FILED RECEIVED
ENTERED SERVED ON
COUNSEL/PARTIES OF RECORD
AUG 13 2025
CLERK US DISTRICT COURT
DISTRICT OF NEVADA
BY: DEPUTY

Andy Michael Thompson
[redacted]

UNITED STATES DISTRICT COURT
DISTRICT OF NEVADA

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

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

**REPLY TO NEVADA SECRETARY OF STATE'S OPPOSITION TO MOTION FOR TEMPORARY RESTRAINING ORDER AND EXPEDITED HEARING**

COMES NOW, Plaintiff brings before this Court (52 U.S.C. §20701 and 42 U.S.C. § 1983 violations) representing discrete injuries to Plaintiff by the Defendant, his recent actions appearing to be in violation of federal law. Plaintiff had sought relief outside of this Court but Defendant will acknowledge neither violation of law nor harm, whether intended or unintended, maintaining a position of having no obligations or responsibility in the matters herein.

## REPLY TO SPURIOUS PLEADINGS

### 1. Baseless Rooker-Feldman

Rather than being "blatantly... and ... clearly violative" (Opposition, page 1), Plaintiff's action here is altogether untouched by Rooker-Feldman. As Plaintiff's case is clearly on active appeal, and the dismissal being therefore not final, Rooker-Feldman is clearly misused against Plaintiff. It states, "We hold that, under what

has come to be known as the Rooker-Feldman doctrine, lower federal courts are precluded from exercising appellate jurisdiction over **final state-court judgments**." (*Exxon Mobil Corp. v. Saudi Basic Indus. Corp.*, 544 U.S. 280, 283 (2005)), bold emphasis added.

Rooker-Feldman is inapplicable to non-final judgments. Defendant correctly pleads that Plaintiff's case is on appeal (Opposition, page 2, 6 and 23) and the Order on Motions fully acknowledges the case is on appeal and that dismissal is not yet final, "if this Court is wrong, or those cases are wrong, or the statues are unconstitutional—all of which Plaintiff suggests is the case—then the Supreme Court is the one to say so" (Order on Motions, page 4, lines 14-17).

The self-contradicting invocation of Rooker-Feldman is a manifest error (*Exxon Mobil Corp.*). Moreover, this action before this Court is not a response the June 18 dismissal in State District Court. This action is independent of the State Court being prompted solely by the actions of the Secretary of State as indicated to this Court in the Gregory Ott July 10 email (Exhibit A of the Declaration for the TRO). Furthermore, Defendant's pre-dismissal position to forego updates has shifted post-dismissal betraying the Appellate process and harming Plaintiff's rights.

Plaintiff's rights did not dissolve at dismissal. Plaintiff seeks limited relief through this Court. Plaintiff is seeking preservation—a necessary step beyond retention due to data and record destruction caused by updates—not access to records: the Supreme Court of Nevada will decide access, as such final determination is currently held in appeal there. Rooker-Feldman's use in Defendant's pleading for

dismissal in an arbitrary leap and must be rejected as false application of doctrine. This action is not seeking this Court's review of the state court's dismissal.

**2. Frivolous is Fictional Mischaracterization**

Plaintiff is accused of bringing frivolous action and seeks to tie that mischaracterization before this court. Plaintiff now argues merit; not because he seeks this Court to review any other court's decision, but to dispel the notion presented to this Court by the Defendant. Plaintiff's case before the Eighth District Court was "not being presented for any improper purpose, such as to harass, cause unnecessary delay, or needlessly increase the cost of litigation," (NRCP 11(b)(1)). Plaintiff rejects this characterization. Plaintiff will here now inform the Court how that the case so maligned is neither "indisputably meritless" or "baseless," (*Bergstrom v Estate of DeVoe* 109 Nev. 575, 578, 854 P. 2d 860, 862 (1993)). The case and claims are substantive.

Plaintiff presented to the district court three primary exhibits detailing how statewide records and data, used by the Secretary for Certification and placed into his custody for reporting, failed to demonstrate valid election results and failed to show a valid election process. Still, Defendant holds to their part in certification of the 2024 General Election (Election):

I. Three days after the Election, on November 8, 2024, Secretary reporting showed that from two counties, Washoe and Clark, nearly 27,000 ballots had disappeared from the statewide mailed ballot totals. The Secretary's office was informed of this staggering amount "sufficient to raise reasonable doubt as to the outcome of the election", NRS 293.410 (2)(f).

All attempts to reconcile this matter have failed. Inexcusably, the evidence submitted has been disregarded and remains unrebutted. All engagement over the missing ballots has made the matter worse, namely: the Secretary was provided data explicitly showing that two counties, Washoe and Clark, distinctly contributed to the total of nearly 27,000 missing ballots, and all engagement by the Secretary has erroneously claimed that by only fixing one unproven copy and paste error from Clark County the whole problem is deemed to be solved.

This impossible math, pleading that fixing one County somehow fixes two, is inexcusable from Nevada's Chief Officer of Elections, NRS 293.124; no faithful execution of duty can tolerate such oversight and deficient administration with such valuable things as the votes of Nevada's Electorate.

II. Five days after the Election, in the Secretary's November 11, 2024 update, the Secretary reported that out of nearly 41,500 more mailed ballots received, less than 1,500 of those ballots contained votes for either Trump or Harris. This represents an unprecedented 96% undervote, statistically and especially unheard of in a presidential election, suggesting that nearly 40,000 ballots added to the totals five days after the Election could very well be fraudulent. It is such a large number so as to potentially reverse the outcome of a third of all down-ballot races.

The Secretary has failed to reconcile this matter. Pleading in multiple court documents, the Secretary has failed to recognize and distinguish the

difference between the Trump/Harris undervotes (ballots having no vote for either Trump or Harris) and Total undervotes (ballots having no vote for any presidential candidate). The Secretary has repeatedly directed Plaintiff to consider their own published data and accept that what Plaintiff puts forth for undervotes, 40,000 is roughly only 3,000. Note, the Secretary engaged this issue and cited their own published data to offer resolution, further establishing their position as Chief Officer.

This resolution, however, is misleading and establishes a nonsensical apples-and-oranges comparison. Trump/Harris Undervotes are not the same as Total Undervotes. Yet, this did not stop the Secretary from asserting Total Undervotes for resolution of the Trump/Harris Undervote problem and ascending to it as a valid resolution, multiple times. The repeated and deficient resolution offered by the Secretary demonstrates clear administrative failure: the Chief Officer is fully expected to administer accurate and sufficient resolutions to complaints of violations, errors and suspected fraud, and the Secretary has demonstrably failed so to do.

