EXHIBIT F

EXHIBIT 1

DATE FILED: August 19, 2022 4:27 PM
FILING ID: DDB7A2C97FFA1
CASE NUMBER: 2022CV31462

DECLARATION

I, Douglas W. Gould, declare under penalty of perjury that the following is true and correct:

I QUALIFICATIONS

My qualifications and experience with regard to computer-based systems and in particular the security aspects of computer-based systems are stated in Exhibit 1.1 attached.

II ACTIVITIES PERFORMED

Computer forensics is the application of investigation and analysis techniques to gather and preserve evidence from a particular computing device about how it has been operated and by whom.

I performed a forensic analysis of an image of the Dominion Voting Systems (DVS) Election Management System (EMS) Server with DVS version 5.11-CO election application software as used in Mesa County in the 2020 general election and the 2021 Grand Junction municipal election. The image replicated the entire EMS server before the May 2021 DVS "trusted build" update.

I also performed a forensic analysis of an image of the Dominion Voting Systems (DVS) Election Management System (EMS) Server with version 5.13-CO election application software taken immediately following the May, 2021 "trusted build" update.

From these images I

(i) determined information about the voting system used in the 2020 general election and 2021 Grand Junction municipal election;

(ii) assessed the impact of the software update (called "trusted build") on the computer and voting system; and

(iii) analyzed the DVS 5.13-CO election software installation (the current voting system software in Mesa County and Colorado).

III CONFIGURATION OF COMPUTER SYSTEM

The DVS EMS Server (hereafter EMS Server) is a computer-based system that, among other functions, reads ballots, interprets markings on ballots, and totals the vote counts in each race in an election. The data from these operations are stored in a Microsoft SQL Server database (a software application) maintained on the EMS Server. The EMS server operates in concert with the Microsoft Windows 2016 Server operating system. The Windows operating system manages all of the resources[1] of the computer system. No software runs on the system without the permission of and restrictions/limitations provided by the operating system. The same operating system was and is used in

[1] Among other resources, Memory, processor time, which programs run and at what priority, which programs can preempt others, Input/Output (including reading and writing to the disks, database, logfiles, etc)., sizes and limitations/restrictions of the system, security and access control.

conjunction with both DVS version 5.11-CO and 5.13-CO. An evaluation of how the DVS functions also requires consideration of how the operating system functions, as the DVS cannot operate independently of the operating system.

Accordingly, my evaluation relates to the EMS Server and the Windows operating system as "configured" when the images were taken. "Configuration" simply means that variable settings in the computer system affect how the system performs. For example, settings can be established for what constitutes a valid password, for who can access the system, for whether and how the system preserves data, and for many other elements of the system's operation.

IV PERFORMANCE STANDARDS APPLIED TO THE DVS VOTING SYSTEM

I was asked to evaluate whether the data retention characteristics of the DVS Voting System, including its EMS server, running with the Windows operating system, substantially complies with the requirements of the Voting Systems Standards (VSS) that were promulgated in 2002 by the Federal Election Commission.[2]

The VSS contains specific requirements for retaining records of the election process. How the system retains records or not is a consequence of configuration settings.

V. VSS REQUIREMENTS

VSS §2.2.11 specifies in pertinent part:

> Regardless of system type, all audit trail information … shall be retained in its original format, whether that be real-time logs generated by the system, or manual logs maintained by election personnel. The election audit trail includes not only in-process logs of election night (and subsequent processing of absentee or provisional ballots), but also time logs of baseline ballot definition formats, and system readiness and testing results.

VSS §2.2.5.1, titled "System Audit Purpose and Context", states on page 2/23:

> Election audit trails provide the supporting documentation for verifying the correctness of reported election results. They present a concrete, indestructible archival record of all system activity related to the vote tally, and are essential for public confidence in the accuracy of the tally, for recounts, and for evidence in the event of criminal or civil litigation.

VSS §2.2.5.2.1 (e), page 2-25 states:

> The generation of audit record entries shall not be terminated or altered by program control or by the intervention of any person. The physical security and integrity of the record shall be maintained at all times.

---

[2] I also found deficiencies in the security aspects of the systems that violate the VSS. Those are not discussed in this declaration, as they are beyond its scope.

VSS §2.2.4.1 (h), page 2-23 states "To ensure system integrity, all systems shall" :

> Maintain a permanent record of all original audit data that cannot be modified or overridden but may be augmented by designated authorized officials in order to adjust for errors or omissions (e.g., during the canvassing process.)

