

WARNING

It is a felony for anyone to sign a petition for the convening of a grand jury with any name other than his own, or knowingly to sign his name more than once for the convening of the grand jury, or to sign such petition when he is not a legal voter of the county.

**IN THE DISTRICT COURT OF TULSA COUNTY
STATE OF OKLAHOMA**

IN RE: PETITION OF QUALIFIED ELECTORS OF TULSA COUNTY FOR THE
IMPANELING OF A GRAND JURY

Case No. _____

PETITION FOR IMPANELING A GRAND JURY

The undersigned qualified electors of Tulsa County, Oklahoma petition for the impaneling of a grand jury under Section 18 of Article II of the Oklahoma Constitution and 38 O.S. secs. 101 through 108. A copy of this petition is filed with the Tulsa County Court Clerk before the obtaining of any signatures, as 38 O.S. sec. 101 requires.

Person filing this petition

Name: _____

Mailing address for court notices: _____

I. SUBJECT MATTER

The transmission of Social Security Administration data through a third-party server not approved to hold that data and outside the agency's security protocols; the copy of the agency's Numident file that a whistleblower disclosure describes in a cloud environment lacking independent security controls; whether records containing personal identifying information of Tulsa County residents were among the data transmitted or copied; and any disclosure or attempted disclosure of Social Security Administration records to a private political advocacy group.

II. AREAS TO BE INQUIRED INTO

1. The transmission of Social Security Administration data through the third-party service Cloudflare between March 7, 2025 and March 17, 2025, and whether records of Tulsa County residents were among the data transmitted.
2. The identity of each person who transmitted, requested, approved, or supervised that transmission.

3. The present location of that data, who has had access to it, and whether it still exists on any third-party system.
4. The copy of the Numident that the whistleblower disclosure of August 26, 2025 describes in a cloud environment lacking independent security controls, and each person who requested, approved, created, or had access to that environment.
5. The security and audit controls applied to that copy of the Numident, and any record of access to that copy.
6. The Voter Data Agreement signed in March 2025 by a member of the Social Security Administration's DOGE Team in his capacity as an agency employee, and the identity of the private advocacy group party to that agreement.
7. Whether any Social Security Administration data was matched against, or disclosed for matching against, any state voter roll.
8. The scope of authorization actually granted within the Social Security Administration for each transmission, copy, disclosure or use of data at issue, and whether any of them exceeded that authorization.
9. Each person's role in the acts described, for the purpose of applying 21 O.S. secs. 1953 and 1958.

III. GENERAL ALLEGATIONS

Each allegation identifies the record it comes from.

1. The Numerical Identification System, known as Numident, is the Social Security Administration's master file of information submitted in applications for Social Security cards. It contains names, Social Security numbers, dates and places of birth, and parents' names for more than 300 million people. (Social Security Bulletin, Vol. 69, No. 1 (2009); Social Security Administration History FAQ.)
2. Tulsa County, Oklahoma had 669,279 residents at the 2020 census. (United States Census Bureau.)
3. On January 16, 2026, the United States Department of Justice filed a Notice of Corrections to the Record, ECF No. 197, in American Federation of State, County and Municipal Employees, AFL-CIO v. Social Security Administration, No. 1:25-cv-00596-ELH (D. Md.), correcting

statements Social Security Administration officials had previously made to that court. (Federal court filing.)

4. That filing states that beginning March 7, 2025 and continuing until March 17, 2025, members of the Social Security Administration's DOGE Team were using links to share data through the third-party server Cloudflare; that Cloudflare is not approved for storing Social Security Administration data; and that its use in that manner is outside the agency's security protocols. (ECF No. 197.)

5. That filing states that, because Cloudflare is a third-party entity, the agency "has not been able to determine exactly what data were shared to Cloudflare or whether the data still exist on the server." (ECF No. 197, § VI.)

6. The same filing states that in March 2025 "a political advocacy group contacted two members of SSA's DOGE Team with a request to analyze state voter rolls that the advocacy group had acquired," that "[t]he advocacy group's stated aim was to find evidence of voter fraud and to overturn election results in certain States," and that "one of the DOGE team members signed a 'Voter Data Agreement,' in his capacity as an SSA employee, with the advocacy group," sending the executed agreement to the group on March 24, 2025. It further states: "Email communications reviewed by SSA suggest that DOGE Team members could have been asked to assist the advocacy group by accessing SSA data to match to the voter rolls, but SSA has not yet seen evidence that SSA data were shared with the advocacy group." That review was the agency's own. A grand jury can compel the communications and records the agency reviewed. (ECF No. 197, § V and n.1.)