Furthermore, and even more concerning, the Secretary repeatedly failed to discern the devastating consequence of their own pleading: that 40,000 undervoted mailed ballots on November 11, 2024, six days after the election, thereafter became 3,000 undervoted ballots. This means, according to their apples-and-oranges attempted resolution, that 37,000 ballots would have to have been altered after November 11, 2024 in order for them to plead the

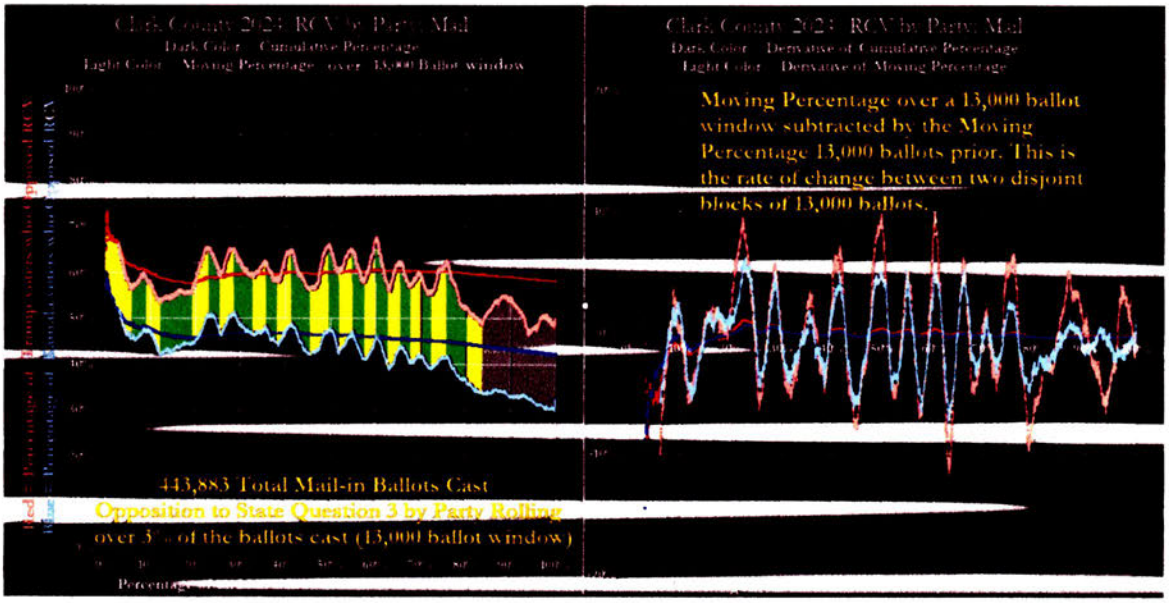
40,000 down to 3,000. That represents 37.000 mailed ballots potentially illegally altered and yet the Secretary has completely failed to notice this.

Now, and furthermore, when we remove the apples-and-oranges condition of the Secretary's pleadings we come to a corrected but still devastating circumstance. Plaintiff submitted Trump/Harris Undervotes in his case. To make a right comparison, distinct Trump/Harris undervoted ballots can be viewed in the Cast Vote Record (CVR)—the official record of all votes cast on all ballots cast in the Election. This is the record used by the Secretary, for their part, in the Certification of Elections, NRS 293.387 and .395. Upon examination of just the Clark County CVR, slightly more than 20,000 Trump/Harris Undervotes are to be found.

- 20,000 is significantly different than 3,000—this shows the magnitude of the inaccuracy of the Secretary's pleadings.
- 20,000 (the apples-to-apples difference between the first-reported 40,000 Trump/ Harris Undervotes and the now 20,000 Trump/Harris Undervotes found in the Clark County CVR), is significant enough to alter the outcomes of one third of all down ballot races.

Plaintiff's case cannot be deemed frivolous given now that two different and independent failures from the Secretary are "sufficient to raise reasonable doubt as to the outcome of the election", NRS 293.410 (2)(f).

III. From the CVR itself, in particular the second one put forth by Clark County from the Election for the first was corrupted, a yet more staggering matter arises. Verified by multiple experts by multiple methods, the Clark County CVR for the 2024 Election shows that 272,800 ballots were manipulated effectively erasing voter intent. Specifically, yet not alone, the manipulation is manifest in the votes for and against Ballot Question 3 on rank choice voting (Q3). For 80% of the counting of mailed ballots, Trump/Harris voter opposition (NO votes) to Q3 is synchronized: they both follow each other with unnatural precision, behavior statistically impossible under a free voting process.




Approximately 462,192 mailed ballots were counted in the Election in Clark County, (https://www.nvsos.gov/sos/home/showpublisheddocument/15579/638672846983070000). 80% of that is 369,754. If 369,754 votes were synchronized, then 369,754

> ballots were violated. If 369,754 ballots were violated, then 369,754 voters were harmed. Akin to a witness's lie which undermines their whole testimony, the CVR allegedly witnesses that the Election is accurate and yet where it is found false in one thing it is assumed false in everything—falsus in uno, falsus in omnibus. This is the principle now thrice shown, that 369,754 manipulated (along with the missing and undervoted) ballots are "sufficient to raise reasonable doubt as to the outcome of the election", NRS 293.410.

What is truly staggering is that all this evidence has been disregarded so as to make it to be discarded. However, it remains unrebutted, and the merits have yet to be considered with any sincerity in adherence to duty. "Frivolous" is false here and this Court should reject such baseless mischaracterization.

**RESPONSE TO DEFENTAN'S MEMORANDUM OF POINTS AND AUTHORITIES**

**3. "Not a Contest" Is Not a Final Judgement**

As Plaintiff's case is on appeal, a final determination that he has not brought a contest has yet to be made. Defendant wishes to proceed in finality and pleads accordingly, yet pleads in error. The statute defining a contest (NRS 293.042) has been misread, or rather not fully read, to enable a conclusion of no contest. That faulty conclusion is the basis of the "no access" argument which is the basis of the "no merit" argument which are extensions of the original fault, not reading and applying the whole statute. See NRS 293.042

> **"NRS 293.042 "Contest" defined.** "Contest" means an adversary proceeding between a candidate for a public office who has received the greatest number of votes and any other candidate for that office or, in certain cases, any registered voter of the appropriate political subdivision, for the purpose of determining the validity of an election."

Upon reading the whole statute, the "in certain cases" clause clearly speaks: three prongs together satisfy the definition of a "**Contest**":

1) Any registered voter

2) Of the appropriate political subdivision

3) Purposing to determine the validity of an election

Plaintiff is 1) a registered voter who voted in the Election (Andy Thompson Declaration), 2) of the appropriate political subdivision—ballot questions have statewide impact, and 3) purposed to determine the validity of the Election upon substantial cause. These prongs demand no mention of a winning candidate as the substantial evidence brought forth implicates Defendant under NRS 293.410 violations establishing explicit grounds for contesting the Election while the same evidence does not distinctly identify a particular candidate. See NRS 293.410, (emphasis added):

> 2. An election may be contested upon any of the following grounds:
> ...
> (c) That:
> (1) Illegal or improper votes were cast and counted;
> (2) Legal and proper votes were not counted; or
> (3) A combination of the circumstances described in subparagraphs (1) and (2) occurred, in an amount that is equal to or greater than the margin between the contestant and the defendant, or otherwise in an amount sufficient to raise reasonable doubt as to the outcome of the election.
> ...
> (f) That there was a malfunction of any voting device or electronic tabulator,

> counting device or computer in a manner sufficient to raise reasonable doubt as to the outcome of the election.

Defendant may be sincere in arguing that Plaintiff has failed to establish a "**Contest,**" but Plaintiff pleads Defendant is sincerely wrong and the controversy is still live on appeal.

