



***Via Electronic Mail***

December 19, 2025

Harmeet K. Dhillon  
Assistant Attorney General  
Civil Rights Division  
U.S. Department of Justice  
950 Pennsylvania Ave., NW 4CON  
Washington, D.C. 20530

Re: DOJ Request

Dear Assistant Attorney General Dhillon,

As Ohio's chief election officer, I am grateful for the opportunity to partner with the federal government in protecting the integrity of our elections. Under the current administration, the Department of Justice has shown a refreshing and welcome commitment to enforcing federal laws designed to prevent illegal voting. For that reason, and pursuant to your requests under federal law, I have instructed my staff to begin the process of providing to the DOJ Ohio's statewide voter file, which we will transfer through the DOJ's secure file-sharing system.

My office fought efforts by the previous administration to block this meaningful partnership, attempting to deny our lawful access to the federal records and systems necessary for the verification of citizenship status and other vital information. On behalf of the state of Ohio, I filed litigation against the Biden administration to establish a voter verification protocol through the Department of Homeland Security's Systematic Alien Verification and Entitlements (SAVE) System. That lawsuit recently resulted in a settlement guaranteeing that Ohio will have access to federal SAVE data for the next 20 years.

My office also partnered this year with personnel at the United States Citizenship and Immigration Services (USCIS) to pioneer SAVE's state-specific search and voter verification capabilities. In a letter dated October 8, 2025, President Trump acknowledged Ohio's leadership in this effort, stating, "You were one of the first leaders to step up and protect the integrity of our elections by using the SAVE system—and I

commend you for your decisive action.” At this moment, we are actively working with USCIS to verify thousands of voter records. As that work continues, I can confidently say that Ohio has the most accurate and accountable statewide voter file in our state’s history, and we look forward to obtaining even more federal resources through the Department of Justice to help us build on that progress.

To that end, the Department of Justice has stated its intent, through written correspondence on August 6, 2025, and August 14, 2025, to assess our state’s compliance with federal law and assist Ohio with the verification of our statewide voter file. I intend to fulfill this request within the requirements of state and federal law.

As you know, the Department’s August 6 letter specifically requests an electronic copy of Ohio’s statewide voter registration list “for purposes of enforcing” the National Voter Registration Act (“NVRA”), 52 U.S.C. § 20501 *et seq.*, and the Help America Vote Act (“HAVA”), 52 U.S.C. § 20901 *et seq.* The letter argues that “[t]he NVRA requires each state ... to make available for inspection ‘all records concerning the implementation of programs and activities conducted for the purpose of ensuring the accuracy and currency of official lists of eligible voters.’” DOJ Letter (Aug. 6), at 1 (quoting 52 U.S.C. § 20507(i)(1)). The letter further contends that the “plain text of § 20507(i) requires disclosure.” *Id.*

The Department’s August 14 letter restates this position and posits additional authority for the requested actions. Specifically, the August 14 letter states that the Department is requesting Ohio’s voter registration list (“VRL”) “to assess your state’s compliance with the statewide VRL maintenance provisions” of the NVRA. DOJ Letter (Aug. 14), at 1. It indicates that the request is made pursuant to the Attorney General’s authority under Section 11 of the NVRA. *See id.* The Department further contends that it has the authority to seek the state’s voter list pursuant to Section 401 of HAVA. *See id.* at 1-2 (citing 52 U.S.C. § 21111). Finally, the letter separately contends that DOJ is empowered to request the voter registration list under Title III of the Civil Rights Act of 1960 (“CRA”). Section 303 of the CRA provides that “[a]ny record or paper required by section 20701 of this title to be retained and preserved shall, upon demand in writing by the Attorney General ... be made available for inspection, reproduction, and copying ....” 52 U.S.C. § 20703; *see* DOJ Letter (Aug. 14), at 2.

I appreciate that you personally took the time to meet on December 15, 2025, to discuss these requests. As noted above, I have instructed my staff to begin the process of fulfilling your request for Ohio's statewide voter file.

As a duty of my office, one of our foremost obligations is to safeguard the personal identifying information of Ohio's nearly eight million registered voters. Ohio has a hard-earned national reputation as the Gold Standard for election administration, and we remain committed to maintaining the security of voter data while simultaneously ensuring the integrity of Ohio's voter roll. In accordance with the Department's August 14, 2025 letter and our subsequent communications, the Ohio Secretary of State's Office understands that the Department of Justice will use the records only for legitimate governmental purposes and will not disclose any of the provided records to any entity except as authorized to do so under 52 U.S.C. § 20704. Further, it is our understanding that all federal data-privacy laws, including, but not limited to, the Privacy Act of 1974, 5 U.S.C. § 552(a), and Section 304 of the CRA, 52 U.S.C. § 20704, will be strictly followed.

Consistent with this understanding, we will work to transfer the requested data as quickly as practicable. We also appreciate your assurance that any notice regarding records identified throughout this process will contain sufficient information to explain why the record is flagged and why it is permissible to remove under federal law.

You have my assurance that election integrity will always be the top priority of my administration, and that begins with our duty under the law to maintain accurate voter rolls. We stand ready and grateful to partner with you in this effort. Thank you for your leadership.

Yours in service,



Frank LaRose

Ohio Secretary of State

# SECRETARY OF STATE

**NANCY LANDRY**  
SECRETARY OF STATE



P.O. BOX 94125  
BATON ROUGE, LA 70804-9125

December 17, 2025

Eric Neff  
Assistant Attorney General  
Civil Rights Division  
U.S. Department of Justice  
eric.neff@usdoj.gov

**RE: United States Department of Justice Civil Rights Division request for Louisiana voter data for list maintenance purposes**

Dear Mr. Neff:

I am writing to follow up on the United States Department of Justice Civil Rights Division (hereinafter "U.S. DOJ") request for Louisiana's voter registration data. The Louisiana Department of State (hereinafter "Department"), pursuant to La. R.S. 18:18, may share its voter registration data with a federal governmental agency for the purposes of its voter list maintenance. By transmission of this letter evidencing its written agreement, the Department hereby agrees to share its data with the U.S. DOJ for this express purpose.

Please provide the U.S. DOJ's information technology contact for the Department's IT Administrator to coordinate with for the secure exchange of this confidential information pursuant to La. R.S. 18:154 and La. R.S. 18:18.

If you have any questions or concerns, please do not hesitate to contact me at (225) 922-0547, or [tray.wood@sos.la.gov](mailto:tray.wood@sos.la.gov).

Sincerely,



Tray Wood  
General Counsel



U.S. Department of Justice

Civil Rights Division

---

Office of the Assistant Attorney General

Washington, D.C. 20530

August 14, 2025

Via Mail and Email

The Honorable Monae Johnson  
Secretary of State  
500 East Capitol Avenue, Suite 204  
Pierre, SD 57501-5070  
[sdsos@state.sd.us](mailto:sdsos@state.sd.us)

Re: **Complete South Dakota's Voter Registration List with All Fields**

Secretary Johnson:

We have received South Dakota's statewide voter registration list ("VRL"). However, as the Attorney General requested, the electronic copy of the statewide VRL must contain *all fields*, including the registrant's full name, date of birth, residential address, his or her state driver's license number or the last four digits of the registrant's social security number as required under the Help America Vote Act ("HAVA")<sup>1</sup> to register individuals for federal elections. *See* 52 U.S.C. § 21083(a)(5)(A)(i).

We have requested South Dakota's VRL to assess your state's compliance with the statewide VRL maintenance provisions of the National Voter Registration Act ("NVRA"), 52 U.S.C. § 20501, *et seq.* Our request is pursuant to the Attorney General's authority under Section 11 of the NVRA to bring enforcement actions. *See* 52 U.S.C. § 20501(a).

