Ray Lutz
Executive Director, Citizens Oversight
https://citizensoversight.org
https://auditengine.org

raylutz@citizensoversight.org
619-820-5321 (mobile)
619-440-3646 (support)

March 13, 2025

(REF: M2034)

Shirley N.Weber, Ph.D.
California Secretary of State
Office of Voting Systems Technology Assessment
VotingSystems@sos.ca.gov

Comment on Dominion Democracy Suite 5.19

The County Clerk/Registrar of Voters (CC/ROV) Memorandum #25009 provided notice of a public hearing regarding the application for approval of Dominion Voting Systems, Inc.'s Democracy Suite 5.19 Voting System.
https://admin.cdn.sos.ca.gov/elections/ccrov/2025/january/25009rr.pdf

The notice also stated that "Anyone wishing to submit written comments can do so by delivering it to the hearing or by e-mailing it to VotingSystems@sos.ca.gov by 5:00 p.m. on March 13, 2025."

This document provides the comments from Citizens' Oversight Projects. Our team has experience with voting systems and election procedures, as well as experience with computer technology hardware and software. Please take careful note of our comments and record them in the public record for this approval project.

References:
All reports are at
https://www.sos.ca.gov/elections/ovsta/frequently-requested-information/dominion-voting

The following points were mentioned by the staff report. We have made comments about these points.

1. **Event log can be disabled.** To check this, staff can turn to the "Event Viewer" which "will indicate the Event Log status and identify which user performed specific actions." It does not say if the Event viewer just shows current status or can also show if log was disabled in the past. There are no criteria to require personal usernames, so it may just show "admin" disabled it. pp.12-13 of https://votingsystems.cdn.sos.ca.gov/vendors/dominion/ds519/ds519security-report.pdf

   What is the rationale for allowing the event log to be disabled? Logging is an important security function that allows all events in the operation to be disclosed. It would be far better to eliminate the option of disabling the logs, and logging all events, so that any unusual events could be detected.

   Further, logs should be improved with hashes for each log entry and a hash of that with prior log hashes, to make it more difficult to alter the logs.

   We believe that certification should not be granted due to this security concern.

2. Administrators have access to election returns without limits on timing, e.g. before election day. They need software limits. p.28 of https://votingsystems.cdn.sos.ca.gov/vendors/dominion/ds519/ds519security-report.pdf

3. Adjudication software has a vulnerability in error handling. Proper use will avoid this, but adjudication is done in large volume, hard to supervise, and changes votes. It should not be certified with this vulnerability. p.8 of https://votingsystems.cdn.sos.ca.gov/vendors/dominion/ds519/ds519software-report.pdf

4. They reported "a single user account that contained administrative privileges". Not clear if reviewers wanted more for backup, or to have 2 people working together to make changes. SOS should require at least 2 accounts to be logged in to make administrative changes, and that there be at least 4 administrative accounts, so there are backups. p.37

5. Five people with disabilities tried the machines, and found audio of widely varying volume, repetitive, needing to press each letter of a write-in twice, and being bumped back to earlier steps too often and unexpectedly. This should

not be certified.
https://votingsystems.cdn.sos.ca.gov/vendors/dominion/ds519/ds519aup-report.pdf

6. They say the Canon scanner digitally changes the ballot images: "After scanning, the device imprints details about the scanning event onto the ballot and adds this information digitally to the ballot image." Having software alter the ballot images should not be allowed, since it can too easily change votes, accidentally or on purpose. If this rule is not in the CA standards, it should be added for the future. p.19 of https://votingsystems.cdn.sos.ca.gov/vendors/dominion/ds519/ds519functional-report.pdf

7. They say it protects privacy, though ICX screen is big, nearly vertical, and easy to read from a distance. It needs a curtain or to face the wall. p.11 of https://votingsystems.cdn.sos.ca.gov/vendors/dominion/ds519/ds519staff-report.pdf

8. "Testing also uncovers other findings, which do not constitute non-compliance, and those findings are reported to the voting system vendor to address the issues procedurally." These should be reported so counties can be aware of them. p.1 of https://votingsystems.cdn.sos.ca.gov/vendors/dominion/ds519/ds519staff-report.pdf

9. People have wanted hashes of ballot images and CVRs. We see that "The examination determined that all results files and election relevant data either transmitted or contained in removable media are encrypted or digitally signed." p.30 of https://votingsystems.cdn.sos.ca.gov/vendors/dominion/ds519/ds519security-report.pdf

   While this is a positive claim, as members of the public, **we have never seen any digital signatures associated with election data**, nor have we seen any method for independent verification of these signatures.