**4. Statutory Restrictions on Access**

Plaintiff seeks preservation not access. NRS 293.391, 293B.155, and 293B.170, restricting access and designating code as proprietary (NRS 293B.104), are irrelevant, as the TRO seeks preservation under 52 U.S.C. §20701, not access, which is under state court jurisdiction (Case No. A-24-906377-C, on appeal). Moreover, the SOS, as Chief Election Officer (NRS 293.124), can easily direct clerks to preserve records (NRS 293B.1045(6)) and duplicate code without disclosing proprietary information, avoiding Dominion's interests. Plaintiff also asserts it would be improper to yield deference to Defendant's interpretation on ambiguous statue, (Opposition, page 12).

**5. No Federal Jurisdiction Over State Election Law**

This action arises under 28 U.S.C. §1331, involving federal law violations (52 U.S.C. §20701, 22-month preservation; 42 U.S.C. §1983, voting rights deprivation) via the SOS's update approval (Ott Email, July 10, 2025). The TRO is independent of state election law disputes (Case No. A-24-906377-C), with the non-final dismissal (appeal, Case No. 90846) ensuring no state law infringement (Skinner, 562 U.S. at 532) as this is a separate federal constitutional challenge. The SOS's jurisdiction

claim can be viewed as a bad-faith attempt to evade federal liability continuing a pattern of inapplicable arguments.

**6. No Irreparable Harm**

As with the District Court, so here, Defendant is supplied with expert Declarations elucidating the destructive nature of Dominion systems in both their standard operating and updating process, (Parikh Declaration (¶¶ 12, 15–17) and Gould Declaration (Findings and Conclusions 4)). Updates, currently underway, (Ott Email), will destroy CVRs/code, causing irreparable harm to Plaintiff's voting rights (42 U.S.C. §1983). The SOS's authority to direct clerks (NRS 293B.1045(6), Ott Email) and custodial role over code, showing that claims of no control (NRS 293.391(1), 293B.105) are misleading: since Defendant shows power to order the update, he has proven he can order it to cease, per his statutory authority as Chief Officer NRS 293.124. Furthermore, it is noteworthy that Defendant rejected updates pre-dismissal and pursued them post-dismissal.

**7. No Likelihood of Success on Merits**

Plaintiff's voter status is undisputed (Thompson Declaration), and injury from SOS's update approval risks destroying evidence of irregularities (27,000 missing ballots, 96% undervote, 369,754 manipulated ballots), violating 52 U.S.C. §20701 and 42 U.S.C. §1983. Plaintiff has a clear individual right, and 52 U.S.C. §20701's preservation mandate supports a §1983 claim, as voting rights deprivation (Gonzaga Univ. v. Doe, 536 U.S. 273, 283 (2002)) is clear from SOS actions, in the light of Parikh and Gould Declarations.

County clerks and Dominion are not needed (Fed. R. Civ. P. 19), as the SOS's authority (NRS 293B.1045(6)) and custodial role allow preservation without impairing others' interests. If this was so, and certainly it is not, then Defendant's ordering of the updates (Ott Email) must then be considered an impairment to Clerk and Dominion interest. The Chief Officer is a sufficient person of sufficient statutory authority to grant relief, to order a pause on updates so that preservation can be ensured.

**8. Public Interest and Bond**

Elections are yet many months away, late May 2026. Mock elections are not critical at this time. The potential Mineral County Recall (Clerk Email) would have almost no effect, if any, on the TRO. Public interest greatly favors efforts to preserve integrity in the face of harmless delay. The burden of preservation is minimal not gargantuan. Defendant appears to intimidate the Plaintiff rather than deal sincerely, pleading gratuitously for a $26,531,312.50 bond. Plaintiff will happily pay the reasonable bond for true preservation.

## CONCLUSION

Plaintiff's compelling evidence of irregularities (27,000 missing ballots, 96% undervote, nearly 369,754 manipulated ballots) and robust legal arguments under 52 U.S.C. §20701 and 42 U.S.C. §1983 decisively establish the need for a TRO. The SOS's authority to pause updates ensures preservation of election records, safeguarding voting rights and serving the public interest.

**PROOF OF SERVICE**

I, Andy Michael Thompson, certify that on August 13, 2025, I served a true and correct copy of the Reply to the Nevada Secretary of State's Opposition to Motion for Temporary Restraining Order and Expedited Hearing (with Exhibits 1-6) by certified mail, return receipt requested, addressed to the following party:

Gregory D. Ott, Chief Deputy Attorney General
Office of the Attorney General
100 N. Carson Street
Carson City, NV 89701

Dated: August 13, 2025

/s/ Andy Michael Thompson
Andy Michael Thompson
1157 Teal Point Drive
Henderson, NV 89074
weareheavenbound@yahoo.com
(702) 467-4374
Plaintiff, Pro Se

FILED RECEIVED
ENTERED SERVED ON
COUNSEL/PARTIES OF RECORD
AUG 13 2025
CLERK US DISTRICT COURT
DISTRICT OF NEVADA
BY: DEPUTY

Andy Michael Thompson
[redacted]

UNITED STATES DISTRICT COURT
DISTRICT OF NEVADA

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

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

# EXHIBITS 1-6


| | |
|---|---|
| Exhibit 1 – Order on Motions | Pages 1-6 |
| Exhibit 2 – Declaration for Voter Status | Pages 7-10 |
| Exhibit 3 – Ott Email | Page 11 |
| Exhibit 4 – Parikh Declaration | Pages 12-19 |
| Exhibit 5 – Gould Declaration | Pages 20-28 |
| Exhibit 6 – Mineral County Email | Page 29 |

# EXIBIT 1

ELECTRONICALLY SERVED
8/4/2025 3:50 PM

Electronically Filed
08/04/2025 3:50 PM
CLERK OF THE COURT

**ORDR**

**DISTRICT COURT**
**CLARK COUNTY, NEVADA**
* * * *

ANDY THOMPSON,
Plaintiff,

vs.

NEVADA SECRETARY OF STATE,
Defendant.

CASE NO.: A-24-906377-C
DEPARTMENT 29

**ORDER ON MOTIONS FOR RECONSIDERATION OF JUNE 18, 2025 ORDER AND FOR PRESERVATION OF JUDICIAL ECONOMY, EMERGENCY MOTION FOR STAY OF ELECTION MACHINE OVERWRITE, EMERGENCY MOTION TO EXPEDITE RULINGS ON PENDING MOTIONS**

This Court's Order on June 18, 2025, entered on June 19, 2025, details much of the history in this case. The Court incorporates that history here by reference but reiterates one point:

On March 25, 2025, Plaintiff filed a Motion for Temporary Restraining Order and a Motion to Reconsider the Motion to Preserve Evidence. In that Motion Plaintiff threatened the court with a personal lawsuit if THE COURT caused further delays or THE COURT continued to disregard legal duties:

JACOB A. REYNOLDS
DISTRICRT JUDGE
Department 29
Las Vegas, NV 89155

> Accordingly, this motion serves not only to request reconsideration, but also to **put the Court on notice** that further delays or disregard for clearly established legal duties may form the basis of a civil rights claim under **42 U.S.C. § 1983**. Judges do **not enjoy immunity** when acting in **clear absence of jurisdiction**, or where they **knowingly deprive constitutional rights**.