The VSS states its purposes to include ensuring that sufficient records *shall be* retained to detect and prosecute civil rights violations, election crimes, or to audit the performance of the voting system, and *to reconstruct* an election.

VI THE OPERATING SYSTEM DELETES CRITICAL RECORDS UNDER BOTH DVS VERSIONS

As stated, both DVS version 5.11-CO and 5.13-CO operate under the Microsoft Windows 2016 Server operating system. I found that configurations for both DVS 5.11-CO before the "trusted build" and for DVS 5.13-CO after the "trusted build" limited log file size to 20 MB. Accordingly, record retention behavior of the system running DVS version 5.13-CO will be identical to the record retention behavior of the system running DVS version 5.11-CO. I observed that 5.11-CO software configurations resulted in destruction of electronic files that VSS requires to be retained. The records destroyed included *election records, audit trail records and computer log records.*[3].

My examination of the operating system configuration in the images of the Mesa County EMS Server found that the system was configured for very small logfile sizes. Logfiles are the records of what occurs within the system, when it occurs, who caused it to occur, and what were the consequences of the occurrence. Logfiles are records of the activity of the system running on the server, in this case the DVS voting system. They are essential for any audit of how the system performed its functions during an election or at any other time.

If properly configured and compliant with the VSS, the operating system logfiles will contain the time-stamped IP addresses and identity of all users connecting to the system; they will indicate which user or programmed authority caused the execution of each program, the time of execution and all error conditions including whether a storage device ran out of space or other errors not generated by human input. A single logfile entry (i.e., including one election-related record) requires approximately 68 kilobytes of space in the logfile. Performing the division (20 megabytes divided by 68 kilobytes) yields 294 records as the maximum number of records that a 20 megabyte logfile can retain. When the logfile size exceeds 20 megabytes, the computer operating system will discard the oldest record (to make space for the next record) and replace it with the newest record, overwriting the data, overriding the requirement in law for the records to be preserved.

It is not possible to reconstruct how the system processed election data without complete logfiles. When logfiles are configured to a very small size, only the newest information

---

[3] Complete details of the forensic examinations and the findings for DVS version 5.11-CO, supporting this declaration are contained in the two forensic reports entitled "Mesa County Colorado Voting System Report #1" (hereafter referred to as "Report #1") and "Mesa County Colorado Voting System Report #2" (hereafter referred to as "Report #2) which are incorporated fully herein.

about the system's operation can be preserved; previous information automatically is deleted to make room for more recent information. Accordingly, short logfile sizes prevents the preservation of data relating to the system's past operations, including its processing of elections.

The DVS system copies selective data from system records into a database using a program that is part of the election software called the "EMS Logger." The EMS Logger contains a set of logfile data that is insufficient to audit the integrity of or reconstruct an election and does not comply with the VSS requirement to retain data "in its original format." (Section V, VSS Requirements, §2.2.1.1)

VII DATA RETENTION PERIODS

I was asked to evaluate whether the DVS Voting System, including the EMS server, retains data for periods required by the VSS.

The VSS requires data retention after elections for specific periods and specific reasons. The VSS states "Because the purpose of this law is to assist the Federal government in discharging its law enforcement responsibilities in connection with civil rights and elections crimes, its scope must be interpreted in keeping with that objective" and specifies that "The appropriate state or local authority **must preserve all records that may be relevant** to the detection and prosecution of federal civil rights or election crimes for the 22-month federal retention period, if the records were generated in connection with an election that was held in whole or in part to select federal candidates."[4] (emphasis added)

The VSS continues to state (in the same reference) "Regardless of system type, all audit trail information . . . shall be retained **in its original format**, whether that be real-time logs generated by the system, or manual logs maintained by election personnel. The election audit trail includes not only in-process logs of election night (and subsequent processing of absentee or provisional ballots), but also time logs of baseline ballot definition formats, and system readiness and testing results."[5] (emphasis added)

VSS Vol. 1, §2.2.5.1, titled "System Audit Purpose and Context", states on page 2/23, "Election audit trails provide the supporting documentation for verifying the correctness of reported election results. They present a concrete, indestructible archival record of all system activity related to the vote tally, and are essential for public confidence in the accuracy of the tally, for recounts, and for evidence in the event of criminal or civil litigation."

