIAL

enables direct access to the vote data. This dangerous combination constitutes what is commonly known 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 **Error! Reference source not found.** 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.

CONFIDENTIAL

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.

CONFIDENTIAL

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.

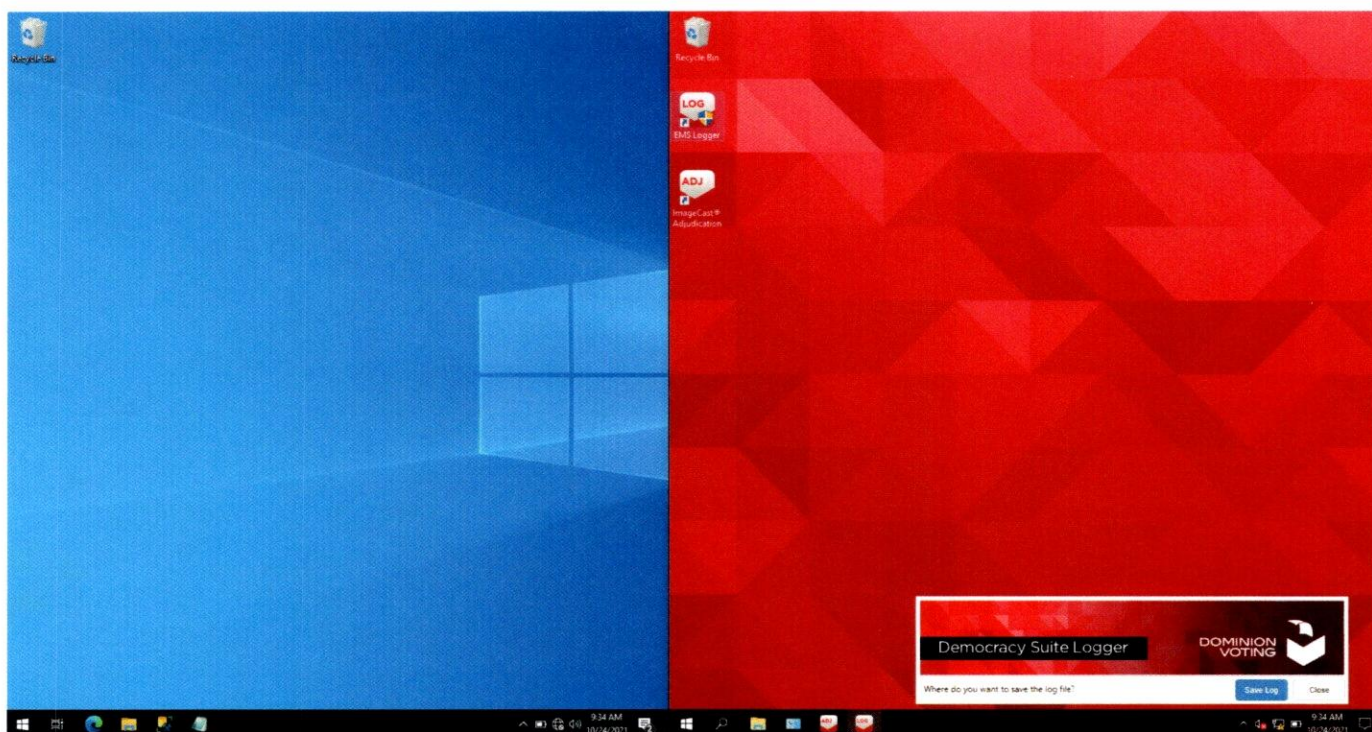


Figure 3 - Test Workstation and Dominion EMS server

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

CONFIDENTIAL

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.

environments on a single computer, but the results were verified and duplicated using two different computers and 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.

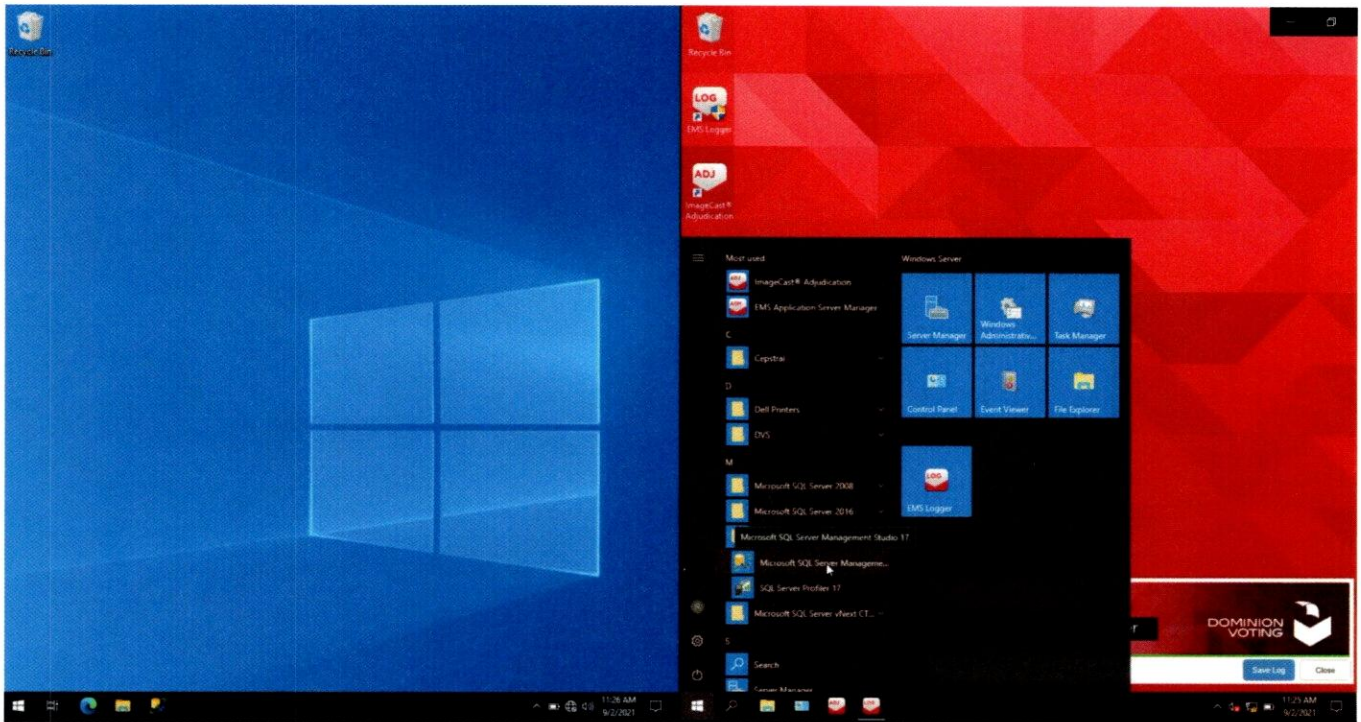


Figure 4 - Installed Microsoft Software

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.

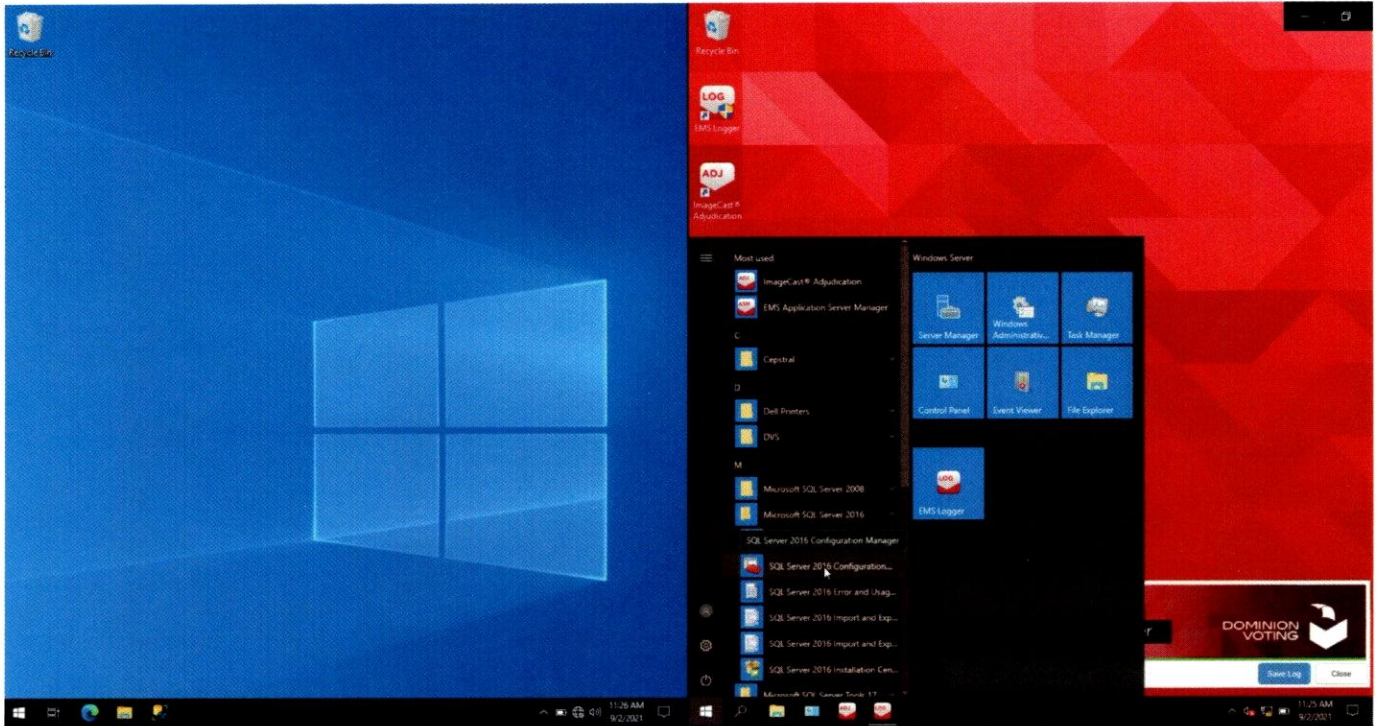


Figure 5 - SQL Server 2016 Configuration Manager

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.

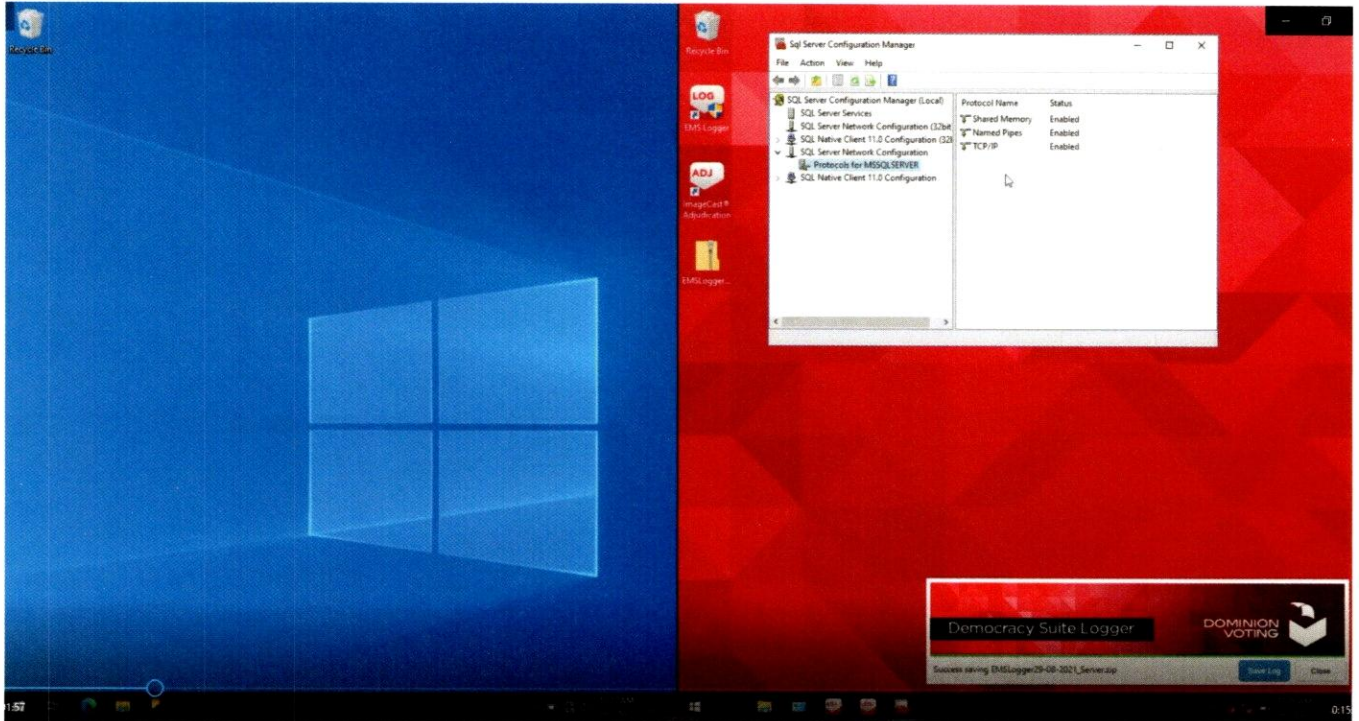


Figure 6 - SQL Server 2016 Configuration Manager – Network Protocols enabled

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>

CONFIDENTIAL

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.

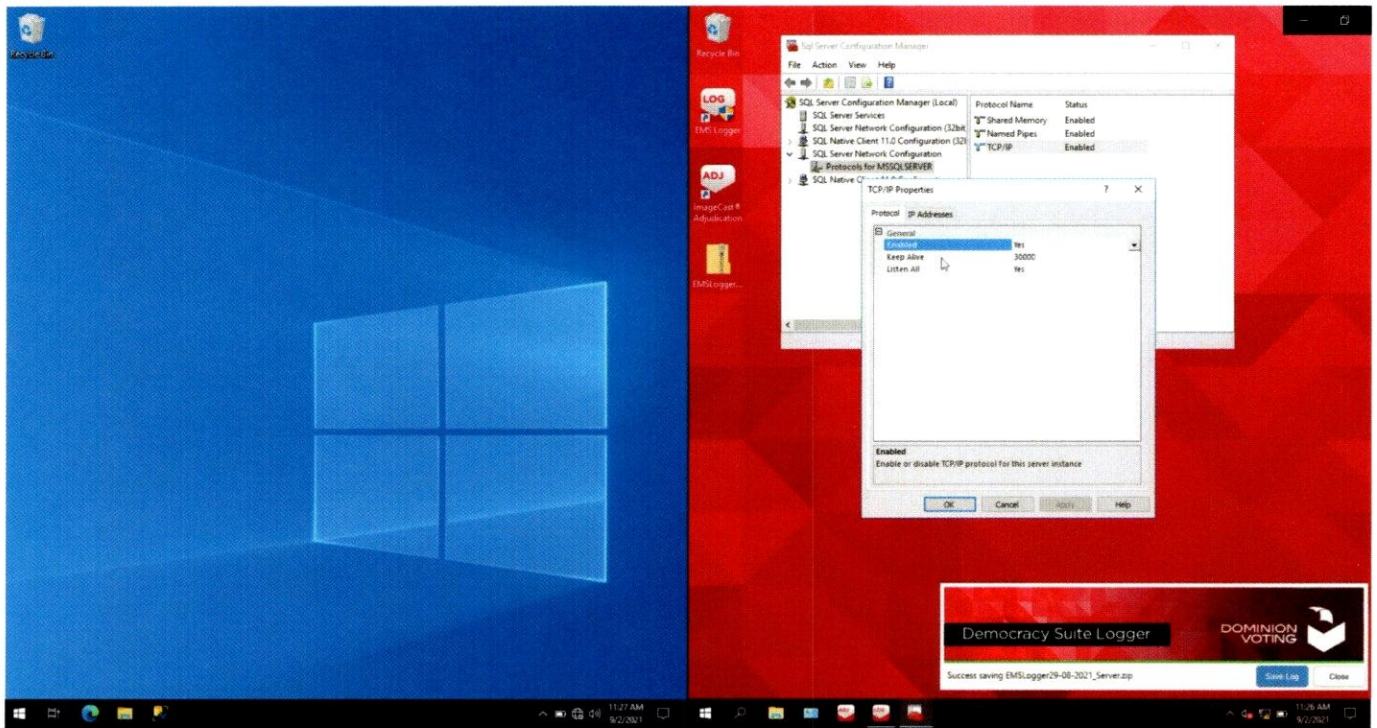


Figure 7 - TCP/IP Properties

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.