(Mot. at 3-4.) Notably, those bolded statements were bolded in **Plaintiff's** original filing. They are not added emphasis by the Court. Plaintiff's meaning was clear *inter alia* Plaintiff was blaming the Court for the delays in resolving this issue.

At the Hearing in May, the Court addressed this with the *pro se* Plaintiff. Plaintiff profusely apologized and said no threat was meant. Despite the plain words, the Court did not issue any sanctions at that time.

In the current filings before the Court Plaintiff directly, and unambiguously accuses the Court of "Judicial Complicity" stating that "The facts of this case **do not merely suggest** strategic mooting-they prove it." (Pl's Em. Mot. for Stay at 2 ¶ 6) (bold emphasis **in original**). Once again, the bolded emphasis is in Plaintiff's filing, not added emphasis by the Court.

So even though all prior continuances were based on Plaintiff's failed filings and requests for additional time and extensions, now the Court is being expressly blamed for being "complicit" in some type of strategic delay.

Plaintiff has now also openly threatened the Court with a lawsuit and punitive measures unless he gets his way:

> 15. Plaintiff will immediately pursue appropriate referrals to:
> • The Nevada Commission on Judicial Discipline,
> • The U.S. Department of Justice Office of Inspector General, and
> • The Office of Professional Responsibility,
> …should this Court continue to suppress federal statutory obligations.

(*Id.* at ¶ 15.)

JACOB A. REYNOLDS
DISTRICRT JUDGE
Department 29
Las Vegas, NV 89155

The Court has not alleviated Defendant from any federal statutory requirements. Plaintiff does ask for leniency though based on his *pro se* status. (Pl's Mot. for Recon. ¶¶ 5-9.) Plaintiff suggests his treatment in the prior Order was retribution for his poor wording, threats and so forth. Plaintiff further suggests his case should be allowed to proceed, essentially, because his is *pro se*. (*Id.*) But *pro se* status cannot become a sword to charge through an action and defeat all defenses. That is instead the required role of merit, logic, and reason – not one's status. Plaintiff chooses to proceed *pro se* as is his right, but it is not Defendant's duty, nor is it the Court's duty, to fall upon Plaintiff's sword.

Perhaps the basis of Plaintiff's assumed lack of knowledge of his prior threat is now explained when it is shown that there is no basis for his citation to *State v. Nye County*, 129 Nev. 521 (2013) in the subsequent paragraphs. (Pl's Em. Mot. for Stay at 2 at ¶ 9.) There is no such case, and the case at that citation does not discuss anything supporting the claimed citation. In short, this appears another unfortunate attempt in which the Court has to deal with a party using AI to draft pleadings. In prior cases, this Court has awarded $5,000.00 as a sanction against parties using AI that create non-existent cases which are then submitted to Court under NRCP 11. Plaintiff is bound by NRCP 11 in all of his filings with the Court.

The Court will not condone false filings. Personal attacks on the Court are simply unpersuasive. The Court is unaware of Plaintiff's practice in life, whether Plaintiff finds personal attacks, insinuations, and threats successful in his day-to-day living, but attempting to bully or intimidate the Court is not persuasive – not motivating – and certainly not appropriate.

**DECISION**

Pursuant to EDCR 2.23 the Court finds that it is proper to issue a ruling on this matter at Plaintiff's request and therefore an order is issued without oral argument.

JACOB A. REYNOLDS
DISTRICRT JUDGE
Department 29
Las Vegas, NV 89155

The COURT orders that all aspects of all pending motions are hereby DENIED.

Plaintiff has raised nothing to persuade the Court that any of its orders were in error. Plaintiff has not cited to any statute or case (meaning an actual existing case) that would thwart the reasoning in its prior order. Plaintiff has presented nothing that shows he should be allowed complete and unfettered access to the information he seeks. Plaintiff has not presented any evidence or suggested that he would be able to post a bond sufficient to justify a stay of the Secretary of State's actions to the level he believes he is entitled.

Inasmuch as Plaintiff seeks reconsideration for purposes of judicial economy this argument is misplaced. Now the most economic use of Plaintiff's time for a resolution of this matter is with an appeal to evaluate Plaintiff's argument and to decide if this Court is wrong. This Court made its decision based upon the Nevada Supreme Court's decisions and the legislated statutes of the State of Nevada. Judicial economy now favors taking this matter on appeal so that if this Court is wrong, or those cases are wrong, or the statues are unconstitutional—all of which Plaintiff suggests is the case—then the Supreme Court is the one to say so.

ALL PENDING MOTIONS are therefore DENIED.

The Hearing scheduled for August 7, 2025, is VACATED.

**Dated this 4th day of August, 2025**

Jacob A. Reynolds

DISTRICT JUDGE

**51E C73 1288 264C**
**Jacob A. Reynolds**
**District Court Judge**

JACOB A. REYNOLDS
DISTRICRT JUDGE
Department 29
Las Vegas, NV 89155

**CERTIFICATE OF SERVICE**

I hereby certify that on or about the date signed, a copy of this Order was electronically served to all registered parties in the Eighth Judicial District Court Electronic Filing Program per the attached Service Contacts list and/or placed in the attorney's folder maintained by the Clerk of the Court and/or transmitted via facsimile and/or mailed, postage prepaid, by United States mail to the proper parties as follows:

ANDY THOMPSON
[redacted]

LAENA ST. JULES, ESQ
Senior Deputy Attorney General
Office of the Attorney General
100 North Carson Street
Carson City, NV 89701
Nevada Bar No. 15156
Telephone: (775)684-1265
Facsimile: (775) 684-1108
Email: lstjules@ag.nv.gov

/s/ Melissa Delgado-Murphy

Melissa Delgado-Murphy
Judicial Executive Assistant

CSERV

DISTRICT COURT
CLARK COUNTY, NEVADA

| | |
|---|---|
| Andy Thompson, Plaintiff(s)<br><br>vs.<br><br>Nevada Secretary Of State, Defendant(s) | CASE NO: A-24-906377-C<br><br>DEPT. NO. Department 29 |

**AUTOMATED CERTIFICATE OF SERVICE**

This automated certificate of service was generated by the Eighth Judicial District Court. The foregoing Order was served via the court's electronic eFile system to all recipients registered for e-Service on the above entitled case as listed below:

Service Date: 8/4/2025

| | |
|---|---|
| Gregory Ott | gott@ag.nv.gov |
| andy thompson | weareheavenbound@yahoo.com |
| Laena St-Jules | lstjules@ag.nv.gov |

# EXIBIT 2

Andy Michael Thompson
[redacted]

UNITED STATES DISTRICT COURT

DISTRICT OF NEVADA

| | | |
|---|---|---|
| **Andy Michael Thompson,** *Plaintiff,* v. **Nevada Secretary of State,** *Defendant.* | ) | Case No. 2:25-cv-01284-CDS-EJY |

**DECLARATION OF ANDY MICHAEL THOMPSON AFFRIMING HIS STATUS AS A REGISTERED VOTER WHO VOTED IN THE 2024 GENERAL ELECTION IN THE STATE OF NEVADA**

I, Andy Michael Thompson, declare under penalty of perjury:

1. I am an active registered voter in the State of Nevada.

2. I voted in person in the 2024 General Election

I declare under penalty of perjury under the laws of the United States that the foregoing is true and correct.

