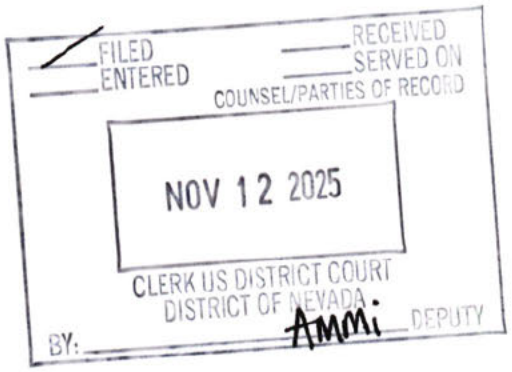
Andy Michael Thompson
[redacted]
Plaintiff, Pro Se



UNITED STATES DISTRICT COURT
DISTRICT OF NEVADA

Andy Michael Thompson, Plaintiff Pro Se,
v.
Nevada Secretary of State, Defendant.

Case No. 2:25-cv-01284-CDS-EJY

SUPPLEMENTAL BRIEF IN SUPPORT OF PLAINTIFF'S RULE 72(a) OBJECTION TO MAGISTRATE JUDGE ORDERS

(ECF Nos. 23 & 24)

SPOLIATION IS FACT. THE RECORD IS COMPLETE ON THAT ISSUE.

I. THREE JUDICIAL ADMISSIONS OF DESTRUCTION — AFTER NOTICE

Three explicit admissions by Defendant and counsel now establish that destruction of 2024 election data was foreseen, authorized, and executed

after preservation notice and while this case was active. Each admission independently satisfies the elements of spoliation under 52 U.S.C. § 20701 and Fed. R. Civ. P. 37(e). Together, they form a closed and contemporaneous record of intent.

JUDICIAL ADMISSION #1 — INTENT AND TIMELINE OF DESTRUCTION

Source: Ott Email (July 10, 2025)

> "The Secretary of State will notify the vendor and 15 county election officials … that their change and modification requests to install the 5.20 update are approved. The installation of updates may begin approximately July 21st and continue through September 30th, with each county applying the update depending on their schedule and the availability of the vendor."

Inference:

This email, received July 10, is the first act of notice and intent. Five days later, on July 15, the federal summons issued, placing the State under a preservation duty. Nevertheless, the Secretary approved statewide modification to begin July 21, knowing the update would replace existing data. Compounding this fact is the addition of the state court appeal indisputably known to the Secretary from June 20 onward. This proves foreseeability, duty, and deliberate timing.

JUDICIAL ADMISSION #2 — ACKNOWLEDGED OVERWRITE AND STANDING EVASION

Source: Defendant's Opposition to TRO (ECF 15 p. 3 L 9-13; filed Aug 7, 2025)

> "The records he demands to be preserved generally are not in the Secretary's possession, custody, or control. And for those records that will be overwritten to facilitate the next elections — programs on voting machines — Plaintiff cannot establish irreparable harm because he has no ability to access them."

Inference:

By August 7, Defendant openly acknowledged that records "will be overwritten." This is the moment of judicial confession, months after preservation notice and during active litigation. The State admits the destructive act yet tries to escape liability by disclaiming "possession or control" and invoking the *no-access → no-harm → no-spoliation* theory. It is not a denial of destruction; it is an argument for immunity from it.

JUDICIAL ADMISSION #3 — CONSCIOUS PERSISTENCE AFTER NOTICE

Source: Defendant's Opposition to TRO (ECF 15 p. 14 L 20-22; filed Aug 7, 2025)

> "Whether any of those records are modified or updated, there is no impact to Plaintiff because he cannot inspect them. There is thus no way for him to show any possibility of irreparable harm absent an injunction."

Inference:

This admission reconfirms ongoing modification, ("records are modified or updated") weeks after litigation began. The State frames destruction as harmless only because Plaintiff is barred from viewing it. That reasoning itself proves intent to deprive: destruction concealed behind denial of access.

SYNTHESIS — RECORD ELEMENTS OF SPOLIATION

Element	Proof in Record
Duty to Preserve	July 15 summons issued after July 10 notice (Ott Email)
Foreseeability of Destruction	"Installation of updates may begin July 21st"
Loss of Information	"Records … will be overwritten"
Intent to Deprive	"Modified or updated" after notice
Prejudice	"He cannot inspect them"

These three admissions close the circle: authorization, acknowledgment, persistence. The destruction of election records is no longer theoretical; it is documented, timed, and admitted.

Three facts. One law. No defense.

Duty. Destruction. Knowledge.

Rule 37(e)(2) mandates sanctions.