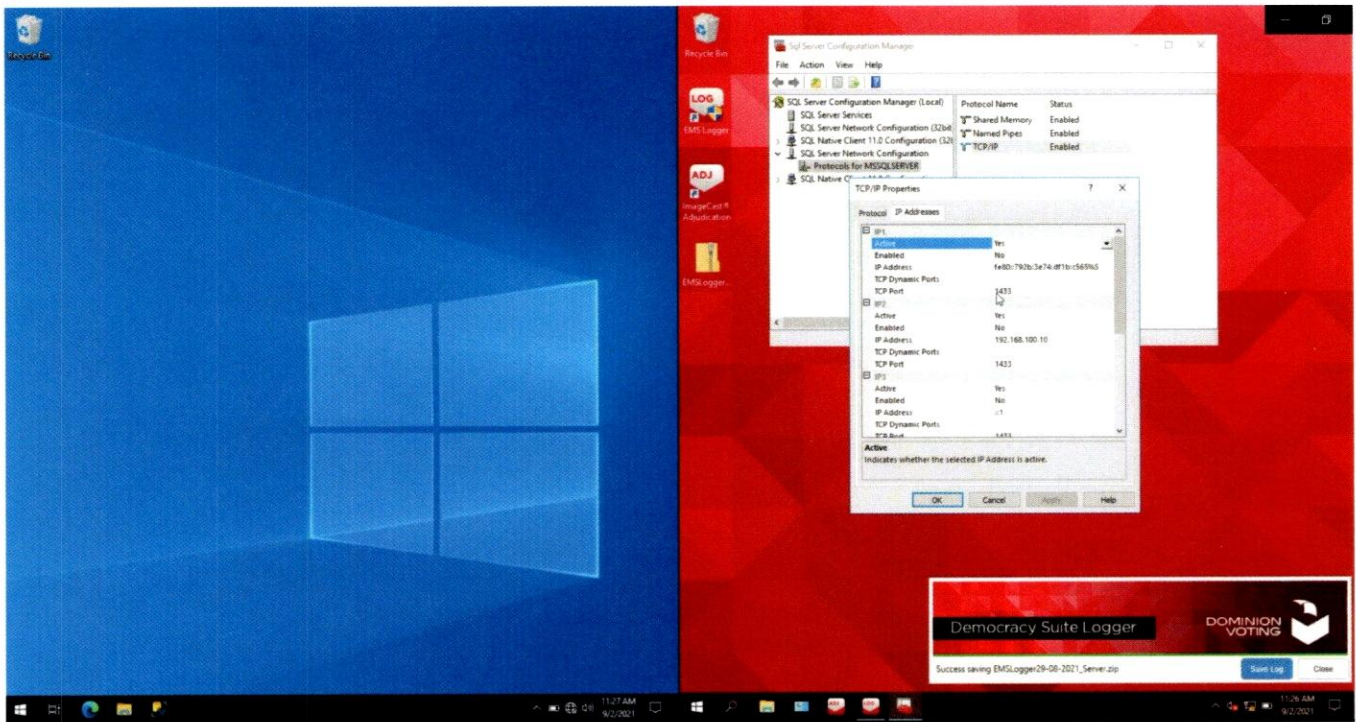


Figure 8 - TCP/IP Properties of SQL Server, attached to port 1433 the standard (default) port.

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

CONFIDENTIAL

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.

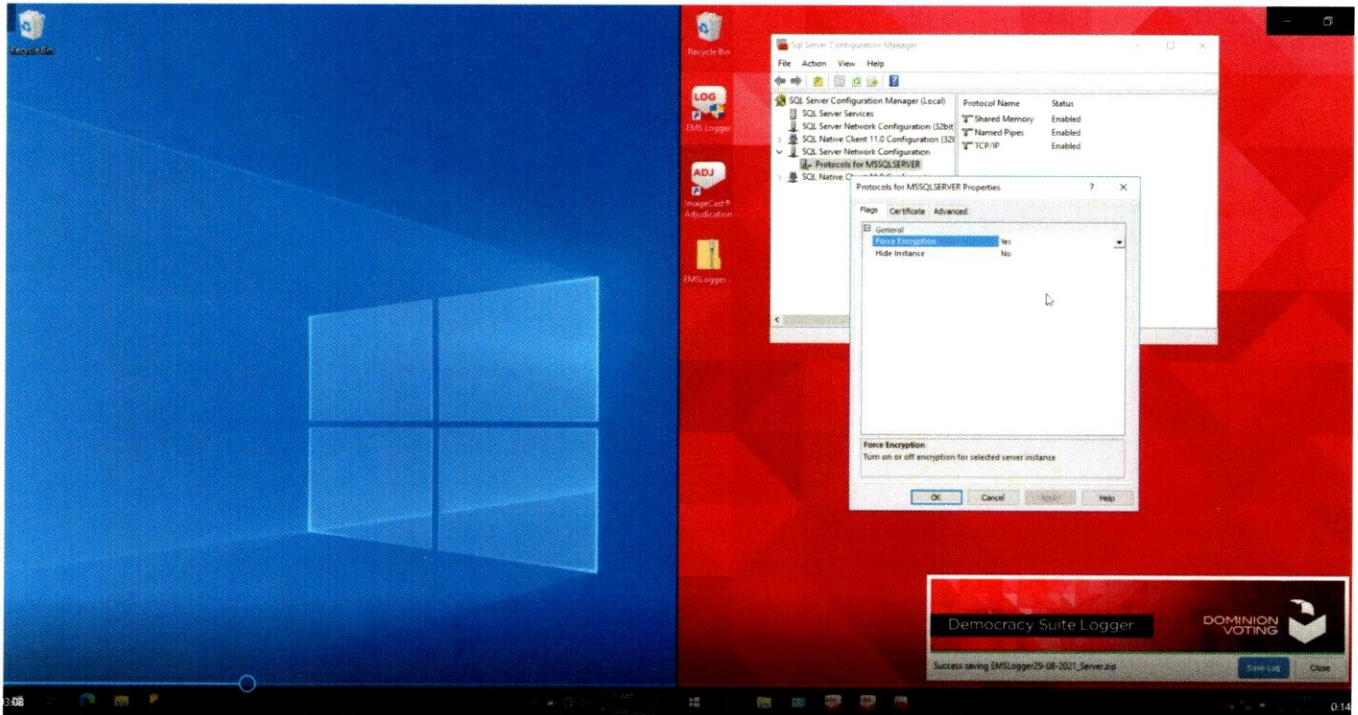


Figure 9 - SQL Server Properties

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.

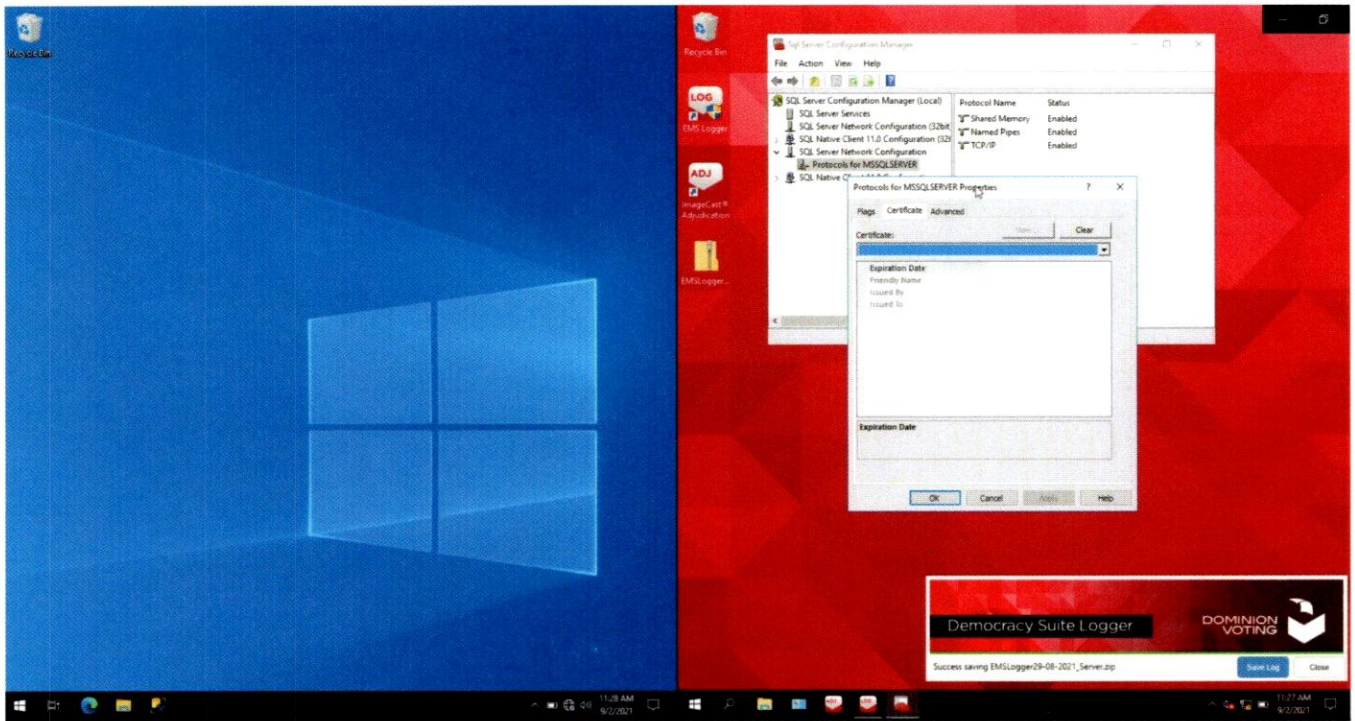


Figure 10 - Encryption is enabled but No Encryption Certificate is configured

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>)

CONFIDENTIAL

EXAMINATION OBJECTIVE 1:

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

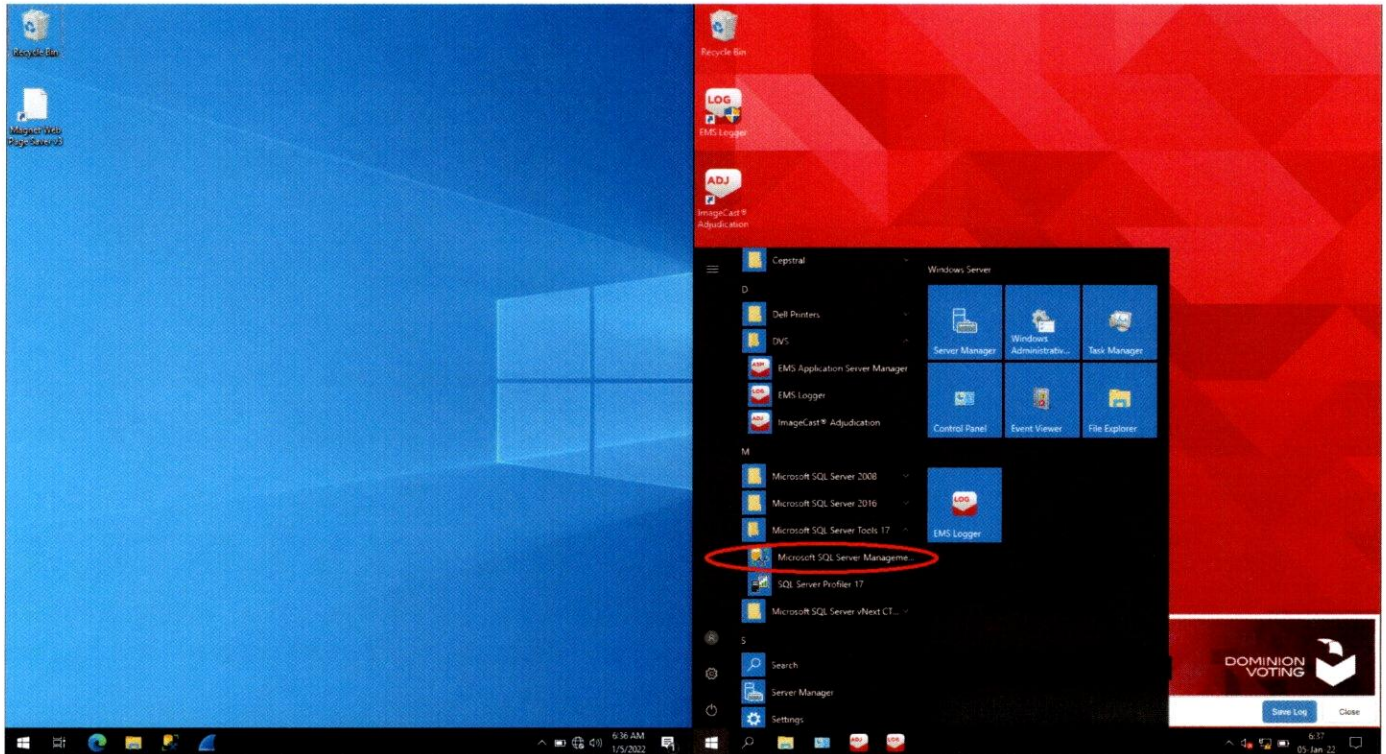


Figure 11 - SQL Server Management Studio (SSMS) software showing in the EMS server Start Menu

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.

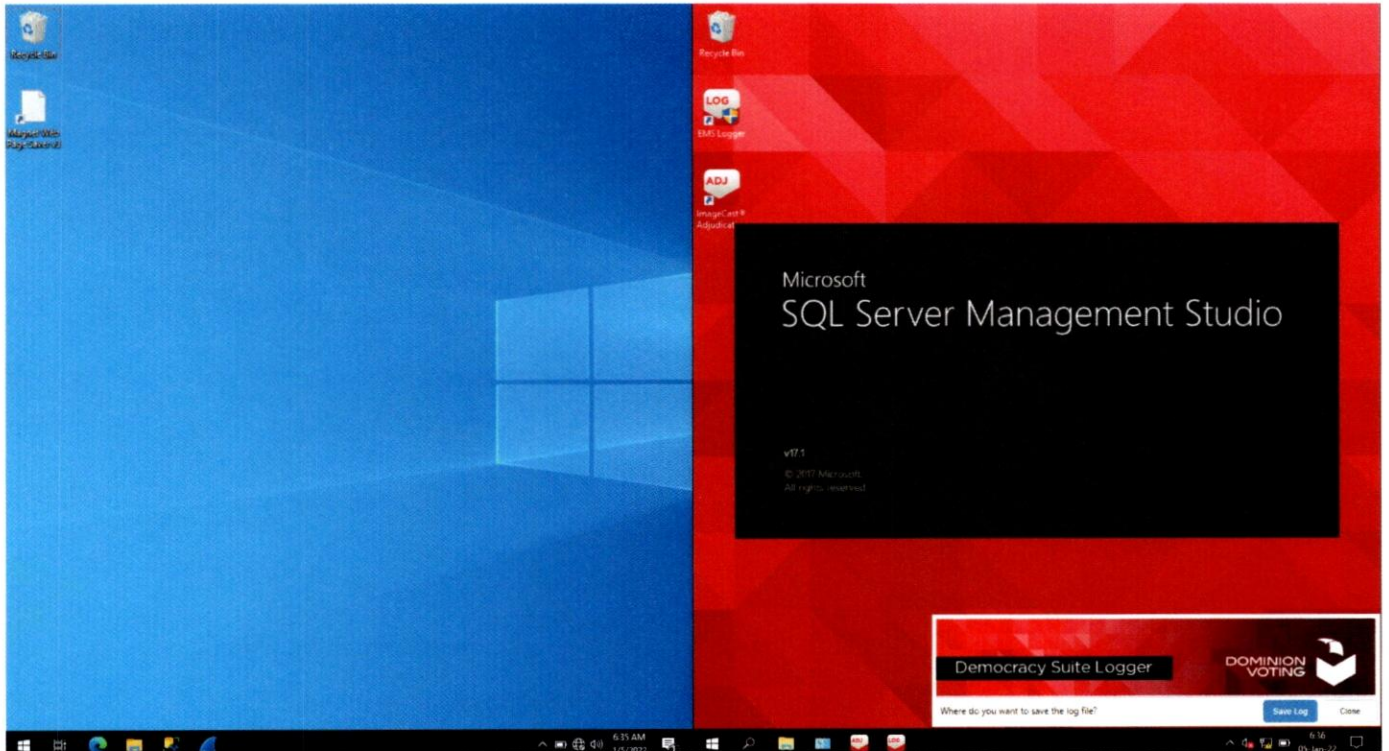


Figure 12 - SSMS is installed and starting on the EMS server system.