---

[4] 2002 Voting System Standards, Volume 1, page 2-34, §2.2.11
[5] *Id.*

A. ROUTINE OPERATION OF THE SYSTEM DESTROYS DATA THAT ARE NECESSARY FOR ANY RECONSTRUCTION OR AUDIT OF AN ELECTION

VSS Vol. 1, §2.2.5.3 addresses specific record retention requirements for "COTS" (Commercial Off-The-Shelf) software.[6]

VSS §2.2.5.3, page 2-26, states:

> Further requirements must be applied to COTS operating systems to ensure completeness and integrity of audit data for election software. These operating systems are capable of executing multiple application programs simultaneously. These systems include both servers and workstations (or "PCs"), including many varieties of UNIX and Linux, and those offered by Microsoft and Apple. Election software running on these COTS systems is vulnerable to unintended effects from other user sessions, applications, and utilities, executing on the same platform at the same time as the election software.
>
> "Simultaneous processes" of concern include unauthorized network connections, unplanned user logins, and unintended execution or termination of login processes. An unauthorized network connection or unplanned user login can host unintended processes and user actions, such as the termination of operating system audit, the termination of election software processes, or the deletion of election software audit and logging data. The execution of an operating system process could be a full system scan at a time when that process would adversely affect the election software processes. Operating system processes improperly terminated could be system audit or malicious code detection.
>
> To counter these vulnerabilities, three operating system protections are required on all such systems on which election software is hosted. First, authentication shall be configured on the local terminal (display screen and keyboard) and on all external connection devices ("network cards" and "ports"). This ensures that only authorized and identified users affect the system while election software is running.
>
> Second, operating system audit shall be enabled for all session openings and closings, for all connection openings and closings, for all process executions and terminations, and for the alteration or deletion of any memory or file object. This ensures the accuracy and completeness of election data stored on the system. It also ensures the existence of an audit record of any person or process altering or deleting system data or election data.

---

[6] The voting system used by Mesa County employs commercial off the shelf (COTS) software. COTS elements include the Microsoft Windows operating system, Microsoft SQL Server Database Management System, and Microsoft SQL Server Management Studio. Therefore, VSS standards relating to COTS elements apply in this case.

> Third, the system shall be configured to execute only intended and necessary processes during the execution of election software. The system shall also be configured to halt election software processes upon the termination of any critical system process (such as system audit) during the execution of election software.

These required records are obtained from operating system logs, Windows "event" logs, application logs (including database logs, logs of custom election software, and other programs that are executed).

Forensic analysis revealed that (a) DVS does not retain all of these records in their original format, and (b) retains only excerpts from some of these logs (the "EMS Logger") rather than complete records on the EMS Server. Forensic analysis further revealed that the DVS EMS Server overwrites operating system logs (original format records, i.e., logfiles) and fails to retain these data as required by VSS §2.2.4.1 (h). The DVS EMS overwrites operating system logfiles because, with the maximum logfile size configured at 20 megabytes, when the logfile exceeds 20 megabytes, record preservation is overridden and the disk file space is re-used, erasing earlier records. This setting ensures that much logfile data automatically will be deleted in the normal operation of the system. This setting is identical in the current version (5.13-CO) voting system and will cause the same overwriting / deletion behavior (the same operating system with the same settings will behave the same way).

My analysis is based upon the forensic images of the Mesa County EMS Server provided to me by legal counsel for Tina Peters. Based on their interviews of the county election personnel who operated the system and controlled access to it, I was informed by attorneys who provided the evidence to me that Mesa County election personnel did not know of any additional archival data or records of the contents of the Mesa County EMS Server.

Because the extremely limited copies of logs that do exist in the EMS Logger database do not contain specifically required content from the 2020 and 2021 elections (version 5.11-CO), because operating system logfile size is limited to 20 megabytes ensuring the overwriting of operating system logfile data, the VSS requirement for retention of logs and records in their "originally generated format" has been violated.

B. THE TRUSTED BUILD DELETED MASSIVE AMOUNTS OF DATA FROM PREVIOUS ELECTIONS LESS THAN 22 MONTHS AFTER SUCH ELECTIONS

The contents of the Mesa County EMS server, including the hard drive of the computer on which it runs, were radically changed in May, 2021. I am told this was done by representatives of the software vendor and the Colorado Secretary of State. Some of the effects of this process were:

1. The hard drive was reformatted. As a result, most of the data previously stored on the hard drive became impossible to retrieve and should be considered deleted.

