EXECUTIVE SUMMARY

This report documents findings in an ongoing forensic examination of images of the hard drives[1] 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 oath[5] 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 vulnerabilities[8] (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 vulnerabilities[9] 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 risk[11] 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.

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, forseeably, 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 records[14] – 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.

(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.