Dated: August 12, 2025
/s/ Andy Michael Thompson
Andy Michael Thompson
[redacted]
Plaintiff, Pro Se

UNITED STATES DISTRICT COURT

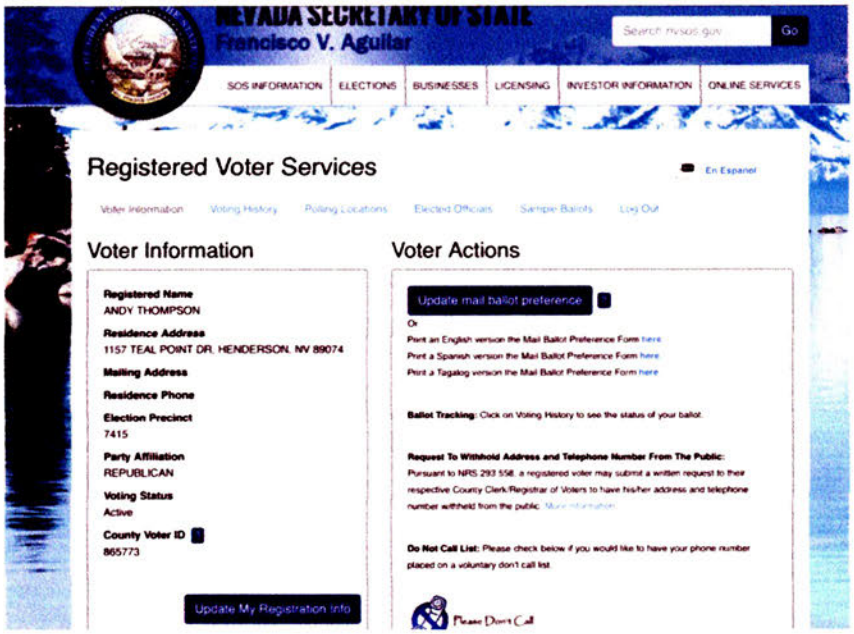
DISTRICT OF NEVADA

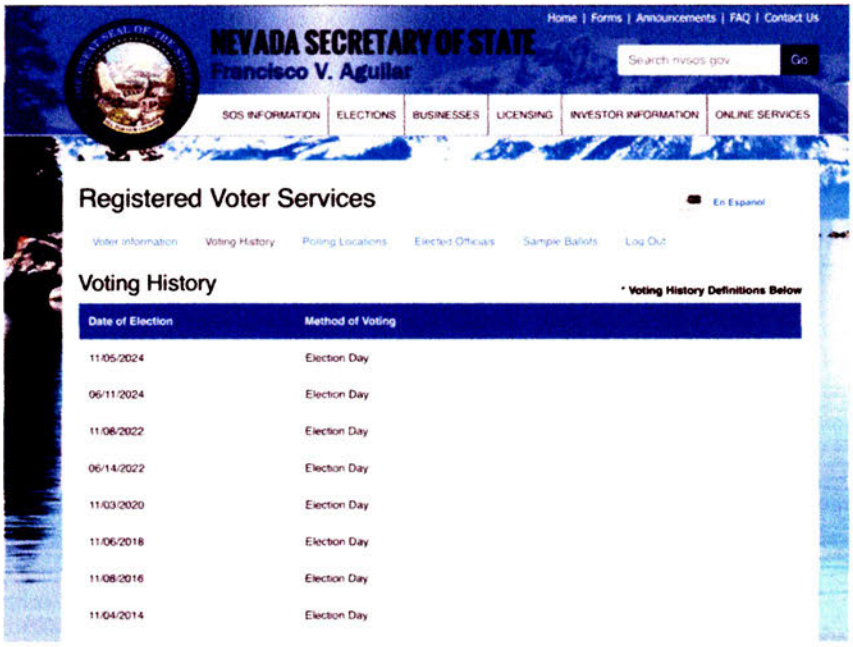
| | | |
|---|---|---|
| **Andy Michael Thompson**,<br>*Plaintiff*,<br>v.<br>**Nevada Secretary of State**,<br>*Defendant*. | ) | Case No. 2:25-cv-01284-CDS-EJY |

EXHIBIT A

Screenshots taken August 12, 2025

Attached to Declaration of Andy Michael Thompson


NEVADA SECRETARY OF STATE
Francisco V. Aguilar
Search nvsos.gov
Go
SOS INFORMATION
ELECTIONS
BUSINESSES
LICENSING
INVESTOR INFORMATION
ONLINE SERVICES
Registered Voter Services
En Espanol
Voter Information
Voting History
Polling Locations
Elected Officials
Sample Ballots
Log Out
Voter Information
Registered Name
ANDY THOMPSON
Residence Address
1157 TEAL POINT DR, HENDERSON, NV 89074
Mailing Address
Residence Phone
Election Precinct
7415
Party Affiliation
REPUBLICAN
Voting Status
Active
County Voter ID
865773
Update My Registration Info
Voter Actions
Update mail ballot preference
Or
Print an English version the Mail Ballot Preference Form here
Print a Spanish version the Mail Ballot Preference Form here
Print a Tagalog version the Mail Ballot Preference Form here
Ballot Tracking: Click on Voting History to see the status of your ballot.
Request To Withhold Address and Telephone Number From The Public:
Pursuant to NRS 293.558, a registered voter may submit a written request to their respective County Clerk/Registrar of Voters to have his/her address and telephone number withheld from the public. More information
Do Not Call List: Please check below if you would like to have your phone number placed on a voluntary don't call list.
Please Don't Call


Home | Forms | Announcements | FAQ | Contact Us
NEVADA SECRETARY OF STATE
Francisco V. Aguilar
Search nvsos.gov
Go
SOS INFORMATION
ELECTIONS
BUSINESSES
LICENSING
INVESTOR INFORMATION
ONLINE SERVICES
Registered Voter Services
En Espanol
Voter Information
Voting History
Polling Locations
Elected Officials
Sample Ballots
Log Out
Voting History
* Voting History Definitions Below
Date of Election
Method of Voting
11/05/2024
Election Day
06/11/2024
Election Day
11/08/2022
Election Day
06/14/2022
Election Day
11/03/2020
Election Day
11/06/2018
Election Day
11/08/2016
Election Day
11/04/2014
Election Day

# EXHIBIT 3

# Thompson v. Secretary of State

- Greg D. Ott

To: me · Thu, Jul 10 at 5:35 PM

## Message Body

Good Evening Mr. Thompson,
As you may know, I've taken primary responsibility of this case back from Ms. St. Jules. As the need to continue elections work is continuing throughout the state, the Secretary has received multiple requests from County officials seeking to install the 5.20 update on mechanical voting systems pursuant to NRS 293B.1045(6). As there is no stay preventing the Secretary from completing his NRS 293B.1045 duties, the Secretary is compelled by statute to consider such requests in good faith.

This email will confirm that on July 18, the Secretary of State will notify the vendor and 15 county election officials (who use Dominion Voting System machines) 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.