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.

CONFIDENTIAL

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.

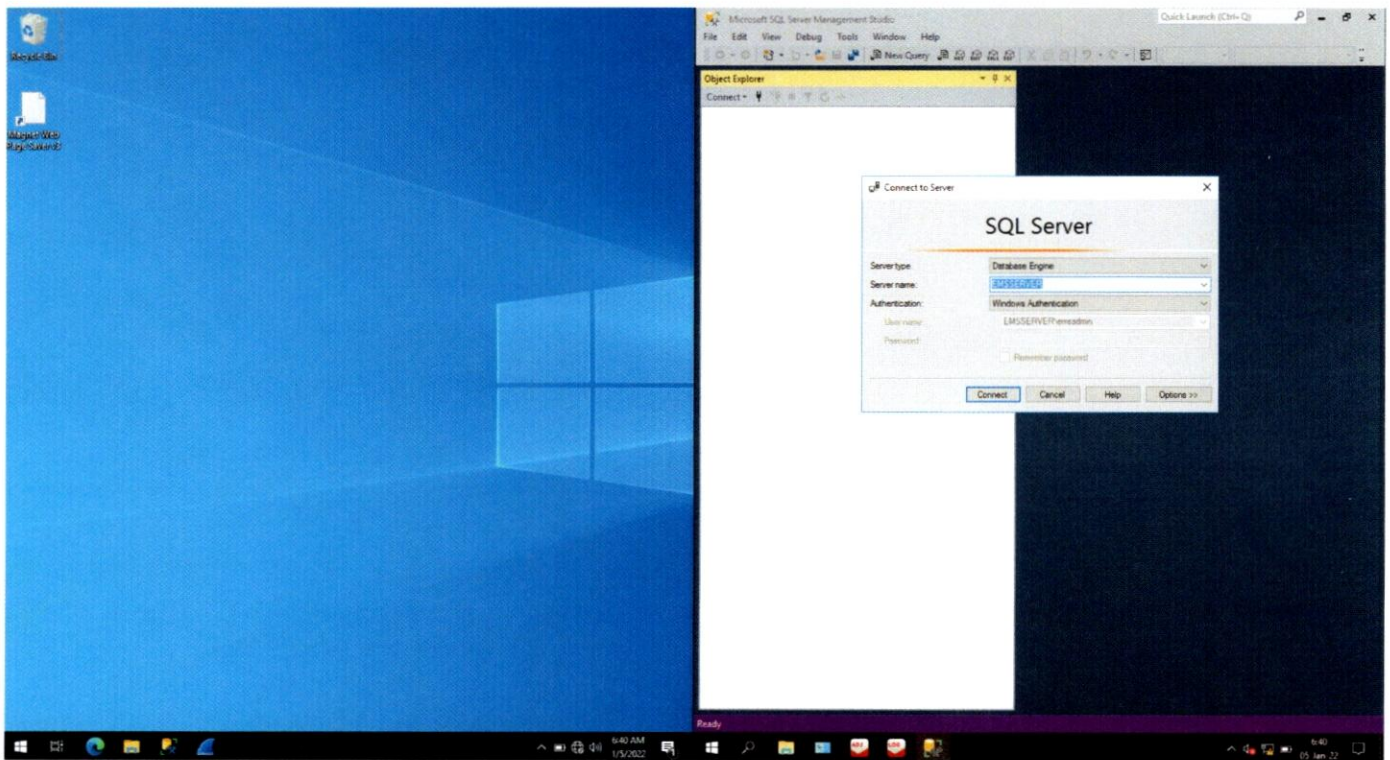


Figure 13 - Logging in to the SQL Server using SQL Server Management Studio

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.

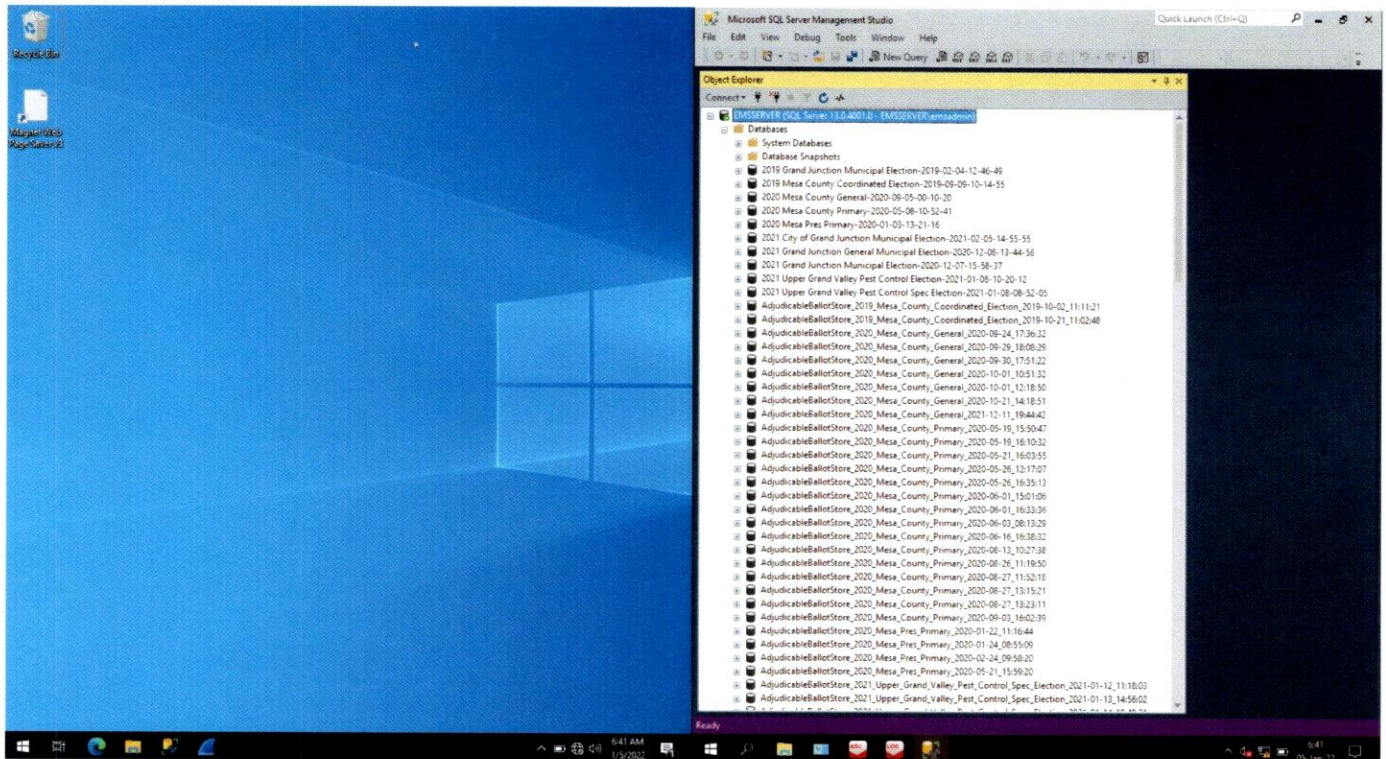


Figure 14 - SSMS enables direct access to the internal databases to anyone logged in to the EMS server

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.

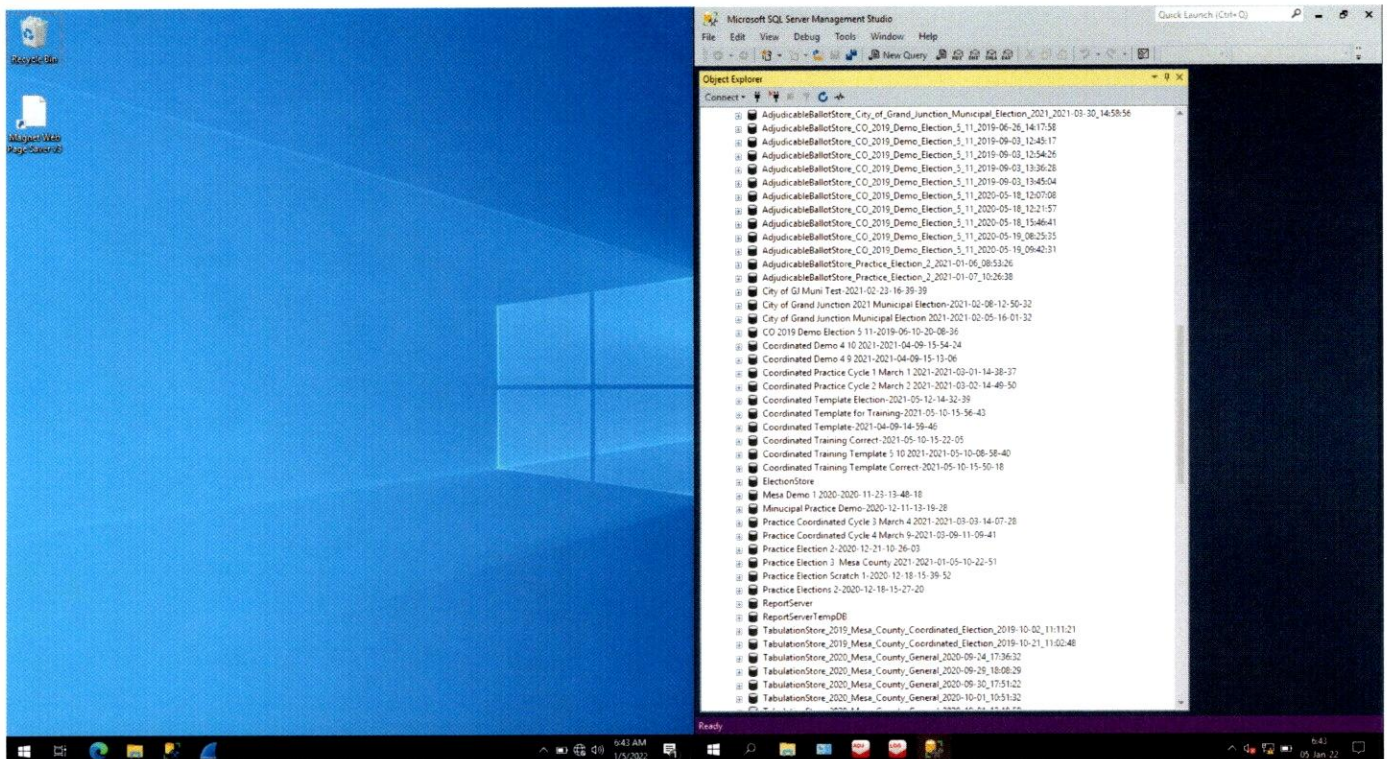


Figure 15 - Databases from many prior elections are fully accessible

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.

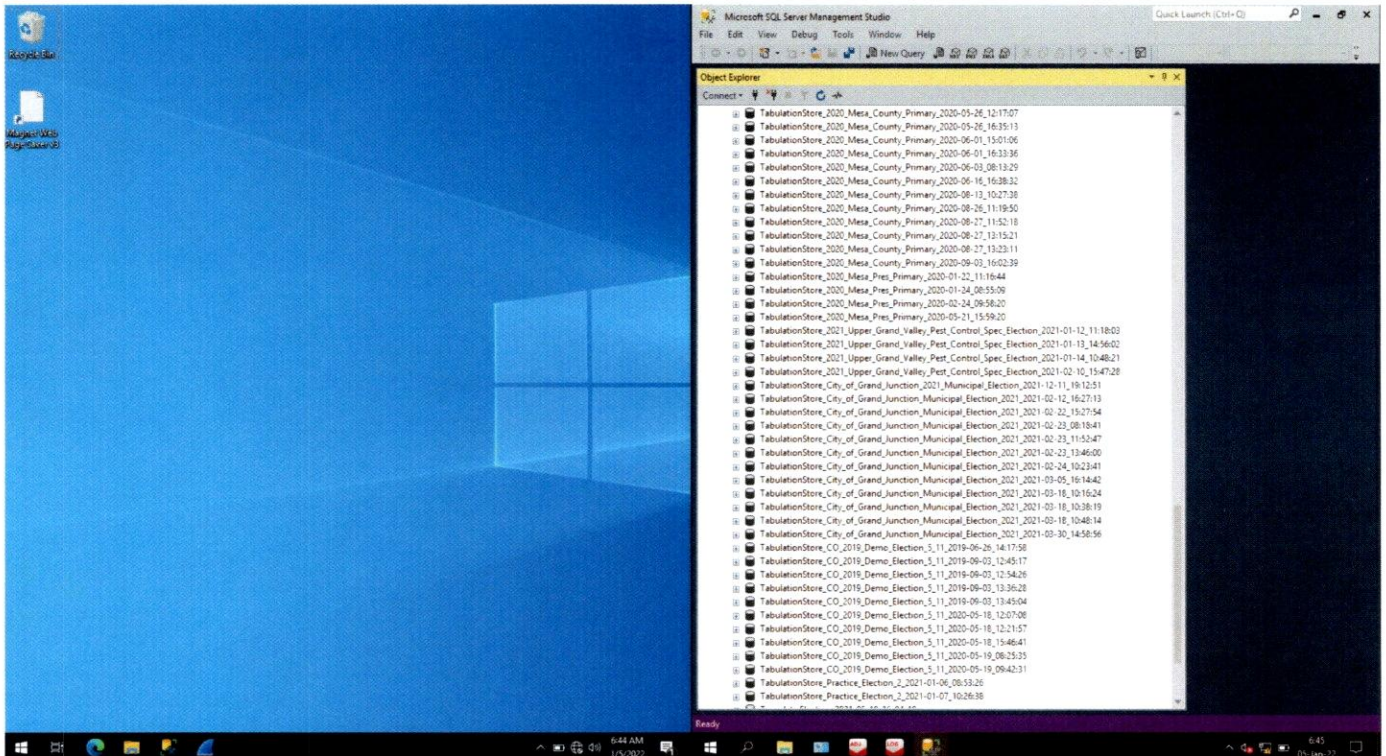


Figure 16 - Additional databases used in previous elections

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.