7. That filing also states that in late December 2025 the agency made two Hatch Act referrals to the U.S. Office of Special Counsel related to the activities described in paragraph 6. (ECF No. 197, § V.)

8. On April 10, 2026, in the en banc appeal in that case, the opinion of Judge Heytens of the United States Court of Appeals for the Fourth Circuit, joined on this point by Chief Judge Diaz and Judge Harris, described that filing this way: "In that notice, the government admits: (1) that it provided inaccurate information to the district court and may not have fully complied with its temporary restraining order; (2) that DOGE used an unauthorized third-party server to share SSA data; and (3) that DOGE team members may have agreed to share SSA data with a political

advocacy group that aims to 'find evidence of voter fraud and to overturn election results in certain States.'" (No. 25-1411, slip op. at 15-16 n.8 (opinion of Heytens, J.)). The federal district court quoted that description in its memorandum opinion of June 26, 2026. On April 14, 2026, the district court granted the plaintiffs' motion for discovery into the matters the Notice of Corrections disclosed (ECF No. 212). On June 26, 2026, it denied the government's motion to rescind that order and wrote that in the Notice of Corrections "defendants disclosed that several sworn declarations previously submitted to the Court were inaccurate." (Mem. Op., June 26, 2026.)

9. On March 10, 2026, the plaintiffs in that litigation filed a Notice of Factual Development informing the court of reported allegations that a former DOGE-affiliated individual may have removed sensitive Social Security data, including records affecting hundreds of millions of people, intending to use it in later work at a private-sector employer. (ECF No. 208, plaintiffs' notice of reported allegations.)

10. In the same Maryland litigation, the district court entered a preliminary injunction on April 17, 2025, ECF No. 147, limiting DOGE access to Social Security Administration records. On June 6, 2025 the Supreme Court of the United States stayed that injunction in No. 24A1063, in an unsigned order. Justice Kagan would have denied the application, and Justice Jackson, joined by Justice Sotomayor, dissented. On April 10, 2026 the Court of Appeals for the Fourth Circuit vacated the injunction and remanded. (Federal court record.)

11. On August 26, 2025, Charles Borges, then the Chief Data Officer of the Social Security Administration, submitted a whistleblower disclosure to the United States Office of Special Counsel and to four committees of Congress. The disclosure states that on June 10, 2025 a request was made to create "a cloud environment to which SSA's Numerical Identification System or 'NUMIDENT' data could be transferred," and it describes the "DOGE specific, self-administered cloud environment lacking independent security controls and hosting a copy of NUMIDENT." The disclosure further states that "no verified audit or oversight mechanisms existed over the DOGE cloud environment set up outside of DIS control." The Numident contains one record for each Social Security number ever assigned, so a copy of it contains the records of every resident of Tulsa County who has been issued a Social Security number. (Disclosure of Charles Borges, Aug. 26, 2025; Social Security Administration Office of the Inspector General, Audit Report A-06-16-50069.)

12. The petitioners do not allege that any person has been convicted of or charged with a crime. The petitioners allege that the United States has told a federal court that Social Security Administration data was shared through a server not approved to hold it and outside agency security protocols, and that the agency has not been able to determine exactly what data were shared or whether the data still exist on that server. Tulsa County residents' records cannot be excluded from that data, because the agency "has not been able to determine exactly what data were shared to Cloudflare." (ECF No. 197, § VI.)

13. On information and belief, based on the facts set out above, the records of Tulsa County residents were among the Social Security Administration data shared through a third-party server the agency had not approved, or copied into a cloud environment lacking independent security controls. The agency holds a record for every resident who has been issued a Social Security number, and it has told a federal court that it "has not been able to determine exactly what data were shared to Cloudflare." Whether residents' records were copied, shared, matched or retained, and by whom, is what this petition asks a grand jury of Tulsa County to determine.

IV. OKLAHOMA STATUTES IMPLICATED

21 O.S. sec. 1953(A)(1): willfully and without authorization gaining access to and copying, making use of, disclosing, or taking possession of a computer, computer system, computer network, data, or other property. A felony under 21 O.S. secs. 1953(B) and 1955(A).