If you have questions about your own rights in this action, please reach out to a lawyer of your choosing, but if you would like to discuss the case with me on behalf of the Secretary of State, feel free to reach out to me with questions.
Best regards, Greg

**Gregory D. Ott**
Chief Deputy Attorney General
Government and Natural Resources Division
Office of the Attorney General
100 N. Carson Street
Carson City, NV 89701
Phone: (775) 684-1229
Fax: (775) 684-1108
gott@ag.nv.gov

**This e-mail and any attachments are confidential and protected by legal privilege. If you are not the intended recipient, be aware that any disclosure, copying, distribution or use of the email or any attachments is prohibited. If you have received this e-mail in error, please notify the sender immediately by replying to the sender and deleting this copy and the reply from your system. Thank you.**

# EXHIBIT 4

**Declaration of Clay U. Parikh**

I, CLAY U. PARIKH, declare under penalty of perjury that the following is true and correct:

1. I have personal knowledge of the matters set forth below and would testify competently to them if called upon to do so.

2. I have a Master of Science in Cyber Security, Computer Science from the University of Alabama in Huntsville. I have a Bachelor of Science in Computer Science, Systems Major from the University of North Carolina at Wilmington. In February 2007 I obtained the Certified Information Systems Security Professional (CISSP) certification and continually maintained good standing, until I released it on 28 February 2024. I also held the following certifications: Certified Ethical Hacker (CEH) and Certified Hacking Forensic Investigator (CHFI).

3. Since December of 2003, I have continually worked in the areas of Information Assurance (IA), Information Security and Cyber Security. I have performed and led teams in Vulnerability Management, Security Test and Evaluation (ST&E) and system accreditation. I have supported both civil and Department of Defense agencies within the U.S. government as well as international customers, such as NATO. I have served as the Information Security Manager for enterprise operations at Marshall Space Flight Center, where I ensured all NASA programs and projects aboard the center met NASA enterprise security standards. I was also responsible in part for ensuring the Marshall Space Flight Center maintained its Authority to Operate (ATO) within the NASA agency. I have also served as the Deputy Cyber Manager for the Army Corps of Engineers where I led and managed several teams directly in: Vulnerability Management, Assessment and Authorization (A&A), Vulnerability Scanning, Host Based Security System (HBSS), Ports Protocols and Service Management, and an Information System Security Manager (ISSM) team for cloud projects. I also have performed numerous internal digital forensic audits. During this time span, I also worked at the Army Threat Systems Management Office

(TSMO) as a member of the Threat Computer Network Operations Team (TCNOT). I provided key Computer Network Operations (CNO) support by performing validated threat CNO penetration testing and systems security analysis. TCNOT is the highest level of implementation of the CNO Team concept.

4. From 2008 to 2017, I also worked through a professional staffing company for several testing laboratories that tested electronic voting machines. These laboratories included Wyle Laboratories, which later turned into National Technical Systems (NTS) and Pro V&V. My duties were to perform security tests on vendor voting systems for the certification of those systems by either the Election Assistance Commission (EAC), or to a state's specific Secretary of State's requirements.

5. In addition to testing the voting systems, I have conducted analysis of system logs from several different electronic voting systems in preparation for various court cases. I have reviewed the Amended Statement of Contest (Case No.: A-24-906377-C), the Nevada Secretary of State's Opposition to Plaintiff's Request, and sections of Nevada Revised Statutes pertaining to elections.

6. The focus of this document is centered on system and application logs, and their requirements per the Voluntary Voting System Guidelines (VVSG). How the log settings should be configured, industry best practice, and preservation of said logs.

## EXECUTIVE SUMMARY

7. There is a ***serious*** auditing and security issue, in relation to system event and security logging with Dominion and ES&S voting systems. Election data is not being properly recorded and maintained per retention requirements. Application, Security, and System event log configurations are not setup appropriately to capture the required events and information set forth in the VVSG for the required timeframe of an election.

8. Nevada law requires testing to Federal Standards and by a Federally accredited laboratory.[1] All Nevada voting systems are currently certified to VVSG 1.0 (2005).[2] The

[1] NV Rev Stat § 293B.063 and NAC 293B.110 (2017)
[2] https://www.nvsos.gov/sos/elections/election-resources/voting-system

preservation of election records is required by both the Help America Vote Act (HAVA) and the VVSG. Section 2.1.10 "Data Retention" of VVSG 1.0 Vol. 1[3] states "Therefore, all voting systems shall provide for maintaining the integrity of voting and audit data during an election and for a period of at least 22 months thereafter." The section further defines logs as part of the election data to be preserved. "Regardless of system type, all audit trail information spelled out in Subsection 5.5 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."

## DETAILED FINDINGS AND CONCLUSIONS

9. There are three basic log types that any information system, to include electronic voting systems, should record; System, Security and Application events. Industry standards and best practices exist that state what should be audited within these event types and the configuration settings for the logging mechanisms. In Volume 1 of the VVSG there are several sections that define what is to be logged. For example; section 4.1.3.1 "Recording Requirements" "g. Log corrected data errors by the voting system", section 5.4.3 "In-process Audit Records" "d. System generated log of all normal process activity and system events that require operator intervention, so that each operator access can be monitored and access sequence can be constructed".

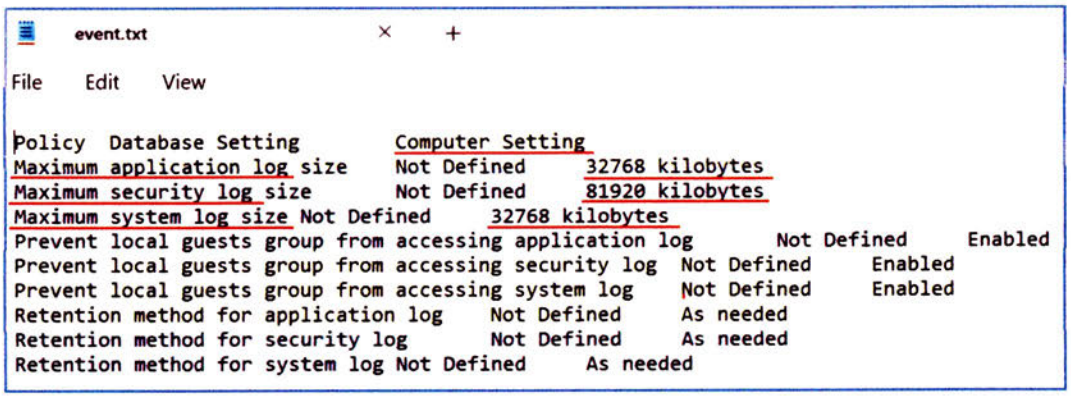
10. Most importantly, section 2.1.10 gives a general timeframe to help estimate the log file sizes needed in order to capture all the required data. Logs must be kept from the time logs of ballot definition formats, through system testing, election night and post-election processing. This means logs must record all the required activities from the date the election project is designed and created through the date when official election results are sent to the state from the county.

11. The Election Management System (EMS) is the heart of any electronic voting

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

system. Dominion and ES&S both use Microsoft Windows as the base Operating System (OS) for their EMS. Microsoft provides recommended maximum log sizes for their Operating Systems.[4] Department of Defense (DoD) systems, which are considered critical infrastructure, just like the voting systems, utilize Security Technical Implementation Guides (STIG) to configure their settings.[5]

12. During my time as a security tester at the VSTLs, I found that auditing was not appropriately implemented and that log file sizes were inadequate. Additionally, my current analysis of voting system logs still confirms these findings. The log files that I have analyzed are often overwritten, destroying required election data that is supposed to be preserved. **Figures 1** and **2** below are examples of my findings while in the VSTL, they are extracts[6] from configuration checks performed on Dominion and ES&S systems.