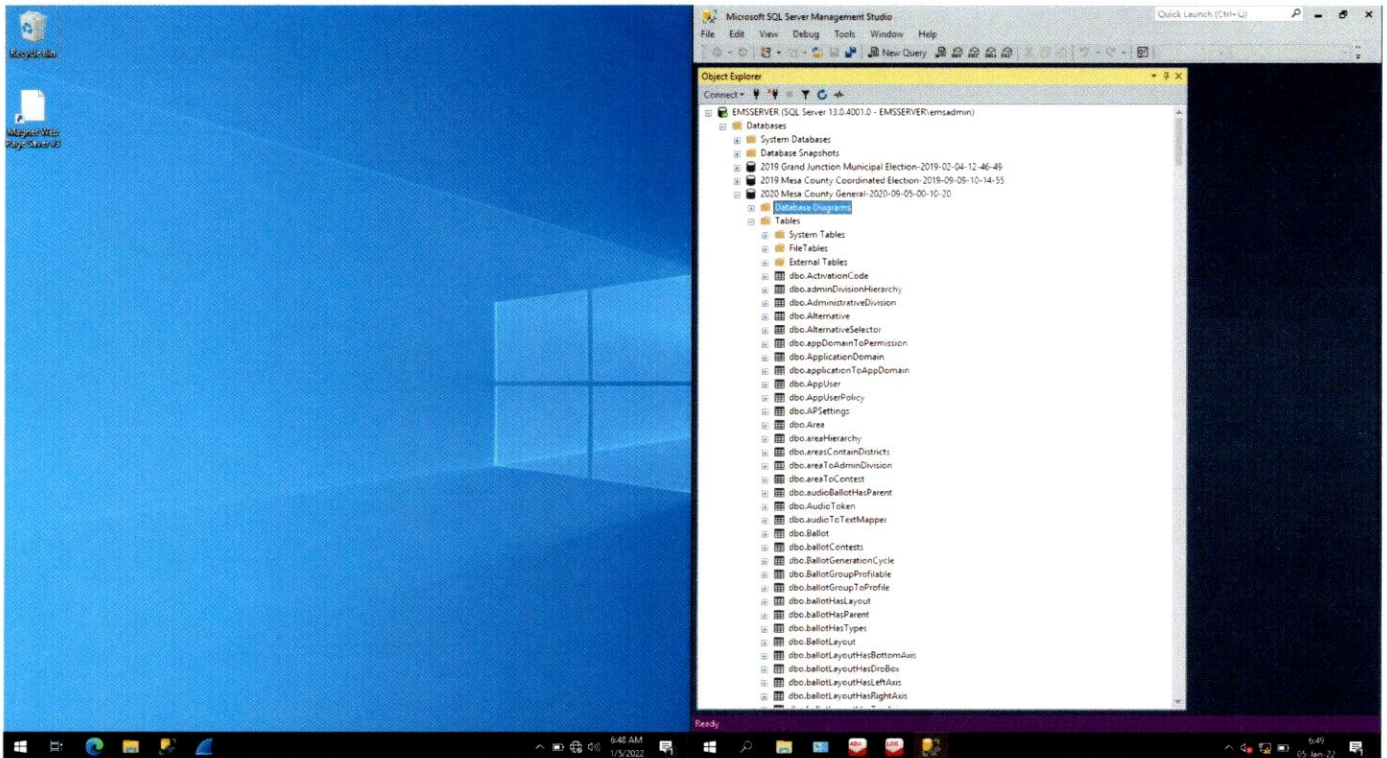


Figure 17 - Internal database tables, including ones with counted votes are accessible

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.

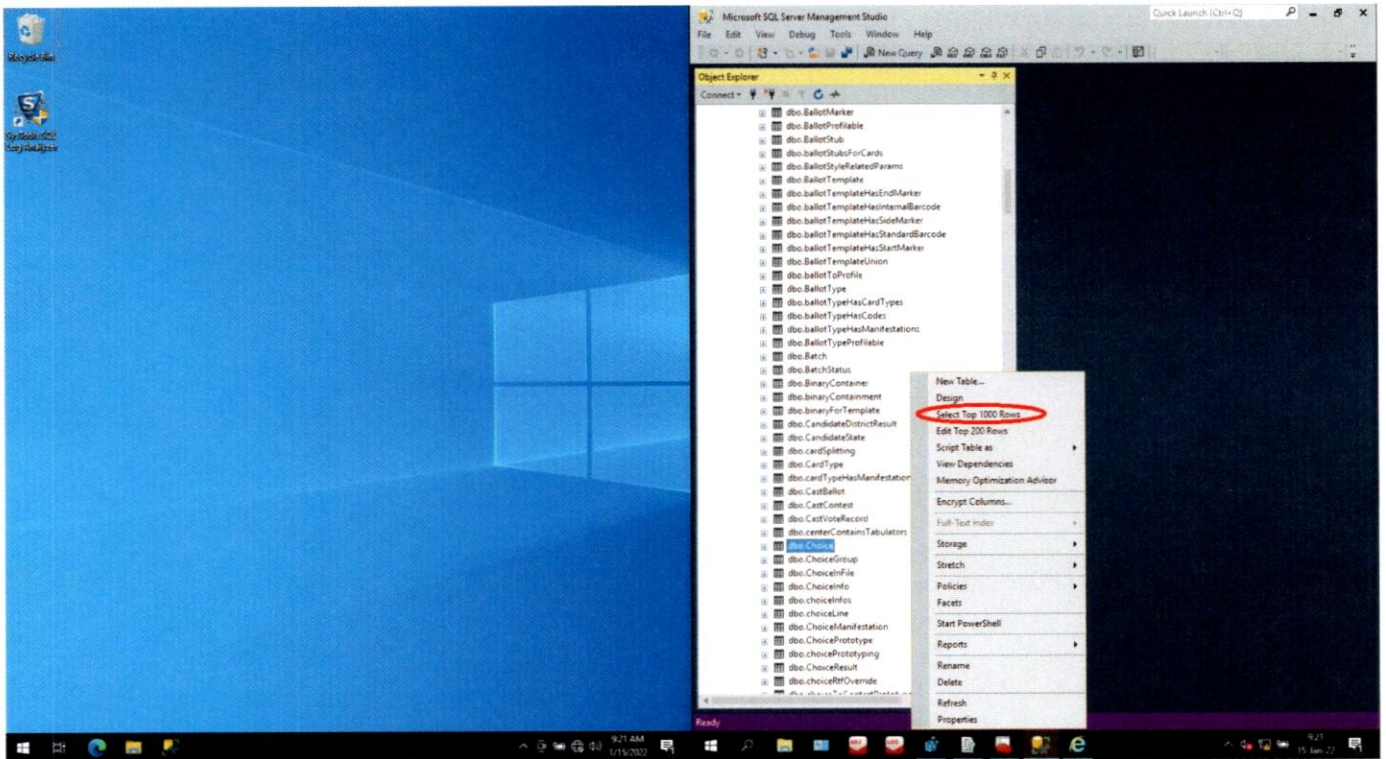


Figure 18 - Menu Option to Select the Top 1000 rows

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.

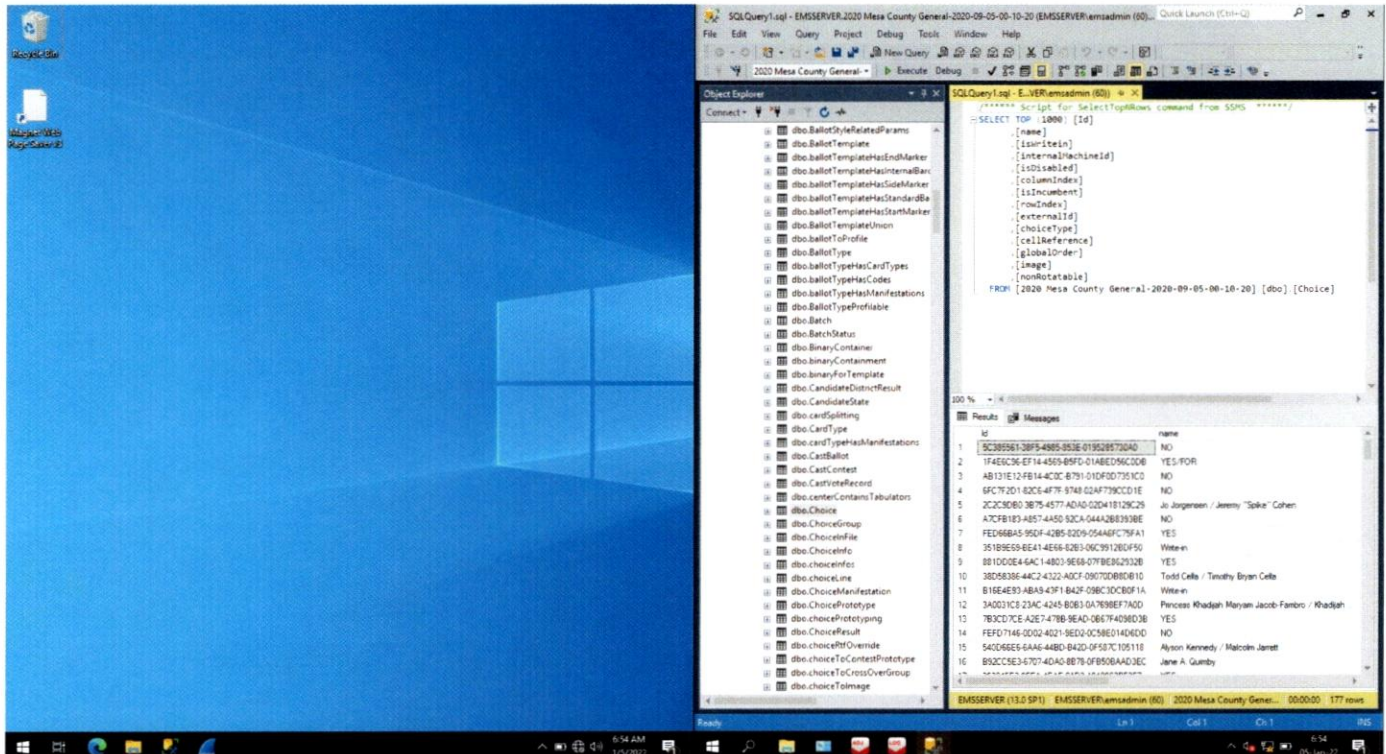


Figure 19 - Accessing the Ballot Choice database table

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.

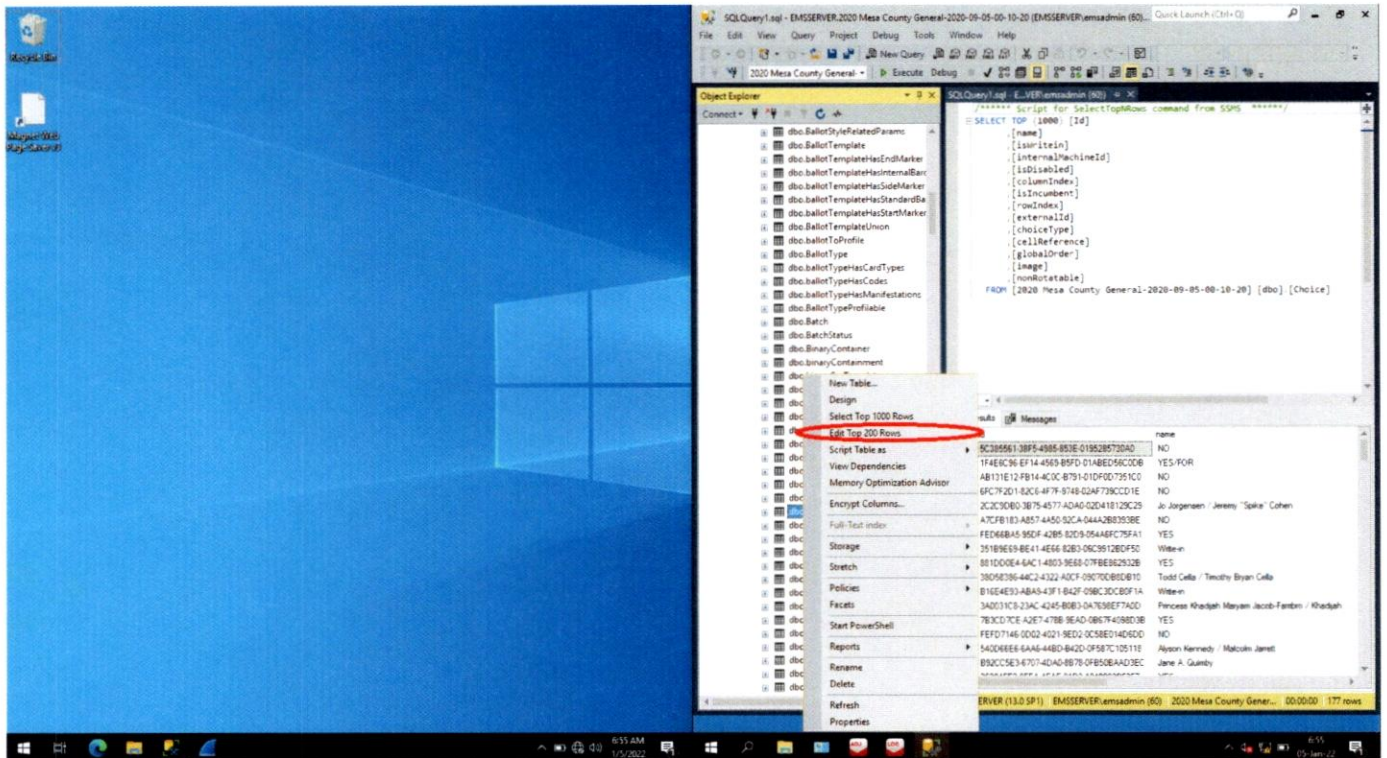


Figure 20 - Test to determine if the Ballot Choice Table can be edited to easily flip the votes

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.

id	name	isWritein	internalMachineld
e9b9e2d-2640-4514-82e1-000000000000	AliceMarie Slaven-Emmond	0	34
9071c815-8041-40e1-aed1-000000000000	YES	0	74
3f77346-9d2c-403a-83ef-000000000000	NO	0	141
88ae2695-9e9b-4eeb-888-000000000000	NO	0	115
18e405e4-a30d-4820-ade1-000000000000	David William Edwards	0	41
1e1fedfc-06af-4856-8d63-000000000000	NO	0	121
400013ab-fcc3-469d-9779-000000000000	Janice Rich	0	35
1ad372a2-99d3-4325-9235-000000000000	YES	0	50
266c5da-552f-490a-b1e1-000000000000	Donald J. Trump / Michael R. Pence	YES	2
ff9ee91f-7b0d-4e4e-92e6-000000000000	YES/FOR	0	84
bb36f293-b735-4cd0-89c0-000000000000	Matt Soper	0	33
daded1a86-c57c-4d3b-92c1-000000000000	YES/FOR	0	64
cc109f17-4bc2-46ab-bbe1-000000000000	Michael G. Rubenson	0	164
d8a6e5d0-119c-4c43-ac31-000000000000	Brock Pierce / Karla Ballard	0	19
5ea99afe-b970-474e-a27a-000000000000	NO	0	137
770c41f71-e376-409b-b125-000000000000	YES/FOR	0	82
22d87a5a-1ab1-403d-b0f1-000000000000	Daniel Doyle	0	24
f3fe735b-c876-4aca-bafe-000000000000	Stephan 'Seku' Evans	0	25
2a7c06ae-1679-4e39-bb51-000000000000	YES	0	152
e4d6fe13-ec99-426d-b031-000000000000	YES	0	108
4c28d26d-3658-4d8b-a5d1-000000000000	NO	0	153
3828c360-efc3-4fee-8ca2-000000000000	YES	0	40
ba45ada5-903c-4400-ac1c-000000000000	NO	0	147
4c4d445b-7808-457f-9933-000000000000	YES	0	148
793d008b-3a0d-4f01-bd31-000000000000	NO	0	101
19163095-606e-4cc2-b186-000000000000	NO	0	115
662a812b-a7e5-434d-b651-000000000000	Bro D. Quimby	0	172
f1baaca1a-a803-4666-b995-000000000000	NO	0	81
b4f018af-82a0-4714-a256-000000000000	YES/FOR	0	68
6da6e43b-e993-4a91-aeb1-000000000000	Howie Hawkins / Angela Nicole Walker	0	5
4151a3c3-d37a-403b-baf1-000000000000	NO	0	113
46aefc3-0baf-4240-a511-000000000000	NO/AGAINST	0	61
8fc22186-9c31-43f1-876f-000000000000	L Marc Montoni	0	43
43b569d2-5631-4679-b691-000000000000	YES	0	96
73da4ced-12c0-4beb-bee1-000000000000	NO/AGAINST	0	57

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.