21 O.S. sec. 1953(A)(3): willfully exceeding the limits of authorization and copying, disclosing, or taking possession of data. A felony under 21 O.S. secs. 1953(B) and 1955(A).

21 O.S. sec. 1953(A)(7): willfully and without authorization providing or assisting in providing a means of accessing a computer, computer system, or computer network in violation of that section. A felony under 21 O.S. secs. 1953(B) and 1955(A).

21 O.S. sec. 1958: communicating with, storing data in, or retrieving data from a computer system or network for the purpose of using that access to violate any provision of the Oklahoma Statutes. A felony.

V. VENUE

The petitioners rely on 22 O.S. sec. 124, which provides: "When a public offense is committed, partly in one county and partly in another county, or the acts or effects thereof, constituting or requisite to the offense, occur in two or more counties, the jurisdiction is in either county." The

Oklahoma Court of Criminal Appeals applied the same "acts or effects" language, then codified at Okla. Stat. 1931 sec. 2730, in *Bozarth v. State*, 1934 OK CR 130. The court upheld venue in the county where a false salary claim mailed from another county was received. In *Strassheim v. Daily*, 221 U.S. 280, 285 (1911), the Supreme Court of the United States wrote: "Acts done outside a jurisdiction, but intended to produce and producing detrimental effects within it, justify a state in punishing the cause of the harm as if he had been present at the effect" The petitioners allege on information and belief that records of Tulsa County residents were among the data described in Section III, and that the effects of any unauthorized copying or disclosure of those records occur in Tulsa County, where those residents live. The petitioners also ask the grand jury to inquire whether any person caused the access of a computer, computer system or computer network from or to Tulsa County. Under 21 O.S. sec. 1957, such a person is deemed to have personally accessed it in each jurisdiction.

VI. LIMITS OF THIS PETITION

This petition alleges no federal offense. It seeks the removal of no Oklahoma public official. It names no person as a defendant. It asks a Tulsa County grand jury to inquire into conduct affecting Tulsa County residents under Oklahoma law.

VII. PRAYER

The undersigned qualified electors of Tulsa County ask that this Court find, under 38 O.S. sec. 102, that the face of this petition states a reasonably specific identification of areas to be inquired into and sufficient general allegations to warrant a finding that such inquiry may lead to information which, if true, would warrant a true bill of indictment; and that upon certification of sufficient signatures by the Tulsa County Election Board, the presiding district judge order the impaneling of a grand jury under 38 O.S. sec. 107, to convene within thirty days of the date the Court Clerk receives that certification, subject to 22 O.S. sec. 345. The undersigned also ask that the order entered under 38 O.S. sec. 102 approve, as to form and content, the signature sheet attached to this petition as the signature form.

Respectfully submitted,

Signature: _____

Date: _____

WARNING

It is a felony for anyone to sign a petition for the convening of a grand jury with any name other than his own, or knowingly to sign his name more than once for the convening of the grand jury, or to sign such petition when he is not a legal voter of the county.

IN THE DISTRICT COURT OF TULSA COUNTY, STATE OF OKLAHOMA

PETITION FOR IMPANELING A GRAND JURY: SIGNATURE SHEET

This sheet is stapled behind the petition approved by order of the Presiding Judge of the District Court of Tulsa County in Case No. _____, entered on _____. The signers below sign that petition. Do not separate this sheet from the petition.

Each signer must be a registered voter of Tulsa County. Print clearly. This sheet is filed with the Tulsa County Court Clerk and becomes part of the court file, which is open to the public unless the court orders it sealed.

#	Signature	Printed name	Residence address	City	Date
1					
2					
3					
4					
5					
6					
7					
8					
9					
10					
11					
12					
13					
14					
15					
16					
17					
18					

CIRCULATOR VERIFICATION: I personally circulated this sheet. I witnessed each signature. To the best of my knowledge each signer is a registered voter of Tulsa County.

Circulator name: _____ Signature: _____
Address: _____ Date: _____

RULES FOR CIRCULATORS: No signature may be collected before the presiding district judge signs the order approving the petition. All signatures must be collected within 45 days of that order. In every packet, this sheet is stapled behind the approved petition. Packets stay stapled while signatures are gathered and when they are filed with the Tulsa County Court Clerk.

Sheet _____ of _____ Person filing: Name _____