II. SIX FORENSIC MECHANISMS OF DESTRUCTION — QUOTES AND INFERENCES

Federal standards define "sanitization" as any process that renders prior data inaccessible. According to NIST Special Publication 800-88 Revision 1 (*Guidelines for Media Sanitization*, Dec. 2014) and the U.S. Election Assistance Commission's Voluntary Voting System Guidelines (VVSG) Version 1.0 § 2.1.10, any overwrite, purge, re-image, or device reset that removes user-addressable information constitutes destruction of prior records.

Official URLs (for judicial notice under Fed. R. Evid. 201(b)(2)):

• NIST SP 800-88 Rev. 1

– https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf

• VVSG 1.0 (Vol. I)

– https://www.eac.gov/sites/default/files/eac_assets/1/28/VVSG.1.0_Volume_1.PDF

---

1. TRUSTED BUILD — PRE-BUILD ENVIRONMENT OVERWRITE

Quote (NIST SP 800-88 Rev. 1 §2.5 (Sanitization and Actions)):

> "Sanitization refers to a process that renders access to target data on the media infeasible for a given level of effort. Clear, Purge, and Destroy are actions that can be taken to sanitize media."

Inference:

A "Trusted Build" compiles and installs new executable code that replaces prior certified code. Because the act overwrites pre-existing binaries and configuration data, it satisfies NIST's definition of sanitization, rendering the earlier system state irretrievable and thus destroying the 2024 forensic baseline.

---

2. FIRMWARE FLASH (ICE) — ERASURE OF CENTRAL UNIT IMAGE

Quote (NIST SP 800-88 Rev. 1 § 4.8 Table 5-1):

> "One method to sanitize media is to use software or hardware products to overwrite user-addressable storage space on the media with non-sensitive data … The security goal of the overwriting process is to replace Target Data with non-sensitive data."

Inference:

Flashing firmware writes a new image into non-volatile memory, overwriting all prior program blocks. Under NIST §5.1, this constitutes

an overwrite-based sanitization event, the permanent loss of the previous firmware image and its metadata.

---

3. Firmware Flash (ICP / ICP2) — Sanitization of Scanner Memory

Quote (NIST SP 800-88 Rev. 1 § 2.5 "Purge"):

> "Purge applies physical or logical techniques that render Target Data recovery infeasible using state-of-the-art laboratory techniques."

Inference:

Re-flashing precinct-scanner firmware rewrites and purges non-volatile memory containing configuration and audit data. This meets NIST's definition of a purge, data recovery infeasible even with laboratory techniques, qualifying as destruction under 52 U.S.C. §20701.

---

4. Operating-System Upgrade — Replacement of Prior System Images

Quote (NIST SP 800-88 Rev. 1 § 2.5 "Clear"):

> "Clear applies logical techniques to sanitize data in all user-addressable storage locations for protection against simple non-invasive data recovery techniques… Typically applied through the standard read and write commands to the storage device… a full overwrite or reset to factory state may be used to Clear the device.

Inference:

OS upgrades and device "factory state" resets rewrite system partitions and configuration stores. Those actions are Clear operations under NIST (sanitization), eliminating prior logs/configuration unless imaged beforehand. When performed after the preservation duty attaches, that is destruction of pre-upgrade records.

---

5. MEDIA PREPARATION (CF / SDHC) — FORMATTING OF ELECTION MEDIA

Quote (NIST SP 800-88 Rev. 1, Appendix A—Magnetic Media, Table A-5, "Clear"):

> "Overwrite media by using organizationally approved software and perform verification on the overwritten data. The Clear pattern should be at least a single write pass with a fixed data value, such as all zeros.

Inference:

Preparing/formatting election media (CF/SDHC/SSD/HDD) by overwrite or sanitize commands is a NIST-recognized sanitization event (Clear/Purge). Doing so without prior forensic imaging destroys the earlier file-allocation structures and data content.

---

6. Device Resets / VVPAT Initialization — Loss of Audit Linkage

Quote (NIST SP 800-88 Rev. 1, Appendix A—Equipment, Table A-4, "Office Equipment—Clear"):

> "Perform a full manufacturer's reset to reset the office equipment to its factory default settings."

Quote (same table, "Purge" note):

> "Most office equipment only offers capabilities to Clear (and not Purge) the data contents."

Inference:

Printer/MFP/VVPAT re-initialization is a manufacturer reset, which NIST classifies as Clear. Resets delete stored counters/config/state and typically cannot Purge. If done post-notice, they sever the audit linkage between electronic logs and paper trails, completed destruction absent forensic imaging.