id	name	internalMachineld
05d99201-3a26-4284-b89...	John Ryan Kell	0
8bcafd3a-4b5f-45b7-a7d4...	Serra Garcia	0
14855e94-f54b-4a6c-a77b...	NO	79
08e7c9b-74c7-479e-88c...	YES/FOR	54
3048d343-2691-4b01-b51...	Bruce Lohmiller	0
1c49777a-c82b-4526-bbc...	NO/AGAINST	55
64850211-d8ba-4347-90b...	YES	128
f304100-e5eb-4002-93b...	YES	102
b1ec1b57-2474-47ce-b05...	NO/AGAINST	67
1214cdd-44eb-4a27-b24...	NO	46
06617779-8a69-4a27-b2c...	NO	155
b62c773c-320c-4a80-b88...	Diane E. Mitsch Bush	0
7957b3ff-e27b-4e7b-aac2...	YES	140
e4a85e1-4a55-480f-a157...	Joseph Kishore / Noorissa Santa Cruz	0
152c3186-7855-4a6b-a77b...	NO	157
b9005a3c-29da-4b7e-b82...	NO	129
80794471-3a2b-4a84-a252...	YES/FOR	56
e47c7a5b-c409-4b79-b811...	YES	78
0e4ef653-4650-4017-b654...	YES	110
25017b66-16d9-4a45-8bb...	NO	111
5a8b09c8-e8ff-4575-ba7e...	Daniel Paul Rubinstein	0
25e71c56-7a71-44bb-bd3...	Lauren Boebert	0
6a4a5c0e-c8a9-4a2b-a35...	YES/FOR	52
8c505a60-5605-4eaf-98eb...	YES/FOR	70
4aa06336-7b4b-4d44-e111...	Joseph R. Biden / Kamala D. Harris	1
b3d40a15-90d0-432b-ed3...	NO	103
edd4ba8f-441e-415f-8ac0...	Kyle Kenley Kopitke / Nathan Re No Sor...	0
9c04aaf0-4a6d-4a10-abe...	YES	158
978c0b1b-39a5-41b9-90a...	Cory Gardner	0
7a22cb7a-59a5-4a83-a15...	NO	127
a7ae17c5-106-4a35-932...	NO/AGAINST	73
33ed259b-4b52-4094-a6b...	NO	125
62aea2b4-c03f-4ea1-baff...	Janet Roudland	0
NULL	NULL	NULL

Figure 22 - Candidate settings for Biden

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

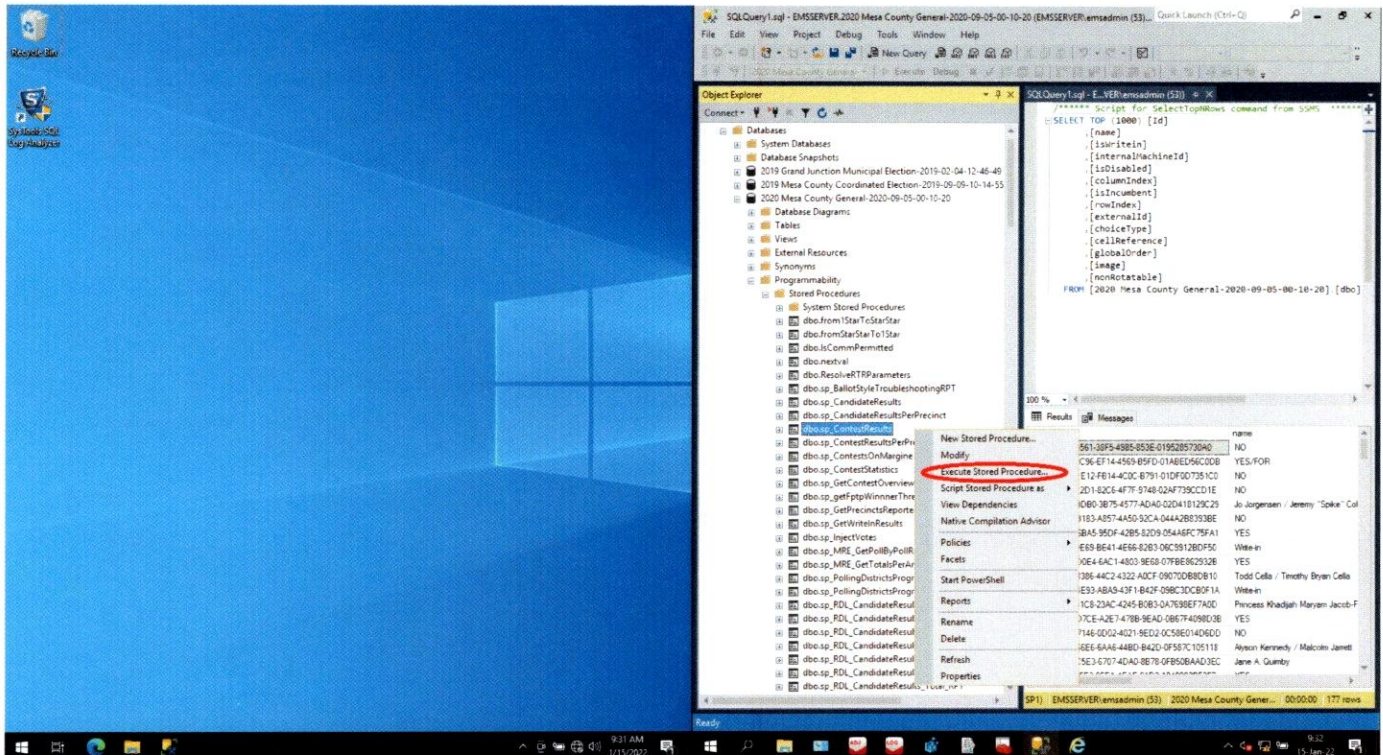


Figure 23 - Pulling up the results report prior to attempting the alteration

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.

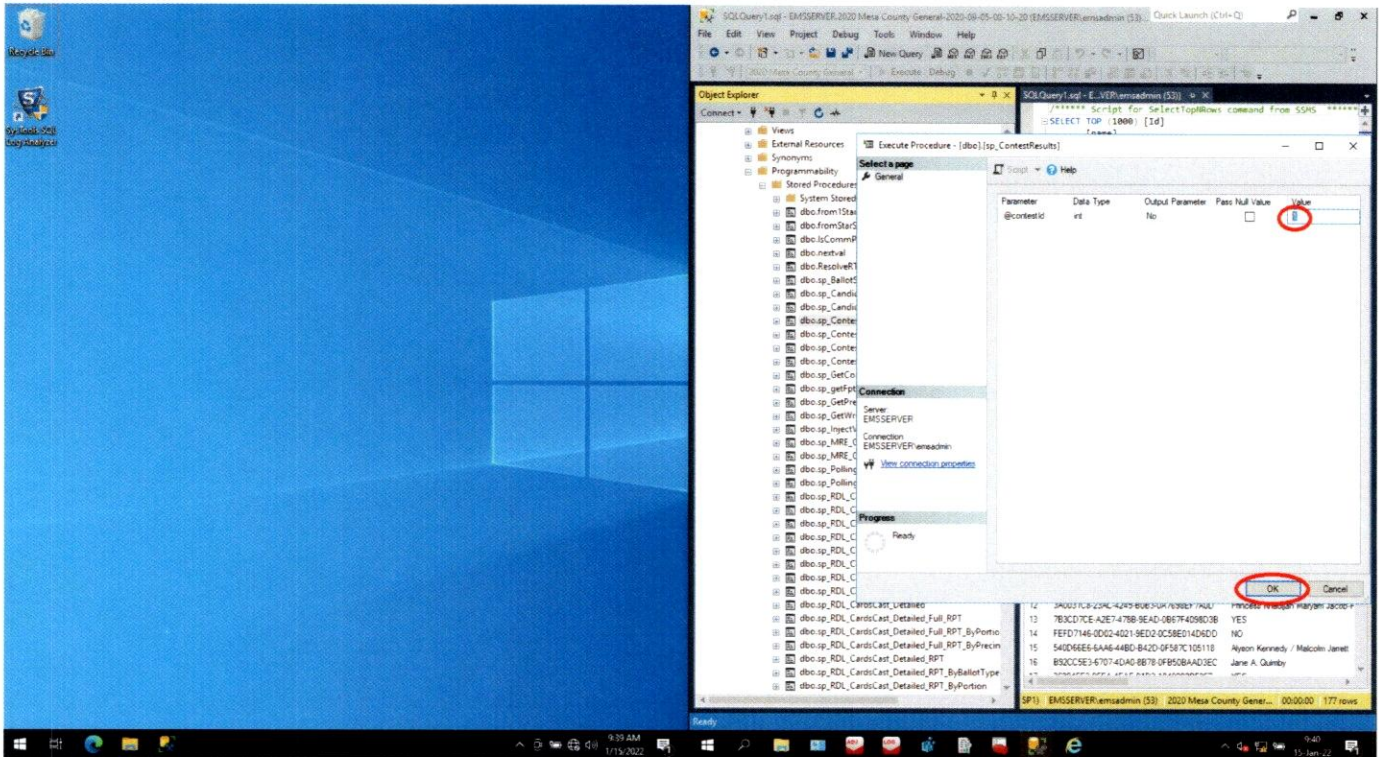


Figure 24 - Run Stored Procedure to pull up a report of Presidential Electors

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

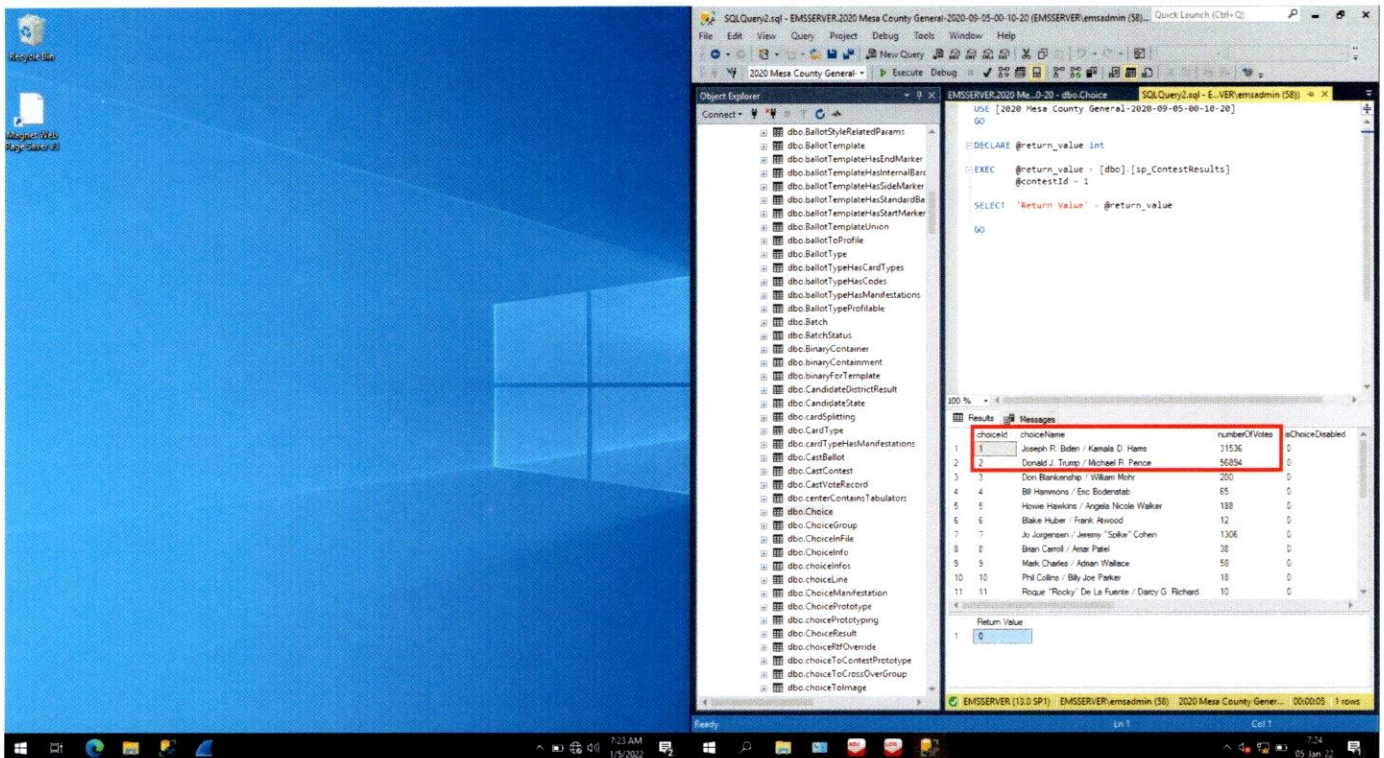


Figure 25 - Retrieved Vote Totals

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.

id	name	c1	internalMachineid
878208b8-0721-4d95-9643...	Jordan "Cancer" Scott / Jennifer Teppol	0	179
6d6c7b08-3f0c-4d64-961...	Jane A. Quimby	0	165
e96de22b-2d40-4514-826...	AliceMarie Slaven-Emond	0	34
9b71c515-8041-40d1-ae3...	YES	0	74
3f773846-9d2c-403a-81ef...	NO	0	141
88ae2955-9d3b-4eeb-888...	NO	0	119
16e425e4-a30d-4820-ade...	David William Edwards	0	41
1e1f6f8c-06af-4856-88d3...	NO	0	121
400013ab-fcc0-489d-9779...	Janice Rich	0	35
fad373e2-99d3-4325-9235...	YES	0	50
3b6c3c6a-592c-400a-b493...	Donald J. Trump / Michael R. Pence	1	1
ffbeef1f-7bd4-4e4e-92e0...	YES/FOR	0	64
bb3e293b-b735-4c02-89c...	Matt Soper	0	33
da6d1a86-c57c-4d3b-92c...	YES/FOR	0	64
cc109f17-4b02-46ab-bbe...	Michael G. Rubenson	0	164
d6a8c5d0-119c-4c43-ec3...	Brock Pierce / Karla Ballard	0	19
5ea9f8e6-b970-474e-a27a...	NO	0	137
70c41f71-e376-489b-b135...	YES/FOR	0	82
22d87a5e-14b1-4034-b0f...	Daniel Doyle	0	24
12f4798b-c376-4c62-bafe...	Stephan "Seku" Evans	0	25
2a7c06ea-1679-4a39-bb2...	YES	0	152
e4d4efb13-ec95-426d-b03...	YES	0	108
4c28d2f6-3658-4a8b-a5d...	NO	0	153
3825c360-cfc3-4fee-f8e2...	YES	0	48
ba83da5a-903c-4400-ec8...	NO	0	147
40d0445b-7808-4579-f933...	YES	0	148
793d000f-bd5d-4801-bd3...	NO	0	101
191630f3-609e-4c2-b186...	NO	0	115
662a0c2b-a7e3-4344-b63...	Brer D. Quimby	0	172
11ba9a14-a882-4666-1995...	NO	0	81
b410184f-82e0-47c4-a256...	YES/FOR	0	60
Adae43b0-6993-4451-ade...	Howie Hawkins / Angela Nicole Walker	0	5
4151a3c2-437a-402b-baf...	NO	0	113
4b6edc55-0b0d-4240-a51...	NO/AGAINST	0	61

Figure 26 - Candidate number for Trump modified

Here, I change the Trump 'internalMachineid' 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.