Key Concerns:

1. **Are Digital Signatures Publicly Verifiable?**

- If election results files are truly signed, the **public should have access to the signatures and the associated public keys** to verify authenticity.
- Without independent validation, the presence of digital signatures remains **an unverifiable claim** rather than a demonstrated security measure.

2. **Which Cryptographic Standards Are Used?**

    - The report does not specify **which encryption and digital signature algorithms** are used.
    - Are modern, **NIST-approved cryptographic standards** (such as **ECDSA, RSA, or Ed25519**) employed?
    - How are key management and **revocation** handled?

3. **Can Election Observers Validate Signatures?**

    - Is there an **official process or tool** for the public, election observers, or auditors to verify digital signatures?
    - If signatures are included in election results files, **where are they published** for public review?

4. **How Are Removable Media Protected?**

    - If election data is stored on USB drives or other removable media, **who has access to the decryption keys?**
    - Are the encryption keys **unique per election** to prevent unauthorized reuse?

Public Comment Requests:

1. **Can the public independently verify election results files using digital signatures? If so, how?**
2. **Where are the digital signatures published, and where can the public obtain the necessary public keys?**
3. **What cryptographic algorithms are used for encryption and signing? Are they NIST-approved?**
4. **What tools are provided to verify digital signatures on election data?**
5. **How is key management handled, and how are outdated or compromised keys revoked?**

> Digital signatures are only meaningful if they can be **independently validated**. We request that the certifying body **clarify how election observers and the public can verify these signatures** to ensure election integrity.

All reports are at https://www.sos.ca.gov/elections/ovsta/frequently-requested-information/dominion-voting

The reports available for review of the Dominion System DO NOT include a list of a software, both as part of the official system and commercially off-the-shelf (COTS) components.

We urge the certifying body to require a **Software Bill of Materials (SBOM)** as part of the certification process for Dominion Democracy Suite 5.19 and all future voting system submissions. An SBOM provides a comprehensive inventory of software components, ensuring transparency, security, and supply chain integrity.

The COTS software included should be in SBOM format and provided for public review.

Rationale for Requiring an SBOM

1. **Transparency & Security**
    - An SBOM documents all software components, dependencies, and third-party libraries, enabling better **vulnerability tracking** (e.g., Log4j, OpenSSL exploits).
    - It ensures that **only authorized software is included** in the deployed system.
2. **Alignment with Election Security Standards**
    - The **U.S. Election Assistance Commission (EAC)**, **NIST**, and **CISA** emphasize **supply chain security** in election systems.
    - The **Voluntary Voting System Guidelines (VVSG 2.0)** stress the importance of **software integrity and auditability**, making an SBOM essential.
3. **Federal & Industry Best Practices**
    - **Executive Order 14028** mandates SBOMs for federal software procurement to improve cybersecurity.

- **CISA** has identified SBOMs as a critical security tool for protecting **critical infrastructure**, which includes election systems.

4. **Prevention of Unauthorized Software Installation**

    - An SBOM would reveal the presence of **Microsoft SQL Server Management Studio (SSMS)** or any other software not explicitly listed in the certified configuration.
    - Ensures election officials and security reviewers can verify **that only certified software is installed and used**.

Key Questions for Certification Review

1. **Was an SBOM included in this certification submission? If not, why?**
2. **In what format(s) is the SBOM provided, and is it machine-readable (CycloneDX, SPDX, SWID)?**
3. **Does the SBOM include all dependencies, including third-party libraries and embedded software?**
4. **Is the SBOM published for public verification, ensuring transparency in certified software?**
5. **How does the certification process ensure that only listed software is installed in actual deployments?**

Given the importance of **software transparency and security in election systems**, we strongly recommend that an **SBOM be required for certification** and that it be made available for independent verification. If an SBOM was not provided in this submission, we request a justification for its absence and a timeline for its inclusion in future certifications.

