IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLORADO

Civil Action No. __1:25-cv-00425 STV

TINA M. PETERS, Applicant,

v.

MOSES "ANDRE" STANCIL in his official capacity as the Executive Director of the Colorado Department of Corrections, and **PHILIP J. WEISER**, in his official capacity as Attorney General of the State of Colorado, Respondents

---

NOTICE OF FILING

To the Court and all parties:

Please take notice that, in response to the Court's invitation to provide additional information (ECF 67), Applicant files herewith the sworn testimony of a former Venezuelan government official who assisted the government in rigging Venezuelan elections using Smartmatic software from 2003 through 2016. Based on his own personal knowledge, computer expertise, and examination of the forensic image preserved by Tina Peters, the witness testified that Smartmatic software has the same structure and vulnerabilities as the Dominion software used in Mesa County and 61 other Colorado counties, and that elections in Colorado

using Dominion software are just as insecure as the elections that were rigged by the Venezuelan government using Smartmatic software. Venezuelan software engineers who designed the Smartmatic software to rig Venezuelan elections now work for Dominion in the United States. The witness also testified that in Venezuela, people who criticized the voting system were prosecuted by the same government that rigged the elections. The evidence before this Court shows that the judge who sentenced Clerk Peters to nine years in prison, and denied her bond on appeal, gave as his justification that Mrs. Peters' public statements about the voting system were "lies" that made her a "danger" to the community. The attached transcripts show that Mrs. Peters' public statements about the voting system were true. There is no legal justification, and there never was, for incarcerating Tina Peters without bond.

SUMMARY OF TESTIMONY WITH CITATIONS TO TRANSCRIPTS

References to transcripts are "AM" (9/18/25 morning transcript) and "PM" (9/18/25 afternoon transcript) with page numbers.

1. Mesa County Forensic Images Exposed Dominion Vulnerabilities

- Mesa County's forensic images of Dominion Software contained the same vulnerabilities the witness had seen in Venezuela's Smartmatic systems:

encryption flaws, plain-text passwords, and exposed source code that allowed undetectable manipulation (PM 50–51).

- Dominion's log files were configured too small, causing data to be overwritten during elections, thereby erasing critical evidence needed for an audit (PM 17–19, 26–27).

- The "trusted build" conducted by the Secretary of State in May 2021 erased all 2020 election records, in violation of 52 U.S.C. § 20701 requiring preservation for 22 months (PM 24–26).

2. U.S. Elections Are Not Secure

- U.S. elections are not secure because Dominion's software contains "basic" vulnerabilities left uncorrected for years, making manipulation possible by any engineer with system access (AM 6, 25–26).

3. SAES Tool and Rigging in Venezuela

- Venezuela used Smartmatic's "SAES data utility tool" to emulate voting machines and inject false votes without detection (AM 12–15; PM 29–31, 45, 51–52).

- Example: In the state of Merida, transmissions for the entire state were falsified through SAES, ensuring the election of a government-favored candidate (PM 29–31).

- SAES data utility tool was presented as a legitimate system-testing tool, but in practice it became the government's instrument to inject phony votes in rigged elections.

4. Suppression of Whistleblowers

- Venezuelans who criticized Smartmatic were prosecuted, often with evidence provided by Smartmatic itself. Judges lacked the expertise to verify whether that evidence was genuine (PM 6–7).

5. Engineers moved from Smartmatic to Dominion

- **Ronald Morales** – Smartmatic engineer now employed by Dominion; installs "man-in-the-middle" systems for remote access to county voting systems (PM 23, 31).

- **David Moreno** – Developed Smartmatic software; now manages Dominion's Texas warehouse and configures U.S. election equipment (PM 31–32).

- **Heider Garcia** – Former Smartmatic engineer; now head of elections in Dallas County, Texas (PM 32–35).

6. Audits Are Controlled and Ineffective

- Election audits only reveal what the companies allow. Source code is withheld, and tools like SAES data utility are excluded from review, leaving true manipulation undetectable (AM 17–18; PM 45).
- Witness confirmed that digital ballot images can be altered inside Dominion machines without trace (PM 43–46).

7. Foreign Manufacturing and Firmware Risks

- Dominion and Smartmatic machines use components manufactured in China and assembled in Taiwan. Firmware may be configured overseas to keep internal modems enabled, permitting covert internet connections even when software reports them disabled (AM 9–12; PM 53).

8. Venezuelan and Cuban Government Involvement

- Venezuela financed Smartmatic with $250,000 to build its election system in 2003, later paying $140 million annually to run the elections. In exchange, the government received 28% ownership and full rights to the source code, stored at the Venezuelan central bank in Caracas (PM 13–15, 48–49).

- Cuban communist managers were directly involved in Venezuela's elections, exercising oversight (PM 7–8).

9. Dominion's International Operations

- Dominion maintains headquarters in the U.S., Canada, and Serbia. The Serbian office is responsible for resolving U.S. election software issues on election days (AM 22).
- Remote access to U.S. election systems is achieved through "man-in-the-middle" setups, allowing Dominion engineers to make changes during elections via VPN or virtual machines (PM 20–23).

10. Witness Qualifications

- The confidential witness testified to having over 20 years of experience in electoral systems and information technology, beginning in Venezuela in 2003. He served as the National Coordinator within the Venezuelan National Electoral Council. In that capacity, he was responsible for:
    - Configuring and managing Smartmatic voting equipment and data transmission systems used nationwide in Venezuela (2003–2016) (AM 7).

- Establishing and overseeing national and state-level "war rooms" (situation rooms) where election results were monitored, manipulated, and directed by top government officials, including the President, Vice President, ministers, and senior military leaders (AM 8).
- Supervising audits conducted with international observers such as the Carter Center and the European Union (AM 9).
- Managing data centers containing voter records, biometric systems, and election backups (AM 10).
- Direct oversight of Smartmatic engineers and technology integration, including interactions with Sequoia and Dominion systems after their acquisitions AM 21-22).

Summary

The witness drew a direct connection between Smartmatic's Venezuelan election rigging and the vulnerabilities found in Mesa County's Dominion forensic images. He testified that Dominion's system architecture shares core elements with Smartmatic, enabling manipulation through the same methods: deliberately small log files, accessible source code, SAES data utility style tools, and remote "man-

in-the-middle" connections. He concluded that Dominion systems, built with Chinese components in a voting system designed by former Smartmatic engineers, are not secure or auditable in U.S. elections.

Respectfully Submitted September 23, 2025.

Patrick M. McSweeney
Robert J. Cynkar
McSweeney, Cynkar & Kachouroff, PLLC
3358 John Hill Tree Road
Powhatan, VA 23139
(804) 937-0895
patrick@mck-lawyers.com

s/ John Case
John Case
John Case, P.C.
6901 S. Pierce St. #340
Littleton CO 80128
(303) 667-7407
brief@johncaselaw.com

THE TICKTIN LAW GROUP
270 SW Natura Avenue
Deerfield Beach, Florida 33441
Telephone: (561) 232-2222

__/s/ Peter Ticktin_____
PETER TICKTIN, ESQUIRE
Florida Bar No. 887935
Serv512@LegalBrains.com

Co-counsel for Applicant Tina M. Peters

CERTIFICATE OF SERVICE

I hereby certify that on September 23, 2025, I electronically filed the foregoing with the Clerk of the Court using the CM/ECF system, which will cause an electronic copy of same to be served on counsel of record via the email addresses that counsel registered with the Court's ECF system.

s/ Linda Good