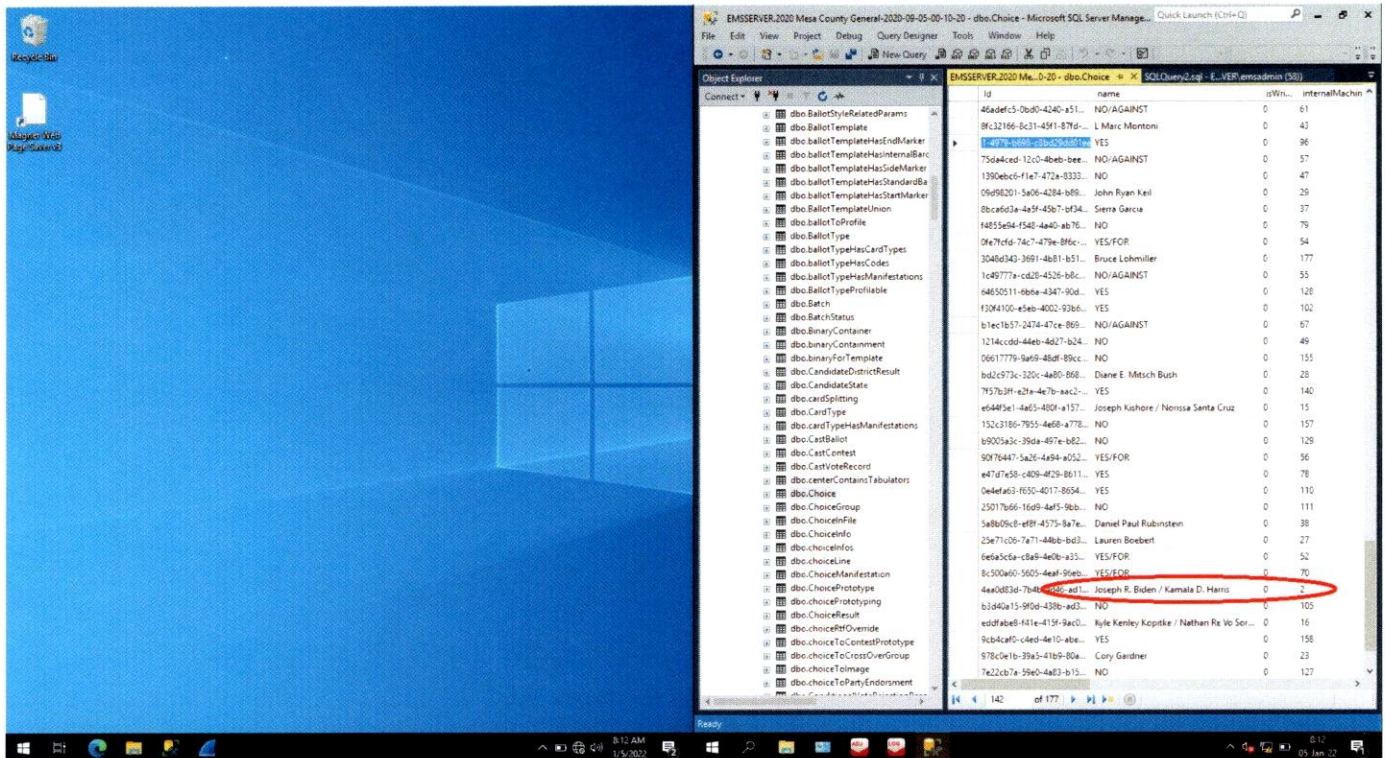


Figure 27 - Candidate number for Biden modified

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

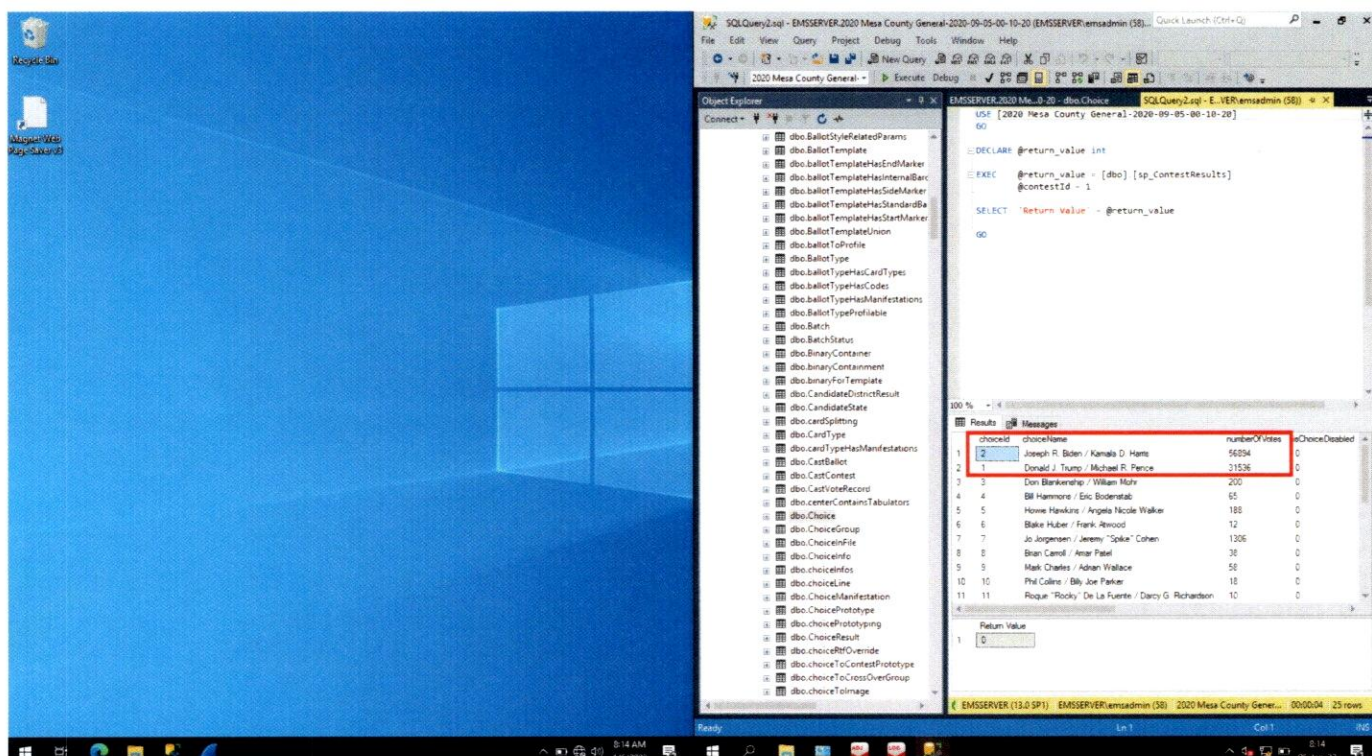


Figure 28 - Vote totals retrieved again after modification.

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 internalMachinelid 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.

CONFIDENTIAL

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.

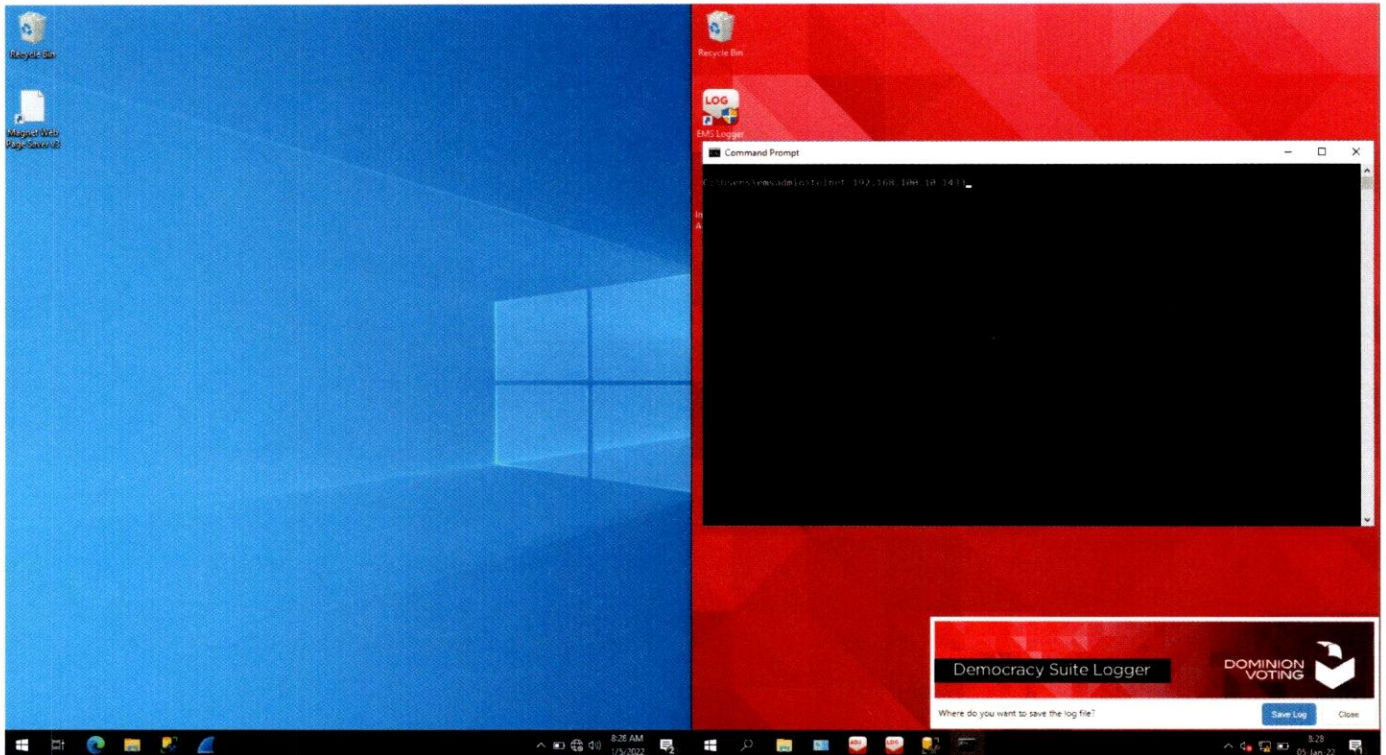


Figure 29 - Accessing port 1433 with Telnet

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.

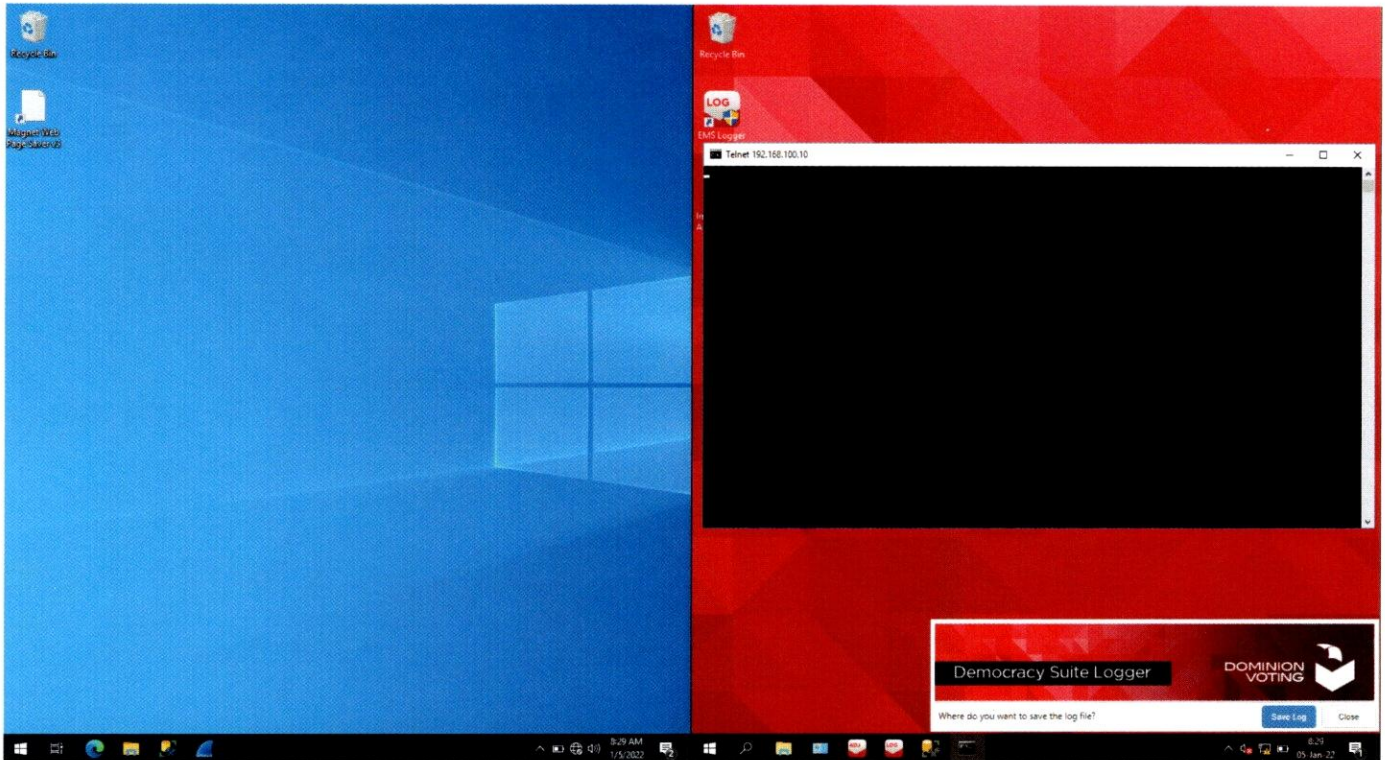


Figure 30 - The EMS server network interface appears to answer a connection to port 1433

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.