The Help America Vote Act ("HAVA"), 52 U.S.C. § 20501, *et seq.*, also provides authority for the Justice Department to seek the State's VRL via Section 401, which makes the Attorney General solely responsible for actions to enforce HAVA's computerized statewide Voter Registration List requirements. *See* 52 U.S.C. § 21111; *see also Brunner v. Ohio Republican Party*, 555 U.S. 5, 6 (2008) (*per curiam*) (finding there is no private right of action to enforce those requirements in HAVA).

---

<sup>1</sup> In charging the Attorney General with enforcement of the voter registration list requirements in the HAVA and in the NVRA, Congress plainly intended that Justice Department be able to conduct an independent review of each state's list. Any statewide prohibitions are clearly preempted by federal law.

In addition to those authorities, the Attorney General is also empowered by Congress to request records pursuant to Title III of the Civil Rights Act of 1960 (“CRA”), codified at 52 U.S.C. § 20701, *et seq.* Section 301 of the CRA requires state and local officials to retain and preserve records related to voter registration and other acts requisite to voting for any federal office for a period of 22 months after any federal general, special or primary election. *See* 52 U.S.C. § 20701.

Section 303 of the CRA provides, in pertinent part, “Any record or paper required by section 20701 of this title to be retained and preserved shall, upon demand in writing by the Attorney General or his representative directed to the person having custody, possession, or control of such record or paper, be made available for inspection, reproduction, and copying at the principal office of such custodian by the Attorney General or his representative...” 52 U.S.C. § 20703.

Pursuant to the foregoing authorities, including the CRA, the Attorney General is demanding an electronic copy of South Dakota’s complete and current VRL. The purpose of the request is to ascertain South Dakota’s compliance with the list maintenance requirements of the NVRA and HAVA.

When providing the electronic copy of the statewide VRL, South Dakota must ensure that it contains *all fields*, which includes the registrant’s full name, date of birth, residential address, his or her state driver’s license number or the last four digits of the registrant’s social security number as required under the Help America Vote Act (“HAVA”)<sup>2</sup> to register individuals for federal elections. *See* 52 U.S.C. § 21083(a)(5)(A)(i).

To the extent there are privacy concerns, the voter registration list is subject to federal privacy protections. Section 304 of the CRA provides the answer:

Unless otherwise ordered by a court of the United States, neither the Attorney General nor any employee of the Department of Justice, nor any other representative of the Attorney General, shall disclose any record or paper produced pursuant to this chapter, or any reproduction or copy, except to Congress and any committee thereof, governmental agencies, and in the presentation of any case or proceeding before any court or grand jury.

Moreover, HAVA specifies that the “last 4 digits of a social security number . . . shall not be considered a social security number for purposes of section 7 of the Privacy Act of 1974” (5 U.S.C. § 552a note); 52 U.S.C. § 21083(c). In addition, any prohibition of disclosure of a motor vehicle record contained in the Driver’s License Protection Act, codified at 18 U.S.C. § 2721(b)(1), is exempted when the disclosure is for use by a government agency in carrying out the government agency’s function to accomplish its enforcement authority as the Justice Department is now doing. That said, all data received from you will be kept securely and treated consistently with the Privacy Act.

---

<sup>2</sup> In charging the Attorney General with enforcement of the voter registration list requirements in the HAVA and in the NVRA, Congress plainly intended that Justice Department be able to conduct an independent review of each state’s list. Any statewide prohibitions are clearly preempted by federal law.

In charging the Attorney General with enforcement of the voter registration list requirements in HAVA and in the NVRA, Congress plainly intended that DOJ be able to conduct an independent review of each state's list. Any statewide prohibitions are preempted by federal law.

To that end, please provide the requested electronic Voter Registration List<sup>3</sup> to the Justice Department within seven days or by August 21, 2025.

The information and materials may be sent by encrypted email to [voting.section@usdoj.gov](mailto:voting.section@usdoj.gov) or via the Department's secure file-sharing system, Justice Enterprise File Sharing ("JEFS"). Should further clarification be required, please contact Maureen Riordan at [maureen.riordan2@usdoj.gov](mailto:maureen.riordan2@usdoj.gov).

Regards,



Harmeet K. Dhillon  
Assistant Attorney General  
Civil Rights Division

cc: Rachel Soulek  
Director, Division of Elections  
500 East Capitol Avenue, Suite 204  
Pierre, SD 57501-5070  
[Rachel.Soulek@state.sd.us](mailto:Rachel.Soulek@state.sd.us)

---

<sup>3</sup> Containing *all fields*, which includes either the registrant's full name, date of birth, residential address, his or her state driver's license number or the last four digits of the registrant's social security number as required by HAVA.

---

**From:** Voting Section (CRT) [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=e68131d470c24fbfabf066ea776544b0-\_MB\_VOTSEC]  
**Sent:** 8/7/2025 9:20:56 PM  
**To:** tre.hargett@tnsos.gov; Tre Hargett [Tre.Hargett@tn.gov]  
**CC:** mark.goins@tnsos.gov  
**Subject:** Please see the attached correspondence  
**Attachments:** State of Tennessee.pdf

Dear Secretary Hargett,

Please see the attached correspondence. If you would like to send responsive materials via the Department's secure file-sharing platform, Justice Enterprise File Sharing (JEFS), please let us know and we will send you instructions. Thank you.

**Voting Section**

Civil Rights Division  
U.S. Department of Justice  
950 Pennsylvania Ave NW- 4CON  
Washington, D.C. 20530  
1(800)253-3931



U.S. Department of Justice

Civil Rights Division

Voting Section  
950 Pennsylvania Ave, NW – 4CON  
Washington, DC 20530

August 7, 2025

Via Mail and Email

The Honorable Tre Hargett  
Secretary of State  
600 Charlotte Ave.  
Nashville, TN 37243-1102  
tre.hargett@tnsos.gov; tre.hargett@tn.gov

Dear Secretary Hargett:

We write to you as the chief election official for the State of Tennessee to request Tennessee’s statewide voter registration list and information regarding Tennessee’s procedures for complying with the statewide voter registration list maintenance provisions of the National Voter Registration Act (“NVRA”), 52 U.S.C. § 20501 *et seq.* On July 8, we contacted you about obtaining an electronic copy of the statewide voter registration list for purposes of enforcing the NVRA and the Help America Vote Act, 52 U.S.C. § 20901 *et seq.*, and we are renewing our request for that information today.

The NVRA requires each state and the District of Columbia to make available for inspection “all records concerning the implementation of programs and activities conducted for the purpose of ensuring the accuracy and currency of official lists of eligible voters.” 52 U.S.C. § 20507(i)(1). Section 11 of the NVRA authorizes the Attorney General to bring NVRA enforcement actions. *See* 52 U.S.C. § 20510.

The plain text of § 20507(i) requires disclosure. The phrase “all records” envisions an expansive application and includes the registration information of cancelled records and accompanying voter history. *Project Vote/Voting for Am, Inc. v. Long*, 682 F.3d 331, 336 (4th Cir. 2012); *see also Voter Reference Foundation, LLC v. Torrez*, 727 F.Supp.3d 1014, 1212 (D. N.M. 2024) (finding “all records” includes voter list). Similarly, “programs and activities conducted for the purpose of ensuring the accuracy and currency of official lists of eligible voters” encompasses a broad range of state programs, including the removal of non-citizens from voter rolls. *Id.* The capacious language of the Public Disclosure Provision has been found to “set[] a floor, not a ceiling” to the types of records that must be disclosed. *Public Interest Legal Foundation, Inc. v. Matthews*, 589 F.Supp.3d 932, 941 (C.D. Ill. 2022) (citing *Project Vote/Voting for Am., Inc.*, 682 F.3d at 337). The request for the statewide voter registration list sits firmly above that floor. Courts have continuously found that Section 8(i) requires the disclosure of voter registration records. *See, e.g., Public Interest Legal Foundation v. Boockvar*, 431 F.Supp.3d 553, 556 (M.D. Pa. 2019) (permitting disclosure of documents regarding “all registrants who were identified as potentially not satisfying the citizenship

requirement”); *Project Vote/Voting for Am, Inc.*, 682 F.3d at 333 (4th Cir. 2012) (requiring disclosure of voter registration applications for “any individual” who timely completed an application) (emphasis added); *Project Vote, Inc. v. Kemp*, 208 F.Supp.3d 1320, 1344 (N.D. Ga. 2016) (holding that “Section 8(i) requires the disclosure of individual voter registration records”).