2. The data deleted included operating system logfiles[7] and Microsoft Windows event logfiles. A total of 695 of these files were deleted: 505 operating system logfiles and 190 windows event files.
3. The data deleted included DVS version 5.11-CO software.
4. New copies of the operating system and the applications running on the system were placed on the hard drive. The DVS applications version 5.13-CO was one of those applications.
5. Ballot images were preserved on a separate disk drive on the EMS Server, but original operating system records were deleted.

The data deleted during the May, 2021 "trusted build" included data required to be retained by the VSS.

VIII DEFICIENCIES CANNOT BE MITIGATED BY ADJUSTING SYSTEM CONFIGURATION

In other settings, such as a computer system operated by a commercial company, some of the foregoing deficiencies could be mitigated or corrected by changing configuration settings. That appears to be impractical if not impossible in the setting of the DVS voting system.

VSS §1.6.1, page 1-14, in relevant part, states:

> Qualification tests validate that a voting system meets the requirements of the Standards and performs according to the vendor's specifications for the system.
>
> After a system has completed qualification testing further examination of a system is required if modifications are made to hardware, software, or telecommunications, including the installation of software on different hardware.
>
> Generally, a voting system remains qualified under the standards against which it was tested, as long as no modifications not approved by an ITA are made to the system.

In the 2002 VSS, an ITA is an "Independent Testing Authority" which is now designated a "Voting System Testing Laboratory" (VSTL) which is accredited by the U.S. Election Assistance Commission.

VSS §1.6.2, page 1-15, in relevant part, states:

> Certification tests are performed by individual states with or without the assistance of outside consultants …

---

[7] There are numerous logfiles with different naming conventions for different purposes. Windows operating system, application, security and setup events are recorded in "event" files with the suffix ".evtx", while many of the functions of the operating system are recorded in logfiles with the filename suffix ".log". There are many other logfiles that include, for example, an inventory of files included in a software update that do not contain information relevant to the reconstruction or audit of an election and are not included in these numbers.

> Certification tests performed by individual states typically rely on information contained in documentation provided by the vendor for system design, installation, operations, required facilities and supplies, personnel support and other aspects of the voting system.

Some reasons why it is impractical to mitigate the system's deficiencies are the following:

First, it is possible that neither the county personnel nor the secretary of state's personnel are competent to adjust system settings or to identify the need for such changes. Indeed, making such changes might violate Colorado law. It also might violate contracts with the vendor of the voting system.

Second, the entire system must be tested by a federally accredited voting system testing laboratory. Adjustments to the system might require testing of the entire system under state and or federal law.

Third, my understanding is that Colorado law and election rules require voting systems to be decertified if there is a suspicion that their operations have been altered. To adjust the system's configuration could require decertification of the system and prevent its use in an election.

Fourth, if the system must be adjusted or reconfigured, this is accomplished by copying a new certified image provided by the vendor onto the hard drive, destroying the data thereon. This would destroy records relating to the 2022 primary election, violating record retention statutes.

FINDINGS AND CONCLUSIONS

1. As delivered to the State of Colorado by Dominion Voting Systems, the DVS EMS Server (version 5.13-CO and version 5.11-CO) is configured to erase (overwrite) critical election records, audit trails, and operational logfile records. Destruction of these data makes it impossible to detect election crimes or civil rights violations. Destruction of data makes it impossible to audit or reconstruct an election.

2. As delivered, the DVS Voting System operating system is configured for a maximum log file size of 20 megabytes. Both the DVS versions 5.11-CO and 5.13-CO contain this same configuration maximum size limit. This logfile size is inadequate to ensure the preservation of election data.

3. DVS software contains an "EMS logger" program that does not "preserve all records that may be relevant to the detection and prosecution of federal civil rights or election crimes," specifically omitting detailed software executions, alterations and deletions of files and external connections to the EMS Server.

4. No audit of the electronic voting and tabulation of ballots is possible because the data necessary to audit, reconstruct the election or detect election crimes have been destroyed, both by configuring the maximum logfile size to be too small, and by deletion of records not otherwise preserved using the "trusted build" process.

5. It is impractical to attempt to correct or even mitigate the effects of the system deficiencies and non-compliance with the VSS.
6. The DVS system does not substantially comply with VSS requirements.

I declare under penalty of the perjury laws of the state of Colorado and the United States that the foregoing is true and correct, and that this declaration was executed this 12th day of August 2022 in Morehead City, North Carolina.

Douglas W. Gould