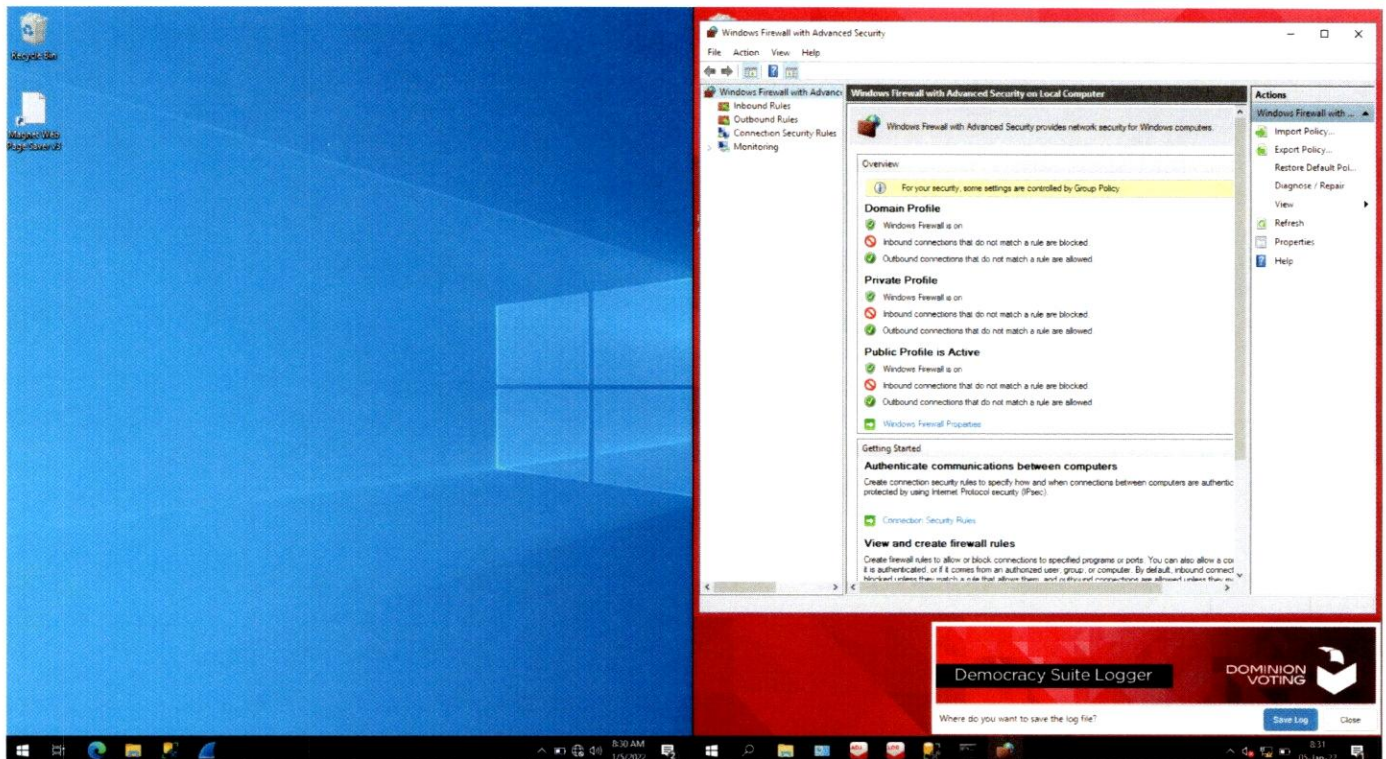


Figure 31 - EMS server has the 'Windows Firewall' enabled

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,

CONFIDENTIAL

- (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

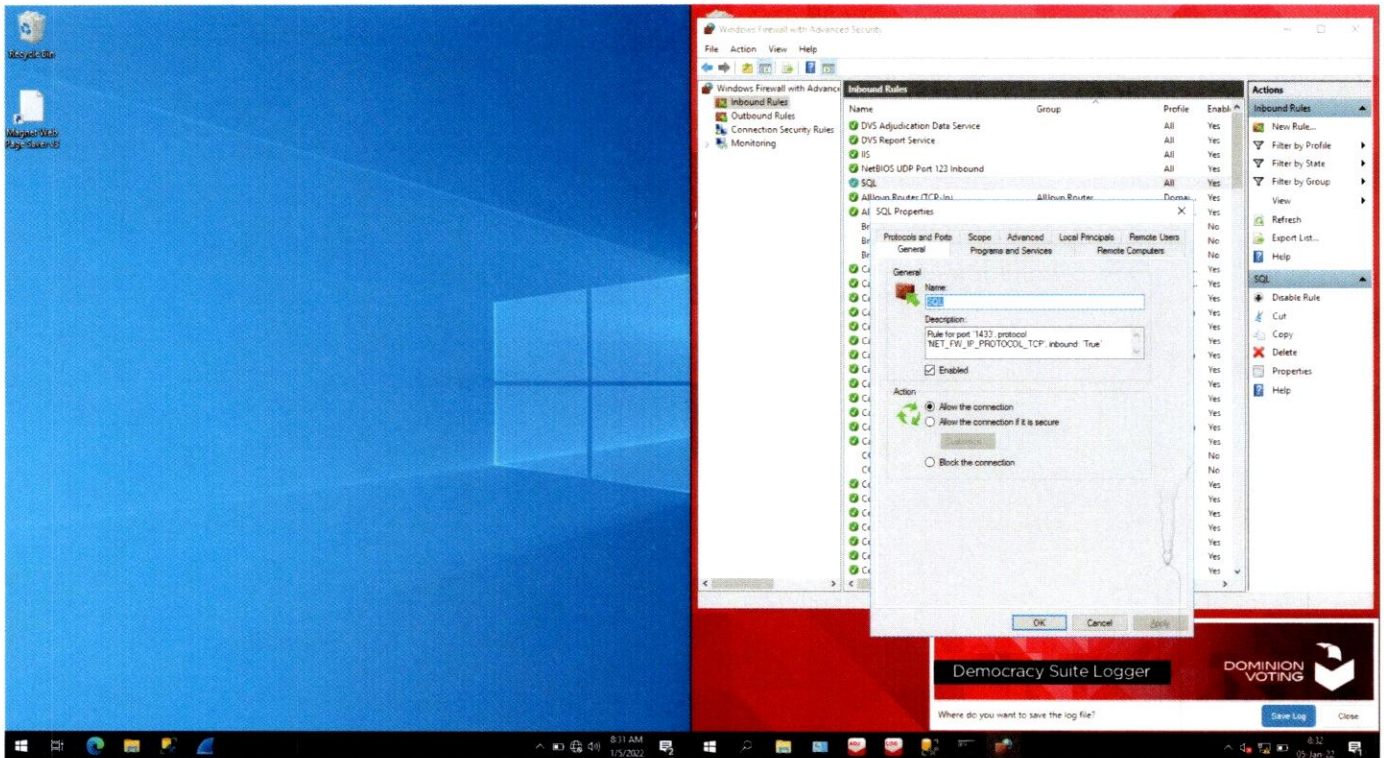


Figure 32 - Windows Firewall Custom SQL entry is enabled

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.

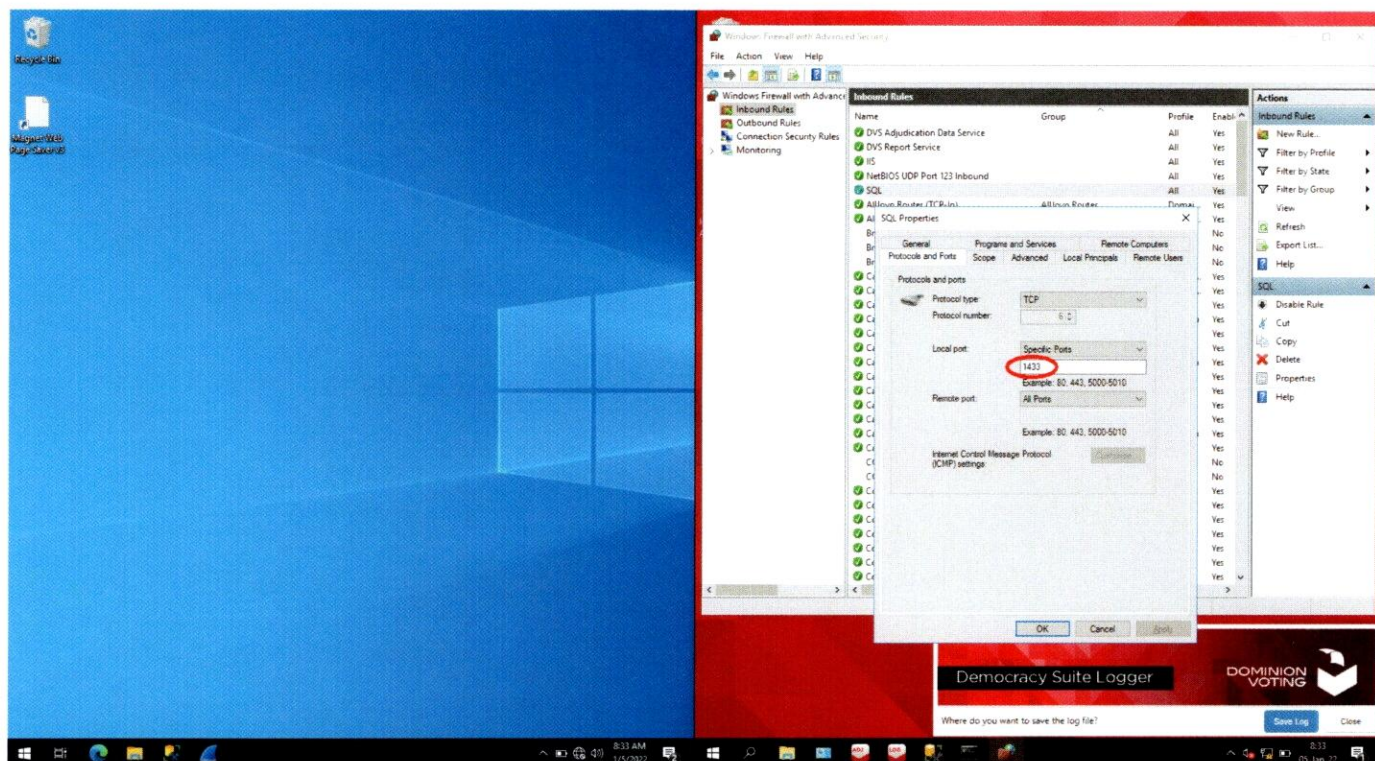


Figure 33 - SQL port 1433 is allowed.

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.

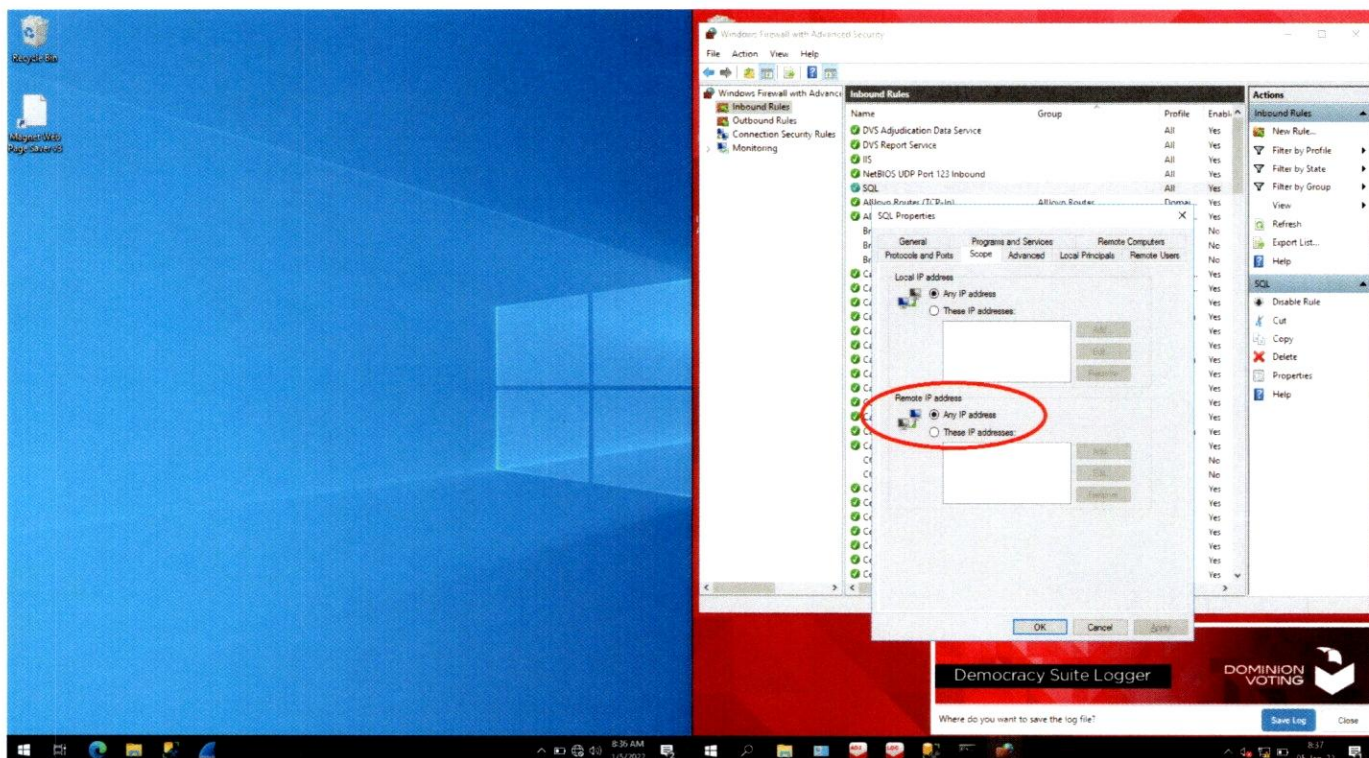


Figure 34 - Access to the SQL database standard port is allowed from ANY IP ADDRESS worldwide.

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."

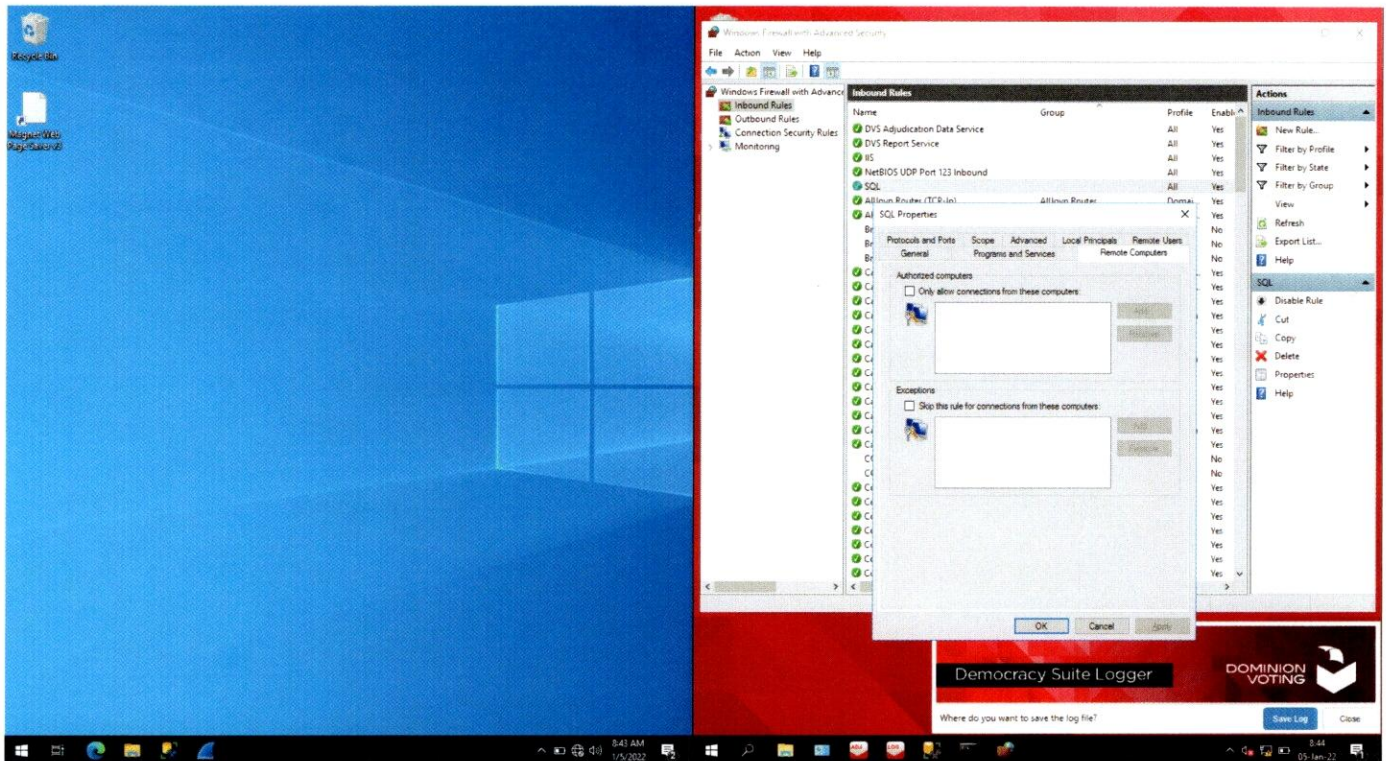


Figure 35 - No additional IP address restrictions or permissions

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.