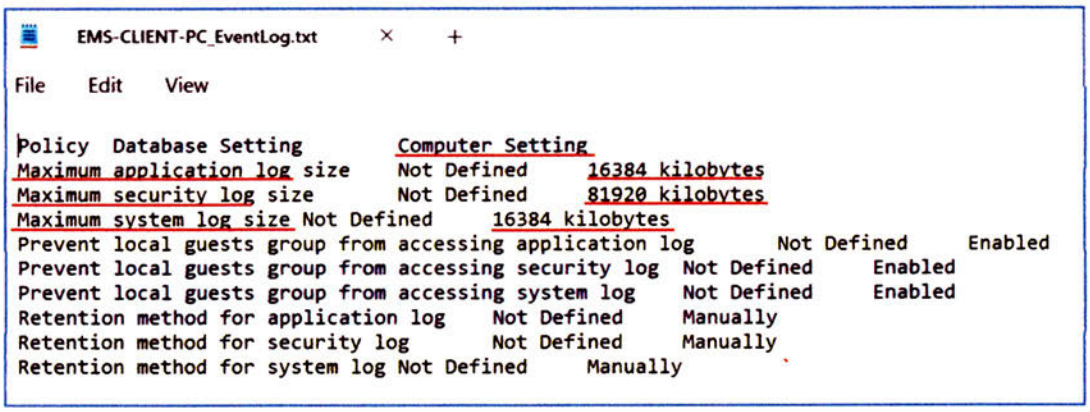

event.txt

File Edit View

| Policy | Database Setting | Computer Setting | |
|---|---|---|---|
| Maximum application log size | Not Defined | 32768 kilobytes | |
| Maximum security log size | Not Defined | 81920 kilobytes | |
| Maximum system log size | Not Defined | 32768 kilobytes | |
| Prevent local guests group from accessing application log | | Not Defined | Enabled |
| Prevent local guests group from accessing security log | | Not Defined | Enabled |
| Prevent local guests group from accessing system log | | Not Defined | Enabled |
| Retention method for application log | | Not Defined | As needed |
| Retention method for security log | | Not Defined | As needed |
| Retention method for system log | Not Defined | As needed | |

**Figure 1**. Dominion DVS 4.14 Event Log settings

[4] https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/dd349798(v=ws.10)
[5] https://public.cyber.mil/stigs/
[6] Screen captures of event log settings, underlined for emphasis.



EMS-CLIENT-PC_EventLog.txt

File Edit View

| Policy | Database Setting | Computer Setting |
|---|---|---|
| Maximum application log size | Not Defined | 16384 kilobytes |
| Maximum security log size | Not Defined | 81920 kilobytes |
| Maximum system log size | Not Defined | 16384 kilobytes |
| Prevent local guests group from accessing application log | Not Defined | Enabled |
| Prevent local guests group from accessing security log | Not Defined | Enabled |
| Prevent local guests group from accessing system log | Not Defined | Enabled |
| Retention method for application log | Not Defined | Manually |
| Retention method for security log | Not Defined | Manually |
| Retention method for system log | Not Defined | Manually |

**Figure 2**. ES&S EVS 5300 Event Log settings

13. The ES&S systems are nowhere close to an acceptable level. Dominion systems while slightly better, still **fail** to meet the basic requirements. Dominion sets their maximum log sizes, for Application and System logs, to the bare minimum of DoD requirements.[7] Dominion doesn't meet the Security log size requirements. **Figure 3** is a screen capture from DoD STIG requirements.[8]

| | | | |
|---|---|---|---|
| | | | provide a trail of evidence in case the system or network is compromised. The Application event log may... |
| V-220781 | Medium | The System event log size must be configured to 32768 KB or greater. | Inadequate log size will cause the log to fill up quickly. This may prevent audit events from being recorded properly and require frequent attention by administrative personnel. |
| V-220780 | Medium | The Security event log size must be configured to 1024000 KB or greater. | Inadequate log size will cause the log to fill up quickly. This may prevent audit events from being recorded properly and require frequent attention by administrative personnel. |
| V-220779 | Medium | The Application event log size must be configured to 32768 KB or greater. | Inadequate log size will cause the log to fill up quickly. This may prevent audit events from being recorded properly and require frequent attention by administrative personnel. |

**Figure 3**. Windows 10 DISA STIG requirements for log size

14. While at first glance it would seem like Dominion is doing a good job by meeting DoD STIG requirements. However, they are **not**. DoD sets a minimum log size, with the consideration of other security requirements. DoD system logs are backed up on a weekly

[7] https://stigviewer.com/stigs/microsoft_windows_10/2024-11-25/finding/V-220781
[8] https://stigviewer.com/stigs/microsoft_windows_10

basis, at a minimum. DoD follows an industry standard, the 3-2-1 backup strategy[9], when it comes to back up and storage. This strategy is pretty much used industry wide for retention and protecting vital data. Additionally, most agencies within DoD far surpass these minimum log size requirements.

15. The voting system vendors do not follow the 3-2-1 backup strategy. This for Dominion systems is a concern because their current log file settings may store four (4) to maybe seven (7) days of log data. This does not cover the required timeframe for a normal election period, as defined in section 2 of the VVSG. Without backups to retain previous log data, required election audit logs are simply overwritten, destroying the data.

16. Worsening this issue is that not all required auditing is enabled on the voting systems. Many of the systems do not have OS auditing enabled, which is required to log events.[10] [11] **Figure 4** and **5** below are examples from testing conducted in the VSTLs.

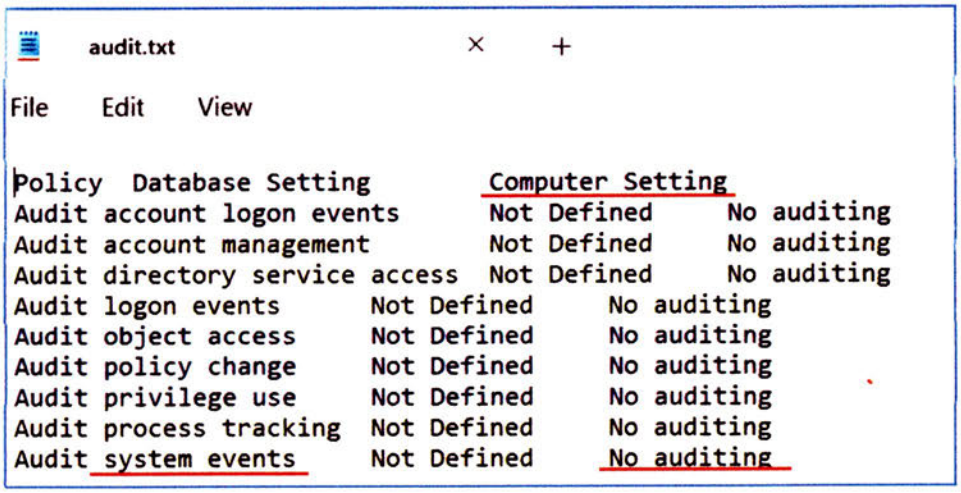



**Figure 4**. Dominion DVS 4.14 Audit settings

[9] https://www.techtarget.com/searchdatabackup/definition/3-2-1-Backup-Strategy
[10] https://learn.microsoft.com/en-us/defender-for-identity/deploy/configure-windows-event-collection
[11] https://learn.microsoft.com/en-us/windows-hardware/drivers/install/enabling-the-system-event-audit-log