Review of COTS and other software components

As there was no list of software components, we turned to the DVS 5.20 release submitted and certified by the EAC.

https://www.eac.gov/sites/default/files/2025-02/DVS%205.20%20Certificate%20and%20Scope%20of%20Conformance.pdf

https://votingsystems.cdn.sos.ca.gov/vendors/dominion/ds519/ds519functional-report.pdf

Potentially Concerning or Outdated Components:

California's review documents need to list third party commercial off-the-shelf (COTS) software, and evaluate its reliability. The application has that information, CCR 2-7-6.1 20701(a)(7). EAC says the following are in a later version, 5.20, so they are likely to be in 5.19, and would create insecurity. Pages 8 & 21 of the Security and Telecommunications Test Report (https://votingsystems.cdn.sos.ca.gov/vendors/dominion/ds519/ds519security-report.pdf) say virus & malware programs are included & updated, and do not give their names or tests for hacking and mistakes.

1. **Visual Studio 2022 Professional**

    - **Why is an IDE (Integrated Development Environment) included in the certified voting system?**
    - **Typically, production environments do not require Visual Studio, as compiled binaries should already be packaged and deployed without needing an IDE.**
    - **If it is only for development and not deployed in the live system, it should not be part of the certification.**
    - **An IDE implies that users will be editing, testing and changing software programs. This should never be part of any critical and certified systems such as a voting system.**

2. **Microsoft SQL Server Management Suite (SSMS)**

    - **This is NOT listed as a COTS component in V5.20 certified system, but we understand that Dominion Election Management System deployments DO include the SSMS.**

      We are concerned that Microsoft SQL Server Management Studio (SSMS) has been included in previous deployments of Dominion's Election Management System (EMS) but is not listed as a Commercial Off-The-Shelf (COTS) component in the certified software package. SSMS is a powerful administrative tool that provides direct database access, potentially bypassing application-level security controls.

      ### Specific Concerns:

      1. **Is SSMS installed or allowed to be installed in certified deployments?**

- **SSMS is not necessary for normal election operations and should not be included in any certified deployment.**
- **If SSMS is installed post-certification, what mechanisms prevent its misuse?**

2. **What prevents unauthorized modifications to the election database?**

    - **If SSMS is present, does the system enforce role-based access controls (RBAC) that prevent election officials from using SSMS to modify vote data?**

    - **Does the SQL Server instance prevent direct modifications outside of the EMS application?**

    - **Even if the database is not altered, the existence of the SSMS would provide a mechanism for election staff to determine the totals of votes cast in early voting prior to the close of polls.**

3. **How does the system detect and prevent direct database access?**

    - **Are SQL audit logs enabled and externally monitored?**
    - **Can logs be tampered with, or is event logging enforced and immutable? (We see event logging can be turned off.)**

    Given that the SSMS could be used inappropriately in election systems, we request transparency on whether SSMS is installed, whether it can be installed post-certification, and what safeguards exist to prevent unauthorized database modifications.

    We urge the certifying body to clarify these points and ensure that SSMS is explicitly prohibited in all certified EMS deployments unless it is necessary for administrative purposes with strict controls.

3. **Windows 11 Professional Instead of Windows Server**
    - **Windows 11 Pro is included as an EMS server component, but Windows Server 2022 is available.**

- **Why are EMS servers running Windows 11 instead of Windows Server?**
- **Workstation OSes like Windows 11 Pro lack the security features of Windows Server for mission-critical applications.**

4. **Android 8.1.0 for ICX Components**
   - **End of support in 2021 → No security updates.**
   - **Why is an unsupported OS used in a voting system?**
   - **Devices should use an actively supported version.**

5. **Outdated .NET and Visual C++ Versions**
   - **.NET Framework 3.5 (Released in 2007) and 4.8 (Released in 2019)**
     - **3.5 is very old and generally discouraged unless absolutely necessary.**
   - **Microsoft Visual C++ Redistributables (2013, 2015)**
     - **While they may be required for legacy compatibility, relying on old runtime libraries introduces security and maintainability risks.**

6. **Use of SQL Server 2022 Standard (Not Enterprise)**
   - **SQL Server Enterprise includes high availability and advanced security features that are critical for an election system.**

7. **Use of SQLite in Multiple Places**
   - **SQLite (1.0.116.1, 3.7.13, various versions) is included.**
   - **SQLite is not a robust database for high-security environments.**
   - **Why is SQLite used when Microsoft SQL Server 2022 is also included?**
   - **SQLite does not support multi-user concurrency well.**

8. **Older Cryptographic Components**
   - **OpenSSL 1.0.2K, 1.0.2j → No longer supported; latest OpenSSL is 3.x.**
   - **Why are old OpenSSL versions still present in a security-sensitive system?**
   - **If needed for legacy reasons, have they been hardened against vulnerabilities?**