Congress passed the NVRA in an effort to “protect the integrity of the electoral process” and “ensure that accurate and current voter registration rolls are maintained.” NVRA § 20501. This intention is achieved through the public disclosure provision, which Congress created to establish external checks on potential administrative oversights or inefficiencies regarding ineligible voters appearing on voter rolls. *See Project Vote/Voting for Am, Inc.*, 682 F.3d at 334-35. State laws are not a bar to providing this information. If the NVRA, a federal act, and state law “do not operate harmoniously in a single procedural scheme for federal voter registration, then Congress has exercised its power to ‘alter’ the state’s regulation, and that regulation is superseded.” *Gonzalez v. Arizona*, 677 F.3d 383, 394 (9th Cir. 2012) (en banc), *aff’d sub nom. Arizona v. Inter Tribal Council of Arizona, Inc.* (“ITCA”), 570 U.S. 1 (2013).

Please also provide a list of the election officials who are responsible for implementing Tennessee’s general program of voter registration list maintenance from November 2022 through receipt of this letter, including those responsible officials not employed by your office (such as local election officials) who are also involved in that effort. Please also provide a description of the steps that you have taken, and when those steps were taken, to ensure that the State’s list maintenance program has been properly carried out in full compliance with the NVRA.

Please provide this information within 14 days of the date of this letter. The information and materials may be sent by encrypted email to [voting.section@usdoj.gov](mailto:voting.section@usdoj.gov) or via the Department’s secure file-sharing system, Justice Enterprise File Sharing (JEFS).

Should further clarification be required, please contact Maureen Riordan at [maureen.riordan2@usdoj.gov](mailto:maureen.riordan2@usdoj.gov). We look forward to your assistance in advance.

Sincerely,



Michael E. Gates  
Deputy Assistant Attorney General  
Civil Rights Division

Maureen Riordan  
Acting Chief, Voting Section  
Civil Rights Division

cc: Mark Goins  
Coordinator of Elections  
312 Rosa L. Parks Avenue, 7th Floor  
Nashville, TN 37243-1102  
mark.goins@tnsos.gov



U.S. Department of Justice

Civil Rights Division

---

Office of the Assistant Attorney General

Washington, D.C. 20530

August 14, 2025

Via Mail and Email

The Honorable Tre Hargett  
Secretary of State  
600 Charlotte Ave.  
Nashville, TN 37243-1102  
[tre.hargett@tnsos.gov](mailto:tre.hargett@tnsos.gov);  
[tre.hargett@tn.gov](mailto:tre.hargett@tn.gov)

Re: **Complete Tennessee's Voter Registration List with All Fields**

Secretary Hargett:

We understand that the time the Justice Department has provided your state to respond to the request for a statewide voter registration list ("VRL") and other information has not reached its deadline.

Given responses from other states thus far, we want to clarify that the Justice Department's request to provide an electronic copy of the statewide VRL should contain *all fields*, which means, your state's VRL must include the registrant's full name, date of birth, residential address, his or her state driver's license number or the last four digits of the registrant's social security number as required under the Help America Vote Act ("HAVA")<sup>1</sup> to register individuals for federal elections. *See* 52 U.S.C. § 21083(a)(5)(A)(i).

We have requested Tennessee's VRL to assess your state's compliance with the statewide VRL maintenance provisions of the National Voter Registration Act ("NVRA"), 52 U.S.C. § 20501, *et seq.* Our request is pursuant to the Attorney General's authority under Section 11 of the NVRA to bring enforcement actions. *See* 52 U.S.C. § 20501(a).

---

<sup>1</sup> In charging the Attorney General with enforcement of the voter registration list requirements in the HAVA and in the NVRA, Congress plainly intended that DOJ be able to conduct an independent review of each state's list. Any statewide prohibitions are clearly preempted by federal law.

The Help America Vote Act (“HAVA”), 52 U.S.C. § 20501, *et seq.*, also provides authority for the Justice Department to seek the State’s VRL via Section 401, which makes the Attorney General solely responsible for actions to enforce HAVA’s computerized statewide voter registration list requirements. *See* 52 U.S.C. § 21111; *see also* *Brunner v. Ohio Republican Party*, 555 U.S. 5, 6 (2008) (*per curiam*) (finding there is no private right of action to enforce those requirements in HAVA).

In addition to those authorities, the Attorney General is also empowered by Congress to request records pursuant to Title III of the Civil Rights Act of 1960 (“CRA”), codified at 52 U.S.C. § 20701, *et seq.* Section 301 of the CRA requires state and local officials to retain and preserve records related to voter registration and other acts requisite to voting for any federal office for a period of 22 months after any federal general, special or primary election. *See* 52 U.S.C. § 20701.

Section 303 of the CRA provides, in pertinent part, “Any record or paper required by section 20701 of this title to be retained and preserved shall, upon demand in writing by the Attorney General or his representative directed to the person having custody, possession, or control of such record or paper, be made available for inspection, reproduction, and copying at the principal office of such custodian by the Attorney General or his representative...” 52 U.S.C. § 20703.

Pursuant to the foregoing authorities, including the CRA, the Attorney General is demanding an electronic copy of Tennessee’s complete and current VRL. The purpose of the request is to ascertain Tennessee’s compliance with the list maintenance requirements of the NVRA and HAVA.

When providing the electronic copy of the statewide VRL, Tennessee must ensure that it contains *all fields*, which includes either the registrant’s full name, date of birth, residential address, his or her state driver’s license number, or the last four digits of the registrant’s social security number as required under the Help America Vote Act (“HAVA”)<sup>2</sup> to register individuals for federal elections. *See* 52 U.S.C. § 21083(a)(5)(A)(i).

To the extent there are privacy concerns, the voter registration list is subject to federal privacy protections. Section 304 of the CRA provides the answer:

Unless otherwise ordered by a court of the United States, neither the Attorney General nor any employee of the Department of Justice, nor any other representative of the Attorney General, shall disclose any record or paper produced pursuant to this chapter, or any reproduction or copy, except to Congress and any committee thereof, governmental agencies, and in the presentation of any case or proceeding before any court or grand jury.

HAVA specifies that the “last 4 digits of a social security number . . . shall not be considered a social security number for purposes of section 7 of the Privacy Act of 1974” (5 U.S.C. § 552a note); 52 U.S.C. § 21083(c). In addition, any prohibition of disclosure of a motor vehicle record contained

---

<sup>2</sup> In charging the Attorney General with enforcement of the voter registration list requirements in HAVA and in the NVRA, Congress plainly intended that DOJ be able to conduct an independent review of each state’s list. Any statewide prohibitions are clearly preempted by federal law.

in the Driver's License Protection Act, codified at 18 U.S.C. § 2721(b)(1), is exempted when the disclosure is for use by a government agency in carrying out the government agency's function to accomplish its enforcement authority as the Justice Department is now doing. That said, all data received from you will be kept securely and treated consistently with the Privacy Act.

