Public Comment

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

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.**

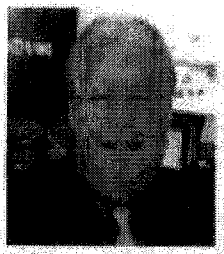
---

[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/.

Doug Gould Biography

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



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

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

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

He is a subject matter expert in:

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

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

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

Doug currently serves as Chief Technical Officer at CyberTeamUS.

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

Doug is an invited conference speaker.

Doug Gould Forensic Addendum

MAJOR FORENSIC CASES

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

INSTRUCTOR OF FORENSICS

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

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