9. **Inconsistent Linux Kernel Versions**
   - **Kernel 2.6.30.9 (uClinux), 4.9.11 (ICP2), and Ubuntu (unspecified version)**
   - **Why are these different versions used instead of a unified, modern Linux kernel?**

- **Some versions are decades old.**

10. **Use of TX Text Control Library for .NET (Version 16.0 from ~2010)**
    - **Why is an old text processing component included?**
    - **If used for generating reports, it may lack modern security patches.**

11. **Old Infragistics UI Libraries**
    - **NetAdvantage 2011.1, 2012 Vol. 1, 2013.1 → Over a decade old.**
    - **Why are outdated UI libraries included?**
    - **If used for legacy reasons, have they been hardened against UI-related vulnerabilities?**

12. **Use of Microsoft Access Database Engine 2010**
    - **Why is Access 2010 used instead of modern database connectivity?**
    - **Access databases are not designed for mission-critical environments.**

The Security and Telecommunications Test Report says the attack team prioritized "easily exploitable vulnerabilities" (p.33). That does not protect us from nation-states or strong criminal groups. It was supposed to have 12 staff weeks, and had less (p.36). Add more time to the review.

The Security and Telecommunications Test Report says "Testing performed" included "picking of locks and attempts to circumvent or bypass security seals and security screws." It says "Testing validated that the requirement was satisfactorily covered." This is misleading, since California Voting System Standards (CVSS) (https://admin.cdn.sos.ca.gov/regulations/elections/california-voting-system-standards.pdf) have no requirements on picking locks and bypassing seals. It is good the locks and seals were tested, so the extent of testing needs to be given, since “no seal is unspoofable (just as no lock is undefeatable)” Johnston & Warner.

Lack of Sufficient Criteria for Auditing

The current certification criteria has a very limited criteria and lacks comprehensive review of the auditability of election results. To ensure transparency and public trust, a separate section should be added to the certification criteria, addressing the following auditability requirements:

1. **Registered Voter List**
    - **The election system should produce a complete list of all registered voters as of the time of the election, in a standardized format.**

2. **List of Actual Voters**
    - **The system should provide a list of all voters who participated in the election, including their voter IDs and relevant voting details, ensuring compliance with privacy and legal protections.**

3. **Cast Vote Record (CVR) Format**
    - **The election system should generate a ballot-by-ballot Cast Vote Record (CVR) with unique but untraceable ballot numbering.**
    - **The recently discovered "DVSorder" vulnerability (see DVSorder.org) demonstrated how an insufficiently robust pseudo-random number generator could reveal the order in which voters cast their ballots.**
    - **Certified systems must mitigate this risk to ensure CVRs can be published without compromising voter anonymity.**

4. **Ballot Image Availability**
    - **The system should provide ballot images that are unlinkable to voter identity and available for public inspection. Each ballot image should be cryptographically hashed, and the hash should be digitally signed using a private key generated internally by the scanner that created it. The public keys of all scanners should be published prior to the election to enable independent verification. This approach ensures that ballot images remain tamper-proof and allows for external validation that no modifications—such as unauthorized alterations or post-processing imprinting—occurred after scanning.**

5. **Batch Reporting for Audits**
    - **If batch processing is used, the Election Management System (EMS) must generate a comprehensive report of all batches and precincts prior to any random selection process for audit purposes.**
    - **This report should be publicly available before any audit begins.**

6. **Database Audit and Log Verification**
    - **The system must define an auditable procedure to snapshot the SQL database before and after the election.**
    - **All log entries should be applied to the initial snapshot to confirm that the final state of the database is consistent with all recorded actions.**
    - **This verification should be a standard election audit practice, with results published for transparency.**

7. **Support for Risk-Limiting Audits (RLAs) and Other Audit Methods**

- **The voting system should support:**
  - **Ballot-comparison Risk-Limiting Audits (RLAs)**
  - **Batch-comparison RLAs**
  - **Exhaustive ballot image audits**
- **The system must facilitate these audit types to ensure election integrity and public confidence.**

A robust auditing framework is essential for verifying the integrity of election results. These criteria should be formally incorporated into the certification process to enhance transparency, prevent vulnerabilities, and provide clear mechanisms for independent verification of election outcomes.

Thank you for this opportunity to comment on this certification. Please feel free to contact Ray Lutz at raylutz@citizensoversight.org if you have any questions.

Sincerely,

Ray Lutz
Executive Director,
Citizens Oversight.