To that end, please provide the requested electronic Voter Registration List<sup>3</sup> to the Justice Department by the date set for your delivery by our original letter, or by August 21, 2025, whichever is later.

The information and materials may be sent by encrypted email to [voting.section@usdoj.gov](mailto:voting.section@usdoj.gov) or via the Department's secure file-sharing system, Justice Enterprise File Sharing ("JEFS"). Should further clarification be required, please contact Maureen Riordan at [maureen.riordan2@usdoj.gov](mailto:maureen.riordan2@usdoj.gov).

Regards,



Harmeet K. Dhillon  
Assistant Attorney General  
Civil Rights Division

cc: Mark Goins  
Coordinator of Elections  
312 Rosa L. Parks Avenue, 7th Floor  
Nashville, TN 37243-1102  
[mark.goins@tnsos.gov](mailto:mark.goins@tnsos.gov)

---

<sup>3</sup> Containing *all fields*, which includes either the registrant's full name, date of birth, residential address, his or her state driver's license number or the last four digits of the registrant's social security number as required by HAVA.

---

**From:** Voting Section (CRT) [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=e68131d470c24fbfabf066ea776544b0-\_MB\_VOTSEC]  
**Sent:** 8/7/2025 9:08:56 PM  
**To:** jnelson@sos.texas.gov; secretary@sos.texas.gov  
**CC:** cadkins@sos.texas.gov  
**Subject:** Please see the attached correspondence  
**Attachments:** State of Texas.pdf

Dear Secretary Nelson,

Please see the attached correspondence. If you would like to send responsive materials via the Department's secure file-sharing platform, Justice Enterprise File Sharing (JEFS), please let us know and we will send you instructions. Thank you.

**Voting Section**

Civil Rights Division  
U.S. Department of Justice  
950 Pennsylvania Ave NW- 4CON  
Washington, D.C. 20530  
1(800)253-3931



U.S. Department of Justice

Civil Rights Division

Voting Section  
950 Pennsylvania Ave, NW – 4CON  
Washington, DC 20530

August 7, 2025

Via Mail and Email

The Honorable Jane Nelson  
Secretary of State  
P.O. Box 12887  
Austin, TX 78701  
jnelson@sos.texas.gov; secretary@sos.texas.gov

Dear Secretary Nelson:

We write to you as the chief election official for the State of Texas to request Texas' statewide voter registration list and information regarding Texas' procedures for complying with the statewide voter registration list maintenance provisions of the National Voter Registration Act ("NVRA"), 52 U.S.C. § 20501 *et seq.* On July 8, we contacted your office about obtaining an electronic copy of the statewide voter registration list for purposes of enforcing the NVRA and the Help America Vote Act, 52 U.S.C. § 20901 *et seq.*, and we are renewing our request for that information today.

The NVRA requires each state and the District of Columbia to make available for inspection "all records concerning the implementation of programs and activities conducted for the purpose of ensuring the accuracy and currency of official lists of eligible voters." 52 U.S.C. § 20507(i)(1). Section 11 of the NVRA authorizes the Attorney General to bring NVRA enforcement actions. *See* 52 U.S.C. § 20510.

The plain text of § 20507(i) requires disclosure. The phrase "all records" envisions an expansive application and includes the registration information of cancelled records and accompanying voter history. *Project Vote/Voting for Am, Inc. v. Long*, 682 F.3d 331, 336 (4th Cir. 2012); *see also Voter Reference Foundation, LLC v. Torrez*, 727 F.Supp.3d 1014, 1212 (D. N.M. 2024) (finding "all records" includes voter list). Similarly, "programs and activities conducted for the purpose of ensuring the accuracy and currency of official lists of eligible voters" encompasses a broad range of state programs, including the removal of non-citizens from voter rolls. *Id.* The capacious language of the Public Disclosure Provision has been found to "set[] a floor, not a ceiling" to the types of records that must be disclosed. *Public Interest Legal Foundation, Inc. v. Matthews*, 589 F.Supp.3d 932, 941 (C.D. Ill. 2022) (citing *Project Vote/Voting for Am., Inc.*, 682 F.3d at 337). The request for the statewide voter registration list sits firmly above that floor. Courts have continuously found that Section 8(i) requires the disclosure of voter registration records. *See, e.g., Public Interest Legal Foundation v. Boockvar*, 431 F.Supp.3d 553, 556 (M.D. Pa. 2019) (permitting disclosure of documents regarding "all registrants who were identified as potentially not satisfying the citizenship

requirement”); *Project Vote/Voting for Am, Inc.*, 682 F.3d at 333 (4th Cir. 2012) (requiring disclosure of voter registration applications for “any individual” who timely completed an application) (emphasis added); *Project Vote, Inc. v. Kemp*, 208 F.Supp.3d 1320, 1344 (N.D. Ga. 2016) (holding that “Section 8(i) requires the disclosure of individual voter registration records”).

Congress passed the NVRA in an effort to “protect the integrity of the electoral process” and “ensure that accurate and current voter registration rolls are maintained.” NVRA § 20501. This intention is achieved through the public disclosure provision, which Congress created to establish external checks on potential administrative oversights or inefficiencies regarding ineligible voters appearing on voter rolls. *See Project Vote/Voting for Am, Inc.*, 682 F.3d at 334-35. State laws are not a bar to providing this information. If the NVRA, a federal act, and state law “do not operate harmoniously in a single procedural scheme for federal voter registration, then Congress has exercised its power to ‘alter’ the state’s regulation, and that regulation is superseded.” *Gonzalez v. Arizona*, 677 F.3d 383, 394 (9th Cir. 2012) (en banc), *aff’d sub nom. Arizona v. Inter Tribal Council of Arizona, Inc.* (“ITCA”), 570 U.S. 1 (2013).

Please also provide a list of the election officials who are responsible for implementing Texas’ general program of voter registration list maintenance from November 2022 through receipt of this letter, including those responsible officials not employed by your office (such as local election officials) who are also involved in that effort. Please also provide a description of the steps that you have taken, and when those steps were taken, to ensure that the State’s list maintenance program has been properly carried out in full compliance with the NVRA.

Please provide this information within 14 days of the date of this letter. The information and materials may be sent by encrypted email to [voting.section@usdoj.gov](mailto:voting.section@usdoj.gov) or via the Department’s secure file-sharing system, Justice Enterprise File Sharing (JEFS).

Should further clarification be required, please contact Maureen Riordan at [maureen.riordan2@usdoj.gov](mailto:maureen.riordan2@usdoj.gov). We look forward to your assistance in advance.

Sincerely,



Michael E. Gates  
Deputy Assistant Attorney General  
Civil Rights Division

Maureen Riordan  
Acting Chief, Voting Section  
Civil Rights Division

cc: Christina Adkins  
Director of Elections  
1019 Brazos St.  
Austin, TX 78701  
cadkins@sos.texas.gov



U.S. Department of Justice

Civil Rights Division

---

Office of the Assistant Attorney General

Washington, D.C. 20530

August 14, 2025

Via Mail and Email

The Honorable Jane Nelson  
Secretary of State  
P.O. Box 12887  
Austin, TX 78701  
[jnelson@sos.texas.gov](mailto:jnelson@sos.texas.gov);  
[secretary@sos.texas.gov](mailto:secretary@sos.texas.gov)

Re: **Complete Texas's Voter Registration List with All Fields**

Secretary Nelson:

We understand that the time the Justice Department has provided your state to respond to the request for a statewide voter registration list ("VRL") and other information has not reached its deadline.