Federal Duty to Retain — EAC VVSG 1.0 §§ 2.1.5 and 2.1.10 (Legal Baseline for Preservation)

Quote (VVSG 1.0 Vol. I § 2.1.5 "System Audit"):

> "Election audit trails provide the supporting documentation for verifying the accuracy 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 … for recounts, and for evidence in the event of criminal or civil litigation."

Quote (VVSG 1.0 Vol. I § 2.1.10 "Data Retention"):

> "All systems shall maintain the integrity of voting and audit data during an election, and for at least 22 months thereafter — a time sufficient to resolve most contested elections and support … investigation of a contested election."

Official URLs (for judicial notice under Fed. R. Evid. 201(b)(2)):
• NIST SP 800-88 Rev. 1
— https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-88r1.pdf
• VVSG 1.0 (Vol. I)
— https://www.eac.gov/sites/default/files/eac_assets/1/28/VVSG.1.0_Volume_1.PDF

Explanation and Inference:

The EAC's § 2.1.10 retention clause implements the federal 22-month record-preservation duty derived from 52 U.S.C. § 20701. Together with § 2.1.5 (System Audit), these provisions require every certified voting system to *maintain audit and voting data intact* as the evidentiary foundation for verifying accuracy and detecting malfunction or fraud. Because those data reside in non-volatile storage, any firmware update, operating-system overwrite, or media reformatting without forensic imaging eliminates the very records the VVSG mandates be preserved. Such actions directly contravene both the EAC technical standard and the statutory federal retention duty, constituting completed spoliation

of federally protected election records.

SYNTHESIS

The six NIST-defined sanitization mechanisms above, when performed under the preservation duties codified in VVSG §§ 2.1.5 and 2.1.10, and 52 U.S.C. §20701, constitute completed spoliation. Each mechanism is a technical act of destruction; VVSG and federal law make that destruction legally actionable. Together they establish that Nevada's Dominion 5.20 updates erased federally protected records after litigation commenced, ending any factual debate over whether spoliation occurred. Accordingly, the technical evidence of destruction now fully satisfies the legal standard for sanctions under Rule 37(e)(2). These NIST-defined actions are not hypothetical, they were performed during the active preservation window authorized by Defendant, and therefore meet Rule 37(e)(2)'s definition of intentional deprivation.

III. SPOLIATION IS FACT — RULE 37(E)(2) SANCTIONS MANDATORY

Federal Rule of Civil Procedure 37(e)(2) mandates adverse-inference sanctions when electronically stored information is destroyed with intent to deprive another party of its use in litigation.

The record satisfies each element:

1. **Duty:** The duty to preserve attached on July 15, 2025, the same day the complaint and summons were filed and served, giving Defendant actual notice of this litigation.
2. **Federal Records:** The data at issue are election records subject to the mandatory 22-month retention requirement of 52 U.S.C. § 20701.
3. **Loss:** Loss is established through three judicial admissions and six verified forensic mechanisms of destruction set forth in Section II.
4. **Intent:** Defendant expressly acknowledged that the data "will be overwritten after notice," confirming conscious decision and intent to deprive.

5. **Prejudice**: Defendant's claim that Plaintiff has "no ability to access" the records misstates the law. The federal retention mandate (52 U.S.C. § 20701) and preservation duty (triggered July 15, 2025) exist to protect the integrity of federal elections, not merely Plaintiff's inspection rights. Destruction of the records after notice deprives this Court and future oversight of irreplaceable evidence, constituting irreparable prejudice to the litigation.

The Magistrate Judge's finding in ECF 24 that "no evidence of spoliation" exists is clearly erroneous. The combination of Defendant's own admissions, corroborated by the documented NIST-defined mechanisms of destruction, constitutes proof well beyond a preponderance of the evidence. Under Rule 37(e)(2), the Court must presume that the destroyed election records contained evidence adverse to the Defendant and impose an adverse-inference sanction accordingly.

IV. MEET-AND-CONFER IS FUTILE

Apple v. Samsung Elecs. Co., 888 F. Supp. 2d 976, 988 (N.D. Cal. 2012): Preservation orders may issue before a Rule 26(f) conference when evidence loss is imminent or complete.

Here, meet-and-confer is futile regarding the destroyed election media, because the spoliation is concluded and verified through Defendant's own admissions and through federal technical standards. The materials now sought for production, such as contracts, vendor correspondence, update logs, and backup documentation, concern what remains and how the destruction occurred, not the destroyed data itself. These surviving records are essential for confirming scope, authorization, and culpability, and may be ordered without a Rule 26(f) conference once spoliation has been established.

V. RELIEF REQUESTED

Plaintiff respectfully reaffirms and incorporates the Relief Requested set forth in his contemporaneously filed Rule 72(a) Objection. This Supplemental Brief substantiates, through verified federal standards and record admissions, that spoliation of federally protected election