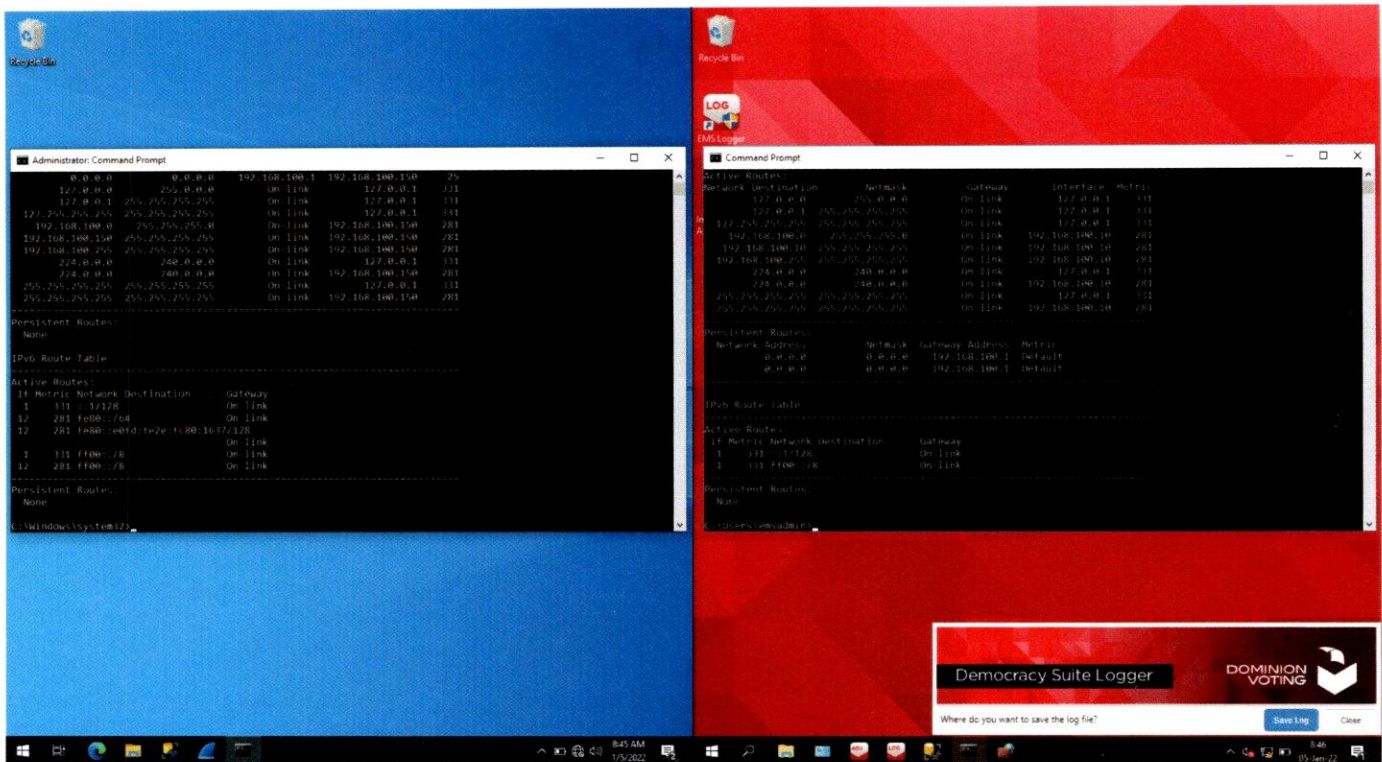


Figure 36 - Test Workstation, 192.168.100.150, and EMS, 192.168.100.10, are on the same subnet

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.

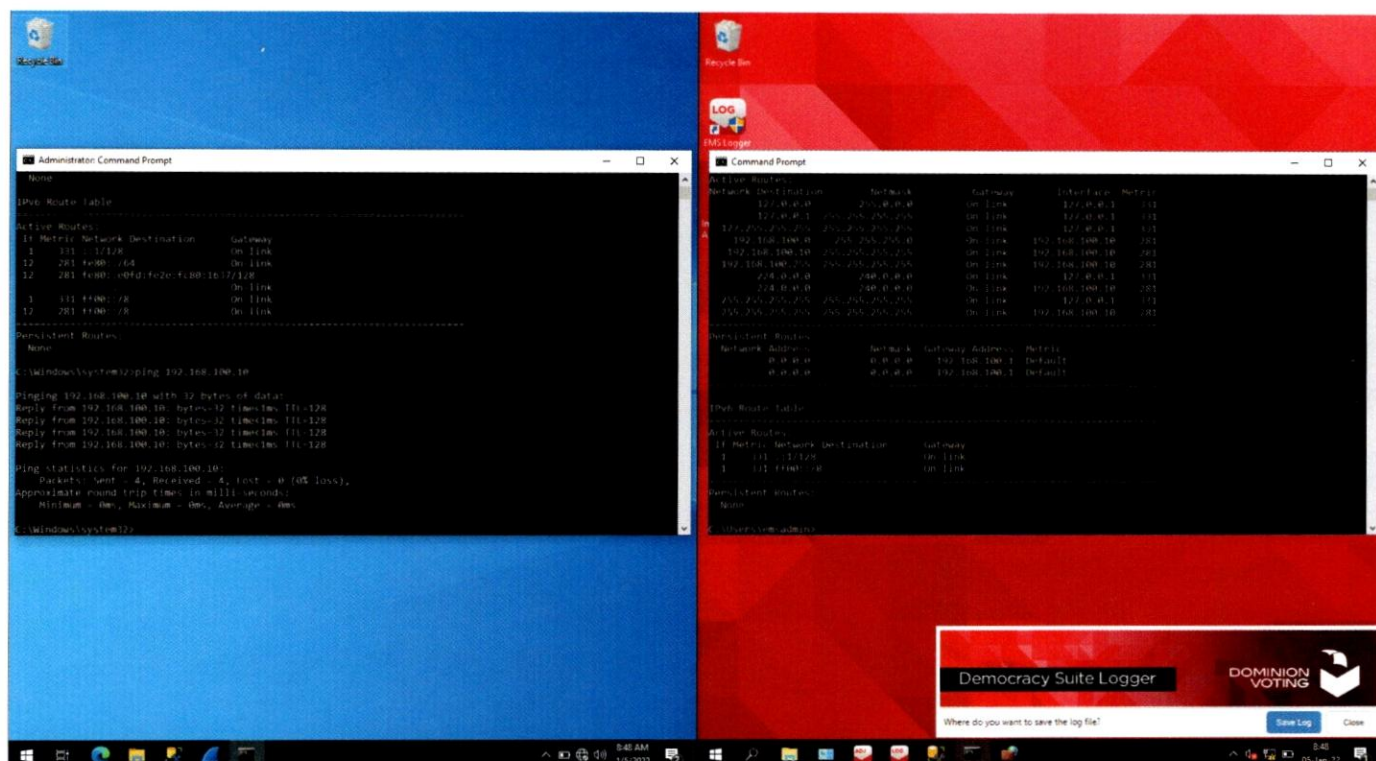


Figure 37 - Mesa EMS server is responding to network ping test.

'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.

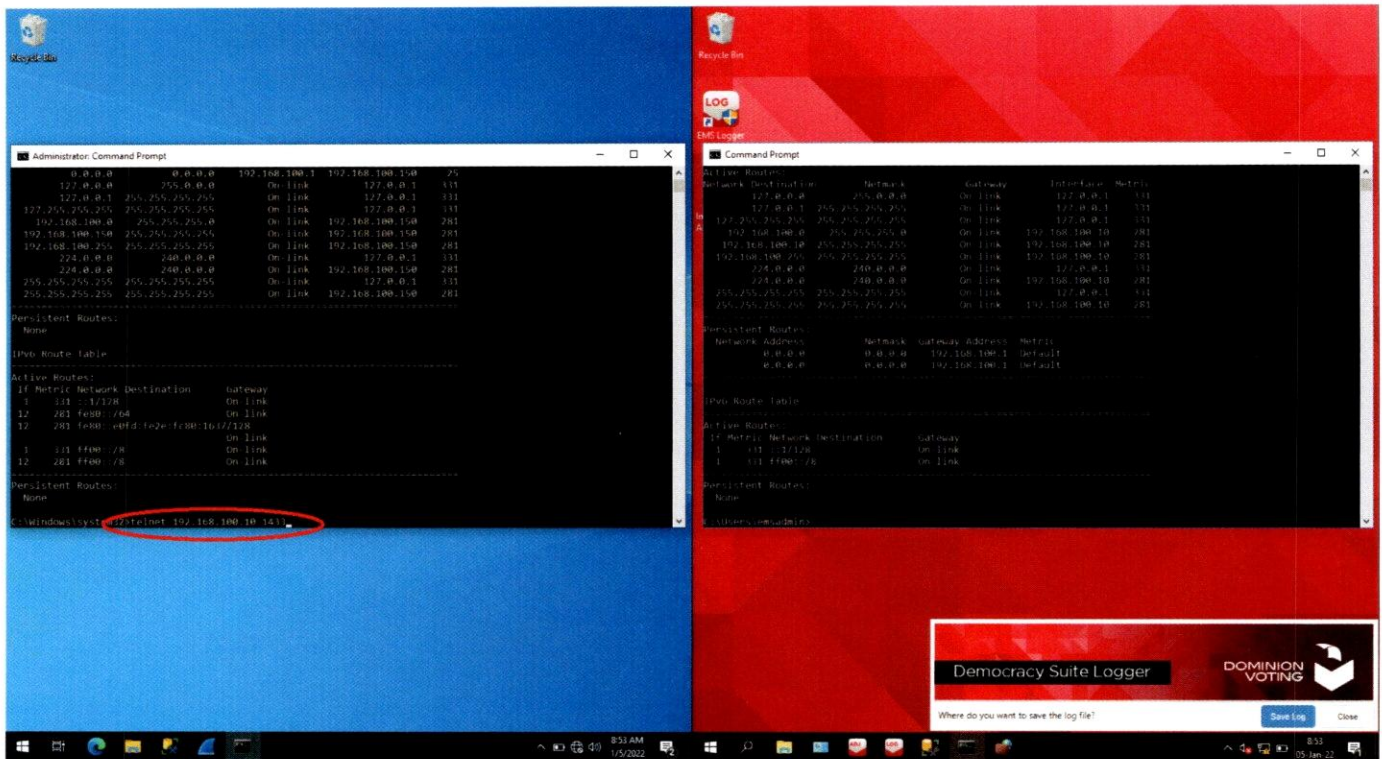


Figure 38 - Telnet connectivity test from separate computer not part of the Dominion system

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.

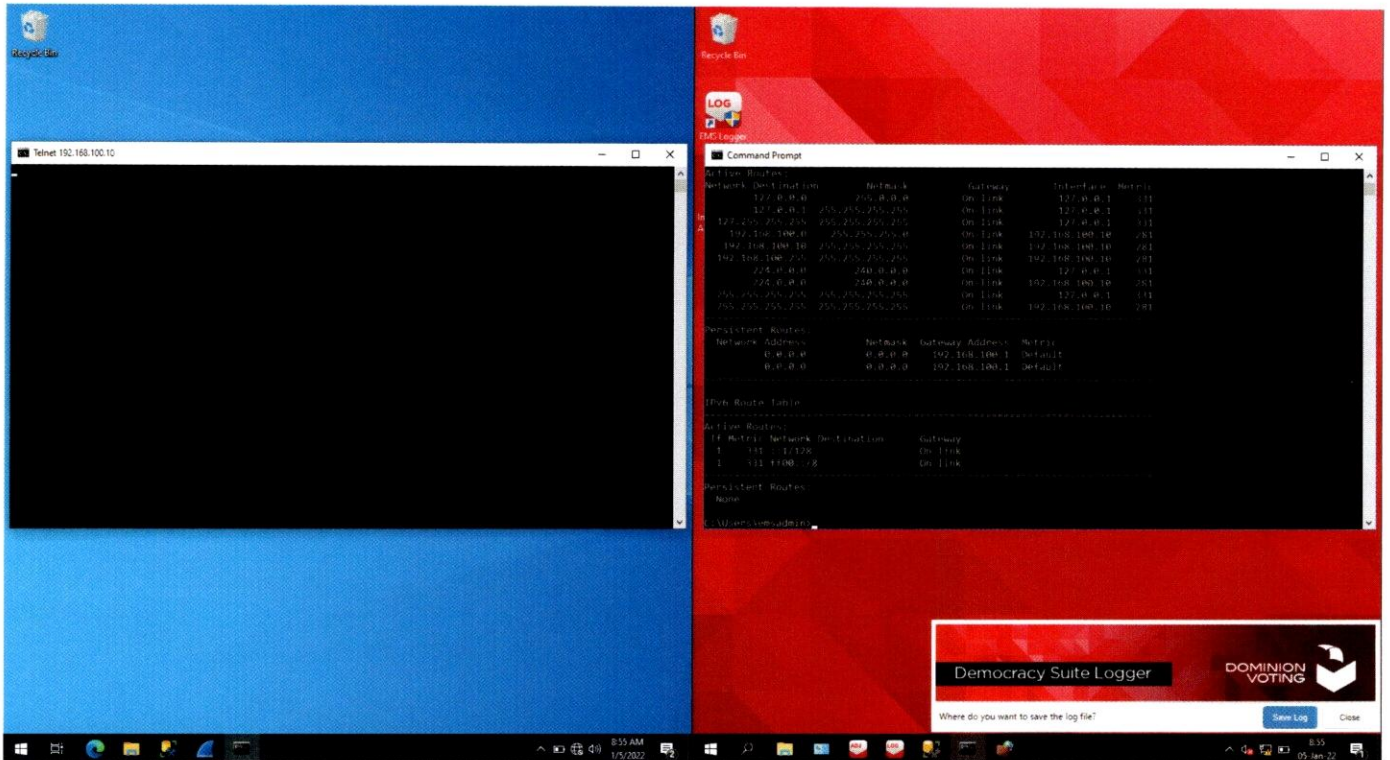


Figure 39 - Telnet to EMS server port 1433 (SQL) succeeds

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.

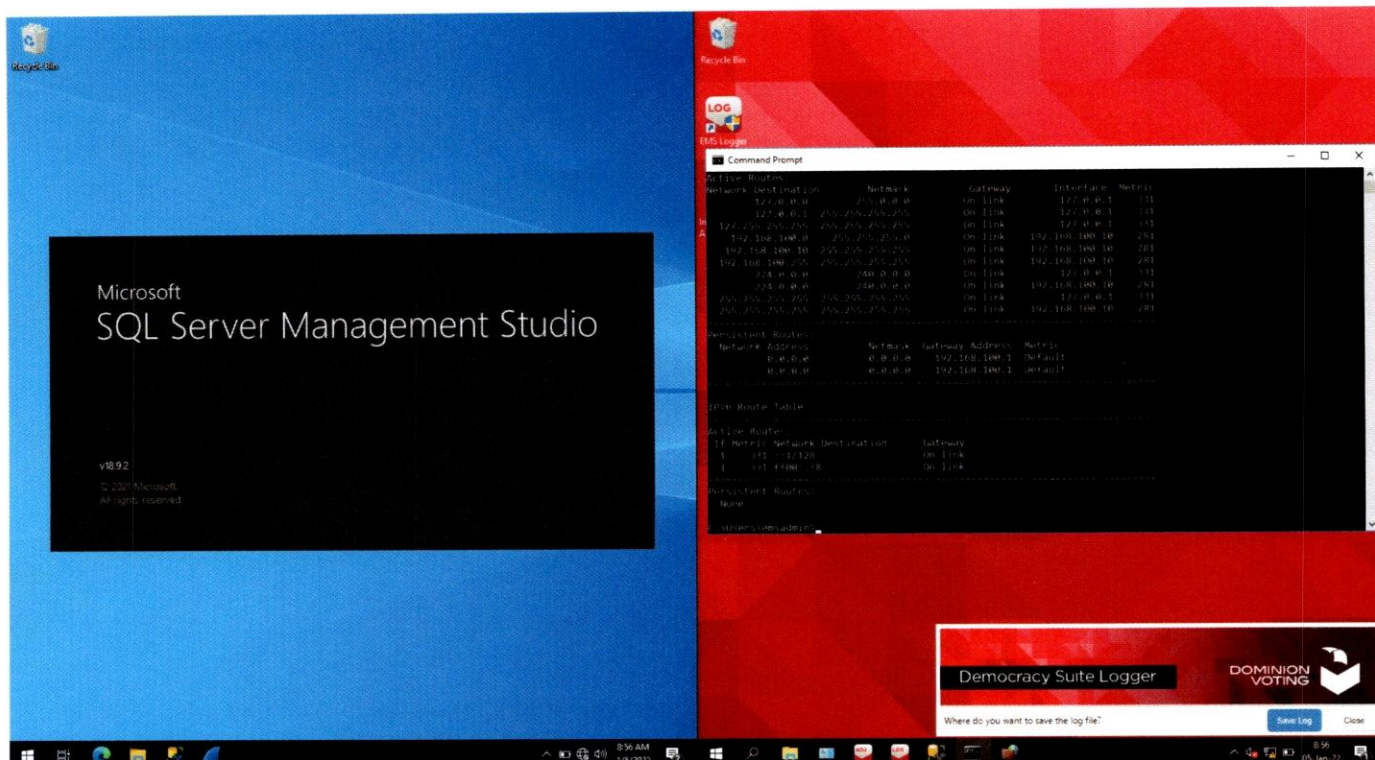


Figure 40 - SSMS access test from separate computer not part of the DVS D-Suite system

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.