Given responses from other states thus far, we want to clarify that the Justice Department's request to provide an electronic copy of the statewide VRL should contain *all fields*, which means, your state's VRL must include the registrant's full name, date of birth, residential address, his or her state driver's license number or the last four digits of the registrant's social security number as required under the Help America Vote Act ("HAVA")<sup>1</sup> to register individuals for federal elections. *See* 52 U.S.C. § 21083(a)(5)(A)(i).

We have requested Texas's VRL to assess your state's compliance with the statewide VRL maintenance provisions of the National Voter Registration Act ("NVRA"), 52 U.S.C. § 20501, *et seq.* Our request is pursuant to the Attorney General's authority under Section 11 of the NVRA to bring enforcement actions. *See* 52 U.S.C. § 20501(a).

---

<sup>1</sup> In charging the Attorney General with enforcement of the voter registration list requirements in the HAVA and in the NVRA, Congress plainly intended that DOJ be able to conduct an independent review of each state's list. Any statewide prohibitions are clearly preempted by federal law.

The Help America Vote Act (“HAVA”), 52 U.S.C. § 20501, *et seq.*, also provides authority for the Justice Department to seek the State’s VRL via Section 401, which makes the Attorney General solely responsible for actions to enforce HAVA’s computerized statewide voter registration list requirements. *See* 52 U.S.C. § 21111; *see also Brunner v. Ohio Republican Party*, 555 U.S. 5, 6 (2008) (*per curiam*) (finding there is no private right of action to enforce those requirements in HAVA).

In addition to those authorities, the Attorney General is also empowered by Congress to request records pursuant to Title III of the Civil Rights Act of 1960 (“CRA”), codified at 52 U.S.C. § 20701, *et seq.* Section 301 of the CRA requires state and local officials to retain and preserve records related to voter registration and other acts requisite to voting for any federal office for a period of 22 months after any federal general, special or primary election. *See* 52 U.S.C. § 20701.

Section 303 of the CRA provides, in pertinent part, “Any record or paper required by section 20701 of this title to be retained and preserved shall, upon demand in writing by the Attorney General or his representative directed to the person having custody, possession, or control of such record or paper, be made available for inspection, reproduction, and copying at the principal office of such custodian by the Attorney General or his representative...” 52 U.S.C. § 20703.

Pursuant to the foregoing authorities, including the CRA, the Attorney General is demanding an electronic copy of Texas’s complete and current VRL. The purpose of the request is to ascertain Texas’s compliance with the list maintenance requirements of the NVRA and HAVA.

When providing the electronic copy of the statewide VRL, Texas must ensure that it contains *all fields*, which includes either the registrant’s full name, date of birth, residential address, his or her state driver’s license number, or the last four digits of the registrant’s social security number as required under the Help America Vote Act (“HAVA”)<sup>2</sup> to register individuals for federal elections. *See* 52 U.S.C. § 21083(a)(5)(A)(i).

To the extent there are privacy concerns, the voter registration list is subject to federal privacy protections. Section 304 of the CRA provides the answer:

Unless otherwise ordered by a court of the United States, neither the Attorney General nor any employee of the Department of Justice, nor any other representative of the Attorney General, shall disclose any record or paper produced pursuant to this chapter, or any reproduction or copy, except to Congress and any committee thereof, governmental agencies, and in the presentation of any case or proceeding before any court or grand jury.

HAVA specifies that the “last 4 digits of a social security number . . . shall not be considered a social security number for purposes of section 7 of the Privacy Act of 1974” (5 U.S.C. § 552a note); 52 U.S.C. § 21083(c). In addition, any prohibition of disclosure of a motor vehicle record contained

---

<sup>2</sup> In charging the Attorney General with enforcement of the voter registration list requirements in HAVA and in the NVRA, Congress plainly intended that DOJ be able to conduct an independent review of each state’s list. Any statewide prohibitions are clearly preempted by federal law.

in the Driver's License Protection Act, codified at 18 U.S.C. § 2721(b)(1), is exempted when the disclosure is for use by a government agency in carrying out the government agency's function to accomplish its enforcement authority as the Justice Department is now doing. That said, all data received from you will be kept securely and treated consistently with the Privacy Act.

To that end, please provide the requested electronic Voter Registration List<sup>3</sup> to the Justice Department by the date set for your delivery by our original letter, or by August 21, 2025, whichever is later.

The information and materials may be sent by encrypted email to [voting.section@usdoj.gov](mailto:voting.section@usdoj.gov) or via the Department's secure file-sharing system, Justice Enterprise File Sharing ("JEFS"). Should further clarification be required, please contact Maureen Riordan at [maureen.riordan2@usdoj.gov](mailto:maureen.riordan2@usdoj.gov).

Regards,



Harmeet K. Dhillon  
Assistant Attorney General  
Civil Rights Division

cc: Christina Adkins  
Director of Elections  
1019 Brazos St.  
Austin, TX 78701  
[cadkins@sos.texas.gov](mailto:cadkins@sos.texas.gov)

---

<sup>3</sup> Containing *all fields*, which includes either the registrant's full name, date of birth, residential address, his or her state driver's license number or the last four digits of the registrant's social security number as required by HAVA.

---

**From:** Neff, Eric (CRT) [Eric.Neff@usdoj.gov]  
**Sent:** 12/9/2025 1:17:10 PM  
**To:** GeneralCounsel [GeneralCounsel@sos.texas.gov]  
**CC:** Christina Adkins [CAdkins@sos.texas.gov]; Secretary [Secretary@sos.texas.gov]  
**Subject:** RE: DOJ CRT proposed MOU  
**Attachments:** EXECUTED MOU DOJ-TX 12.9.25.pdf

All,

See attached. (Had to wait until my title became official this morning to sign it myself.)

Let me know if you need any assistance with the file sharing execution.

Thanks,  
Eric

**Eric Neff**  
Acting Chief  
Civil Rights Division, Voting Section  
Department of Justice  
150 M St. NE, Ste. 8-139  
Washington, DC 20002  
[Eric.Neff@usdoj.gov](mailto:Eric.Neff@usdoj.gov)  
Office: 202-704-5430  
Cell: 202-532-3628



---

**From:** GeneralCounsel <GeneralCounsel@sos.texas.gov>  
**Sent:** Friday, December 5, 2025 6:53 PM  
**To:** Neff, Eric (CRT) <Eric.Neff@usdoj.gov>  
**Cc:** Christina Adkins <CAdkins@sos.texas.gov>; Secretary <Secretary@sos.texas.gov>; GeneralCounsel <GeneralCounsel@sos.texas.gov>  
**Subject:** [EXTERNAL] RE: DOJ CRT proposed MOU

Mr. Neff,

In reference to your November 25, 2025 correspondence, the Office of the Texas Secretary of State is providing the attached executed copy of the Memorandum of Understanding. Please return a counter-signed version of the MOU once the agreement has been executed by a representative of the Civil Rights Division.

Sincerely,

Adam Bitter

**Adam Bitter**

General Counsel  
Office of the Texas Secretary of State  
(512) 475-2813

**From:** Neff, Eric (CRT) <[Eric.Neff@usdoj.gov](mailto:Eric.Neff@usdoj.gov)>  
**Sent:** Tuesday, November 25, 2025 10:08 AM  
**To:** General Counsel <[GeneralCounsel@sos.texas.gov](mailto:GeneralCounsel@sos.texas.gov)>  
**Cc:** Christina Adkins <[CAdkins@sos.texas.gov](mailto:CAdkins@sos.texas.gov)>; Secretary <[Secretary@sos.texas.gov](mailto:Secretary@sos.texas.gov)>  
**Subject:** DOJ CRT proposed MOU

**This Message Is From an External Sender**

CAUTION: This email originated from OUTSIDE of the SOS organization. Do not click on links or open attachments unless you are expecting the email and know that the content is safe. If you believe this to be a malicious or phishing email, please send this email as an attachment to [informationsecurity@sos.texas.gov](mailto:informationsecurity@sos.texas.gov).