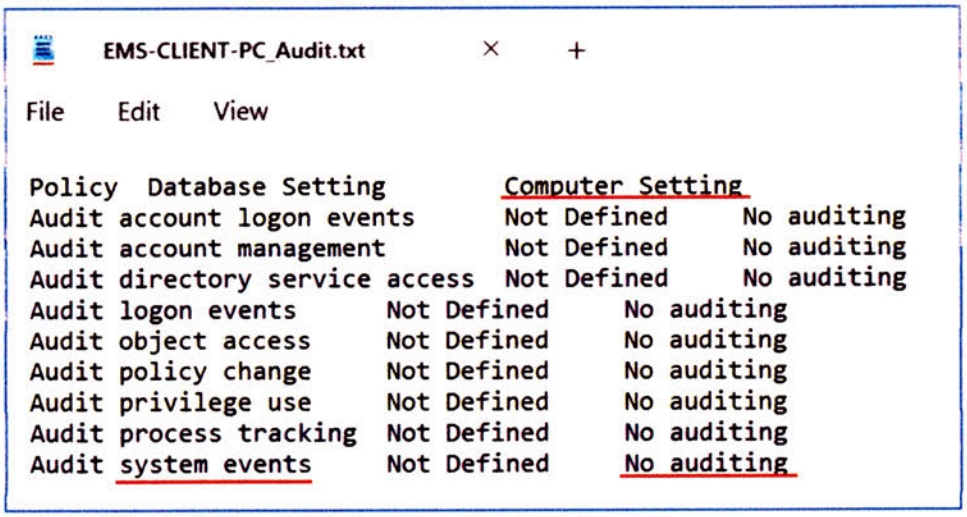



**Figure 5**. ES&S EVS 5300 Audit settings

17. In my current analysis of Dominion Voting Systems, I have found that protocols are enabled and not being audited. For example, I have observed IP version 6 is enabled on the voting system but, is not being audited. Therefore, no logs are created when this IP protocol is used. This is a major security concern. There are audit policy recommendations.[12] However, it is standard practice to audit any action, protocol, or service that is enabled and would be a security concern. All network protocols are a security concern.[13] So, running an unmonitored IP version is a violation of long-standing, **basic** cybersecurity best practices.

18. The protection and integrity of log files is vital to proper record keeping and auditability. User access and file restrictions should always be applied on any information system to protect their integrity. Also, when logs are backed up off of a system there should be hash files created to ensure they maintain file integrity. However, log files should always be made available for audits and analysis. This is their whole purpose.[14]

19. Lastly, log files do not contain any proprietary or classified information. They are not designed to do that. They are designed to record system, security and application

[12] https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/audit-policy-recommendations
[13] https://www.techtarget.com/searchnetworking/definition/protocol
[14] https://www.sumologic.com/glossary/log-file/

events that assist in troubleshooting, compliance and auditing, identify system issues or help identify malicious activity. For these reasons, audit and log configurations should be enabled and adjusted to meet system requirements. Most importantly they should be analyzed.

## CONCLUSION

20. Electronic voting systems overall are full of vulnerabilities with multiple exploits available. The vulnerabilities range from outdated Operating Systems (OS), third party applications, to protocols and services. Adding to these weaknesses is the system configuration. Nearly all aspects of the voting systems do not implement standard security, let alone meet industry best practices when configuring their systems. With Dominion Voting Systems, a malicious actor could manipulate one of the components or the entire system and go undetected, due to the lack of adequate logging.

21. The Secretary of State's opposition to plaintiff's motion[15] about having no ability to obtain access, is flawed. Audit logs do not need the voting system's programs to be analyzed. Also, the statement made about what public interest favors[16], seems to fall short. I would image that public interest would be to ensure confidence, integrity and an accurate election. Ensure that the voting systems stay compliant. The county clerks should be backing up data before implementing any updates. So, updates can occur. However, to stay compliant, section 2 of the VVSG vol. 1 concerning logging must be followed. Additionally, adjusting audit and log size configurations can easily be adjusted while the clerks are doing these "updates". Lastly, audit log information can be and should be backed up and made available for analysis.

I declare under penalty of perjury that the foregoing is true and correct.

Executed on this 17 day of April 2025.

Clay U. Parikh

[15] OPPS Case No. A-24-906377-C Page 2. Lines 19-21
[16] OPPS Case No. A-24-906377-C Page 2. Lines 24-26

# EXHIBIT 5

**EXHIBIT 1**

**DECLARATION**

DATE FILED: August 19, 2022 10:27 AM
FILING ID: 80825D18A248F
CASE NUMBER: 2022CV30529

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.

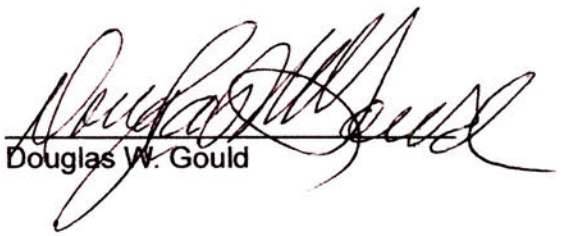
Fourth, if the system must be adjusted or reconfigured, this is accomplished by copying a new certified image provided by the vendor onto the hard drive, destroying the data thereon. This would destroy records relating to the 2022 primary election, violating record retention statutes.

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

# EXHIBIT 6

# Recall

- Teresa McNally

To: me · Thu, Aug 7 at 4:05 PM

## Message Body

Good Afternoon,

I have a recall that is the works for a Commissioner here in Mineral County. All NRS and State of Nevada Recall Guide has been followed for this recall. They have turned in the 45 day count which is very much below the Count needed. I have had one person give me a letter for name to be removed from the petition. To do a recall in Mineral County this will cost the County approximately $35,000 with 3 sites for voting and 26 people working the special election and doing the counts. This includes all requirements for a special election, including mail ballots to 3,000 people.

Have a Wonderful Day

Teresa McNally
Mineral County Clerk-Treasurer
775-945-2446
Clerk-treasurer@mineralcountynv.org

*Mineral County is an Equal Opportunity Provider and Employer.*
*If you wish to file a Civil Rights program complaint of discrimination, complete the USDA Program Discrimination Complaint Form, found online at http://www.ascr.usda.gov/complaint filing cust. html, or at any USDA office, or call (866)632-9992 to request the form. You may also write a letter containing all of the information requested in the form. Send your completed complaint form or letter to us by mail at U.S. Department of Agriculture, Director, Office of Adjudication, 1400 Independence Avenue, S.W., Washington, D.C. 20250-9410, by fax (202)690-7442 or email at program.intake@usda.gov.*
**Please note: Effective October 10, 2016 our new office hours will be: Monday - Thursday 7am to 5pm.**