Report Suspicious

Mr. Bitter,

Following up on my voicemail from today. I am the new point of contact for Voter Roll Maintenance communication. Please see the attached proposed MOU from the Department of Justice. This MOU in our opinion satisfies all reasonable concerns regarding privacy and data security. This MOU includes a request for compliance within 7 days of receipt of this communication. Compliance requires providing all records requested in previous communications with your Department, most notably our letters from August 7 and August 14 of this year.

Please do not hesitate to contact me if you have any questions.

Best,  
Eric

**Eric Neff**

Trial Attorney  
Civil Rights Division  
Department of Justice  
150 M St. NE, Ste. 8-139  
Washington, DC 20002  
[Eric.Neff@usdoj.gov](mailto:Eric.Neff@usdoj.gov)  
Cell: 202-532-3628





U.S. Department of Justice

Civil Rights Division

---

**CONFIDENTIAL MEMORANDUM OF UNDERSTANDING**

**I. PARTIES & POINTS OF CONTACT.**

Requester

Federal Agency Name: Civil Rights Division, U.S. Department of Justice

VRL/Data User: Eric Neff

Title: Acting Chief, Voting Section

Address: 150 M St. NE, Ste. 8-139, Washington DC 20002

Phone: (202) 704-5430

VRL/Data Provider

State Agency Name: Office of the Texas Secretary of State

Custodian: Adam Bitter

Title: General Counsel

Address: P.O. Box 12697, Austin, Texas 78711-2697

Phone: (512) 475-2813

The parties to this Memorandum of Understanding ("MOU" or "Agreement") are the Department of Justice, Civil Rights Division ("Justice Department" or "Department"), and the State of Texas ("Texas").

**II. AUTHORITY.**

By this Agreement, Texas has agreed to, and will, provide an electronic copy of your state's complete statewide Voter Registration List ("VRL" or "VRL/Data") to the Civil Rights Division of the U.S. Department of Justice (at times referred to as the "Department"). The VRL/Data must include, among other fields of data, the voter registrant's full name, date of birth, residential address, his or her state driver's license number or the last four digits of the registrant's social

security number as required under the HAVA to register individuals for federal elections. *See* 52 U.S.C. § 21083(a)(5)(A).

The authorities by which this information is requested by the Department of Justice are:

- National Voter Registration Act of 1993, 52 U.S.C. § 20501, *et seq.*
- Attorney General’s authority under Section 11 of the NVRA to bring enforcement actions. *See* 52 U.S.C. § 20501(a).
- Help America Vote Act of 2002, 52 U.S.C. § 20901, *et seq.*
- Attorney General’s authority to enforce the Help America Vote Act under 53 U.S.C. § 21111.
- Attorney General authority to request records pursuant to Title III of the Civil Rights Act of 1960 (“CRA”), codified at 52 U.S.C. § 20701, *et seq.*
- The Privacy Act of 1974, 5 U.S.C. § 552a, as amended.

### **III. PURPOSE.**

A VRL is a Voter Registration List pursuant to the NVRA and HAVA, commonly referred to as “voter roll,” compiled by a state – often from information submitted by counties – containing a list of all the state’s *eligible* voters. Regardless of the basis for ineligibility, ineligible voters do not appear on a state’s VRL when proper list maintenance is performed by states. The Justice Department is requesting your state’s VRL to test, analyze, and assess states’ VRLs for proper list maintenance and compliance with federal law. In the event the Justice Department’s analysis of a VRL results in list maintenance issues, insufficiency, inadequacy, anomalies, or concerns, the Justice Department will notify your state’s point of contact of the issues to assist your state with curing.

The purpose of this MOU is to establish the parties' understanding as to the security protections for data transfer and data access by the Department of Justice of the electronic copy of the statewide voter registration list, including all fields requested by the Department of Justice.

**IV. TIMING OF AGREEMENT – TIME IS OF ESSENCE.**

Although the Justice Department is under no such obligation as a matter of law, because this Agreement is proposed, made, and to be entered into at your state's request as part of your state's transmission of its VRL to the Justice Department, this Agreement is to be fully executed within seven (7) days of the Justice Department presenting this Agreement to you. Both parties agree that no part of this Agreement or execution is intended to, or will, cause delay of the transmission of your state's VRL to the Justice Department for analysis.

**V. TIMING OF VRL/DATA TRANSFER.**

You agree to transfer an electronic copy of your state's complete statewide VRL/Data to the Civil Rights Division of the U.S. Department of Justice as described in Section III of this Agreement no later than five (5) business days from the execution of this Agreement, which is counted from the last day of the last signatory.

**VI. METHOD OF VRL/DATA ACCESS OR TRANSFER.**

The VRL will be submitted by your state via the Department of Justice's secure file-sharing system, i.e., Justice Enterprise File Sharing (JEFS"). A separate application to use JEFS must be completed and submitted by your state through the Civil Rights Help Desk. JEFS implements strict access controls to ensure that each user can only access their own files. All files and folders are tied to a specific user, and each user has defined permissions that govern how they may interact with those files (e.g., read, write, or read-only).

Whenever a user attempts to access a file or folder, JEFS validates the request against the assigned permissions to confirm that the user is explicitly authorized. This process guarantees that users can only access files and folders only where they have permission. Users are also limited to the authorized type of interaction with each file or folder. Within the Department of Justice, access to JEFS is restricted to specific roles: Litigation Support, IT staff, and Civil Rights Division staff.

#### **VII. LOCATION OF DATA AND CUSTODIAL RESPONSIBILITY.**

The parties mutually agree that the Civil Rights Division (also “Department”) will be designated as “Custodian” of the file(s) and will be responsible for the observance of all conditions for use and for establishment and maintenance of security agreements as specified in this agreement to prevent unauthorized use. The information that the Department is collecting will be maintained consistent with the Privacy Act of 1974, 5 U.S.C. § 552a. The full list of routine uses for this collection of information can be found in the Systems of Record Notice (“SORN”) titled, JUSTICE/CRT – 001, “Central Civil Rights Division Index File and Associated Records,” 68 Fed. Reg. 47610-01, 611 (August 11, 2003); 70 Fed. Reg. 43904-01 (July 29, 2005); and 82 Fed. Reg. 24147-01 (May 25, 2017). It should be noted that the statutes cited for routine use include NVRA, HAVA, and the Civil Rights Act of 1960, and the Justice Department is making our request pursuant to those statutes. The records in the system of records are kept under the authority of 44 U.S.C. § 3101 and in the ordinary course of fulfilling the responsibility assigned to the Civil Rights Division under the provisions of 28 C.F.R. §§ 0.50, 0.51.

VRL/Data storage is similar to the restricted access provided on JEFS and complies with the SORN: Information in computer form is safeguarded and protected in accordance with applicable Department security regulations for systems of records. Only a limited number of staff members who are assigned a specific identification code will be able to use the computer to access

the stored information. However, a section may decide to allow its employees access to the system in order to perform their official duties.

All systems storing the VRL data will comply with all security requirements applicable to Justice Department systems, including but not limited to all Executive Branch system security requirements (e.g., requirements imposed by the Office of Management and Budget [OMB] and National Institute of Standards and Technology [NIST]), Department of Justice IT Security Standards, and Department of Justice Order 2640.2F.

#### **VIII. NVRA/HAVA COMPLIANT VOTER REGISTRATION LIST.**

After analysis and assessment of your state's VRL, the Justice Department will securely notify you or your state of any voter list maintenance issues, insufficiencies, inadequacies, deficiencies, anomalies, or concerns, the Justice Department found when testing, assessing, and analyzing your state's VRL for NVRA and HAVA compliance, i.e., that your state's VRL only includes eligible voters.

You agree therefore that within forty-five (45) days of receiving that notice from the Justice Department of any issues, insufficiencies, inadequacies, deficiencies, anomalies, or concerns, your state will clean its VRL/Data by removing ineligible voters and resubmit the updated VRL/Data to the Civil Rights Division of the Justice Department to verify proper list maintenance has occurred by your state pursuant to the NVRA and HAVA.

#### **IX. CONFIDENTIALITY & DEPARTMENT SAFEGUARDS.**

Any member of the Justice Department in possession of a VRL/Data will employ reasonable administrative, technical, and physical safeguards designed to protect the security and confidentiality of such data. Compliance with these safeguards will include secure user authentication protocols deploying either: (i) Two-Factor Authentication ("2FA"), which requires users to go through two layers of security before access is granted to the system; or (ii) the

assignment of unique user identifications to each person with computer access plus unique complex passwords, which are not vendor supplied default passwords.

The Department will activate audit logging for the records, files, and data containing the state's VRL/Data in order to identify abnormal use, as well as to track access control, on computers, servers and/or Devices containing the VRL/Data.

For all devices storing records, files, and data containing the VRL/Data: there is (i) up-to-date versions of system security agent software that includes endpoint protection and malware protection and reasonably up-to-date patches and virus definitions, or a version of such software that can still be supported with up-to-date patches and virus definitions, and is set to receive the most current security updates on a regular basis; and (ii) up-to-date operating system security patches designed to maintain the integrity of the personal information.

For all devices storing records, files, and data containing the VRL/Data: there is (i) controlled and locked physical access for the Device; and (ii) the prohibition of the connection of the Device to public or insecure home networks.

There will be no copying of records, files, or data containing the VRL/Data to unencrypted USB drives, CDs, or external storage. In addition, the use of devices outside of moving the records, files, or data to the final stored device location shall be limited.

Any notes, lists, memoranda, indices, compilations prepared or based on an examination of VRL/Data or any other form of information (including electronic forms), that quote from, paraphrase, copy, or disclose the VRL/Data with such specificity that the VRL/Data can be identified, or by reasonable logical extension can be identified will not be shared by the Department. Any summary results, however, may be shared by the Department.

In addition to the Department's enforcement efforts, the Justice Department may use the information you provide for certain routine, or pre-litigation or litigation purposes including:

present VRL/Data to a court, magistrate, or administrative tribunal; a contractor with the Department of Justice who needs access to the VRL/Data information in order to perform duties related to the Department's list maintenance verification procedures. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. § 552a(m).

**X. LOSS OR BREACH OF DATA.**

If a receiving party discovers any loss of VRL/Data, or a breach of security, including any actual or suspected unauthorized access, relating to VRL/Data, the receiving party shall, at its own expense immediately provide written notice to the producing party of such breach; investigate and make reasonable and timely efforts to remediate the effects of the breach, and provide the producing party with assurances reasonably satisfactory to the producing party that such breach shall not recur; and provide sufficient information about the breach that the producing party can reasonably ascertain the size and scope of the breach. The receiving party agrees to cooperate with the producing party or law enforcement in investigating any such security incident. In any event, the receiving party shall promptly take all necessary and appropriate corrective action to terminate unauthorized access.

**XI. DESTRUCTION OF DATA.**

The Department will destroy all VRL/Data associated with actual records as soon as the purposes of the list maintenance project have been accomplished and the time required for records retention pursuant to applicable law has passed. When the project is complete and such retention requirements by law expires, the Justice Department will:

1. Destroy all hard copies containing confidential data (e.g., shredding);
2. Archive and store electronic data containing confidential information offline in a secure location; and

3. All other data will be erased or maintained in a secured area.

## **XII. OTHER PROVISIONS.**


- A. Conflicts. This MOU constitutes the full MOU on this subject between the Department and your state. Any inconsistency or conflict between or among the provisions of this MOU, will be resolved in the following order of precedence: (1) this MOU and (2) other documents incorporated by reference in this MOU (e.g., transaction charges).
- B. Severability. Nothing in this MOU is intended to conflict with current law or regulation or the directives of Department, or the your state. If a term of this MOU is inconsistent with such authority, then that term shall be invalid but, to the extent allowable, the remaining terms and conditions of this MOU shall remain in full force and effect.
- C. Assignment. Your state may not assign this MOU, nor may it assign any of its rights or obligations under this MOU. To the extent allowable by law, this MOU shall inure to the benefit of, and be binding upon, any successors to the Justice Department and your state without restriction.
- D. Waiver. No waiver by either party of any breach of any provision of this MOU shall constitute a waiver of any other breach. Failure of either party to enforce at any time, or from time to time, any provision of this MOU shall not be construed to be a waiver thereof.
- E. Compliance with Other Laws. Nothing in this MOU is intended or should be construed to limit or affect the duties, responsibilities, and rights of the User Agency under the National Voter Registration Act, 52 U.S.C. § 20501 *et seq.*, as amended; the Help America Vote Act, 52 U.S.C. § 20901 *et seq.*, as amended; the Voting Rights Act, 52 U.S.C. § 10301 *et seq.*, as amended; and the Civil Rights Act, 52 U.S.C. § 10101 *et seq.*, as amended.
- F. Confidentiality of MOU. To the extent allowed by applicable law, this MOU, its contents, and the drafts and communications leading up to the execution of this MOU are deemed

by the parties as "confidential." Any disclosures therefore could be made, if at all, pursuant to applicable laws or court orders requiring such disclosures.

**SIGNATURES**

VRL/Data Provider

State Agency Name: Office of the Texas Secretary of State

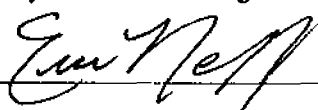
Signature:  Date of Execution: 12/5/25

Authorized Signatory Name Printed: Adam Bitter \_\_\_\_\_

Title: General Counsel \_\_\_\_\_

Requester

Federal Agency Name: Civil Rights Division, U.S. Department of Justice

Signature:  Date of Execution: 12/9/2025

Authorized Signatory Name Printed: Eric Neff \_\_\_\_\_

Title: Acting Chief, Voting Section, Civil Rights Division

---

**From:** Voting Section (CRT) [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=e68131d470c24fbfabf066ea776544b0-\_MB\_VOTSEC]  
**Sent:** 7/15/2025 2:46:31 PM  
**To:** deidrehenderson@utah.gov  
**CC:** ryanowley@utah.gov  
**Subject:** Please see the attached correspondence  
**Attachments:** State of Utah.pdf

Dear Lieutenant Governor Henderson,

Please see the attached correspondence. If you would like to send responsive materials via the Department's secure file-sharing platform, Justice Enterprise File Sharing (JEFS), please let us know and we will send you instructions. Thank you.

**Voting Section**

Civil Rights Division  
U.S. Department of Justice  
950 Pennsylvania Ave NW- 4CON  
Washington, D.C. 20530  
1(800)253-3931



U.S. Department of Justice

Civil Rights Division

Young Section  
950 Pennsylvania Ave, NW - 4CON  
Washington, DC 20530

July 15, 2025

Via Mail and Email

The Honorable Deidre Henderson  
Lieutenant Governor  
P.O. Box 142220  
Salt Lake City, UT 84114-2220  
[deidrehenderson@utah.gov](mailto:deidrehenderson@utah.gov)

Dear Lieutenant Governor Henderson:

We write to you as the chief election official for the State of Utah to request information regarding the state's procedures for complying with the statewide voter registration list maintenance provisions of the National Voter Registration Act ("NVRA"), 52 U.S.C. § 20501 *et seq.*

Please provide a list of the election officials who are responsible for implementing Utah's general program of voter registration list maintenance from November 2022 through receipt of this letter, including those responsible officials not employed by your office (such as local election officials) who are also involved in that effort. Please also provide a description of the steps that you have taken, and when those steps were taken, to ensure that the state's list maintenance program has been properly carried out in full compliance with the NVRA.

The NVRA requires each state and the District of Columbia to make available for inspection "all records concerning the implementation of programs and activities conducted for the purpose of ensuring the accuracy and currency of official lists of eligible voters." 52 U.S.C. § 20507(i)(1). Section 11 of the NVRA authorizes the Attorney General to bring NVRA enforcement actions. *See* 52 U.S.C. § 20510.

Pursuant to Section 20507(i) of the NVRA, the Attorney General requests that you produce for inspection the following records:

The current electronic copy of Utah's computerized statewide voter registration list ("statewide voter registration list") as required by Section 303(a) of the Help America Vote Act. Please include all fields contained within the list. Please produce each list in a .xls, .csv, or delimited-text file format. Please specify what delimiter is used, if applicable, or provide a file layout along with a database user manual, coding list, or other materials that define or explain how a voter record is coded into the statewide voter registration list and reported in the electronic copy of the statewide voter registration list.

Additionally, please provide the following information in electronic form. The time period for these requests is close of registration for the November 2022 general election through the close of registration for the November 2024 general election, the same time period as the most recent report from the Election Assistance Commission's Election Administration and Voting Survey ("EAVS"). If you are unable to provide the data, please explain why the data is not available.

1. A review of the most recent EAVS report shows that Utah has the lowest rate in the nation for voter registration records removed from the voter registration rolls. Only four of Utah's twenty-nine counties provided data regarding removals in response to Question A12a. Please supply the data for the twenty-five remaining counties. Additionally, please explain what actions the State is taking to ensure that voters who should not be on the voter roll are being removed.
2. No data was listed for any county in Utah in the EAVS survey for Question A3d, which asks for information regarding registration transactions submitted by persons already registered to vote. Please provide the data on duplicate registrations for each county in Utah. If such registrations were merged or linked with another record, please provide that information. Additionally, please explain Utah's process for determining duplicates and what happens to the duplicate registrations.
3. Most counties in Utah reported no data for Questions A10b through A10f, which track the outcome of Confirmation Notices that were mailed to registrants. Only six counties provided data for any category and only two counties provided data for all categories. The information on confirmation notices that Utah did provide indicates that those reporting counties generally did not know the result of the confirmation notice. 180,061 (65.8%) of the Result of Confirmation Notice were listed as "not categorized." Please provide the data for each county in Utah for Questions A10b through A10f.
4. Most counties in Utah provided no data on the reasons that voters were removed from the registration rolls, as is requested by Questions A12b through A12h. Only two counties in Utah reported data for voters removed because they moved outside the jurisdiction. Only one county reported data for voters removed because they failed to respond to a sent confirmation notice and failed to vote in the two most recent federal elections. All other categories – including removal of deceased voters, voter's request for removal, felony, and mental incompetence – had no data reported for any county. Please provide the data for each county in Utah for Questions A12b through A12h.
5. In response to Question A12e, Utah reported an aggregate total of 45,342 registrants removed for failure to return confirmation notices. This number is 263.7% of all voters removed from the state registration list, which Utah reported as 17,196. Please provide an explanation for the discrepancy.

Please provide a description of the steps that Utah has taken, and when those steps were taken, to identify registered voters who are ineligible to vote as well as the procedures the state used to remove those ineligible voters from the registration list. Please identify the number of registered

voters identified as ineligible to vote for the time period of the close of registration for the November 2022 general election through present for each of the following reasons:

1. Non-citizen
2. Adjudicated incompetent
3. Felony conviction

For each of those voters identified in categories 1-3 above, provide their registration information on the statewide voter registration list, including their vote history.

Please provide this information within 14 days of the date of this letter. The information and materials may be sent by encrypted email to [voting.section@usdoj.gov](mailto:voting.section@usdoj.gov) or via the Department's secure file-sharing system, Justice Enterprise File Sharing (JEFS).

Should further clarification be required, please contact Maureen Riordan at [maureen.riordan2@usdoj.gov](mailto:maureen.riordan2@usdoj.gov). We look forward to your assistance in advance.

Sincerely,



---

Michael E. Gates  
Deputy Assistant Attorney General  
Civil Rights Division

Maureen Riordan  
Acting Chief, Voting Section  
Civil Rights Division

cc: Ryan Cowley  
Director of Elections  
350 N. State Street, Suite 200  
Salt Lake City, UT 84114-2220  
[ryancowley@utah.gov](mailto:ryancowley@utah.gov)

---

**From:** Voting Section (CRT) [/o=ExchangeLabs/ou=Exchange Administrative Group (FYDIBOHF23SPDLT)/cn=Recipients/cn=e68131d470c24fbfabf066ea776544b0-\_MB\_VOTSEC]  
**Sent:** 8/1/2025 7:10:35 PM  
**To:** Ryan Cowley [ryancowley@utah.gov]  
**CC:** deidrehenderson@utah.gov  
**Subject:** RE: [EXTERNAL] Re: Please see the attached correspondence  
**Attachments:** JEFS\_External Users Agreement.pdf

Dear Mr. Cowley,

The attached form is required to provide access to the JEFS system. On page 1, please fill out the following fields: First Name, Middle Initial, Last name, Organization/Company, Email Address, Address, Zip code, Citizenship of (Country), and Phone number.

After reviewing the remaining pages, please check the box on page 1 regarding Rules of Behavior and sign pages 5-7.

A separate form is required for each person intending to upload documents.

Please let us know if you have any questions.

#### **Voting Section**

Civil Rights Division  
U.S. Department of Justice  
950 Pennsylvania Ave NW- 4CON  
Washington, D.C. 20530  
1(800)253-3931

---

**From:** Ryan Cowley <ryancowley@utah.gov>  
**Sent:** Thursday, July 31, 2025 6:06 PM  
**To:** Voting Section (CRT) <Voting.Section@usdoj.gov>  
**Cc:** deidrehenderson@utah.gov  
**Subject:** [EXTERNAL] Re: Please see the attached correspondence

Maureen, attached is the full response to Mr. Gates letter dated July, 15, 2025. Please send us instructions on how to upload the voter file referenced in the letter using the Justice Enterprise File Sharing system.

Thank you,



**Ryan Cowley** | Director of Elections  
OFFICE OF LIEUTENANT GOVERNOR  
DEIDRE M. HENDERSON  
[LTGOVERNOR.UTAH.GOV](http://LTGOVERNOR.UTAH.GOV)  
801-538-1041

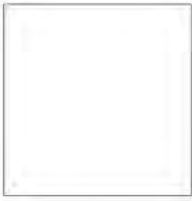
On Tue, Jul 29, 2025 at 4:59 PM Ryan Cowley <[ryancowley@utah.gov](mailto:ryancowley@utah.gov)> wrote:

Maureen, this email is being sent to you in response to the letter from Mr. Gates dated July 15, 2025.

Please be assured that the state of Utah is in compliance with federal election law including NVRA, and has implemented safe, secure, and timely safeguards and processes for maintaining voter registration lists.

Your request has been received, and an additional response will be provided in the near future.

Thank you,



**Ryan Cowley** | Director of Elections  
OFFICE OF LIEUTENANT GOVERNOR  
DEIDRE M. HENDERSON  
[LTGOVERNOR.UTAH.GOV](http://LTGOVERNOR.UTAH.GOV)  
801-538-1041

On Tue, Jul 15, 2025 at 8:46 AM Voting Section (CRT) <[Voting.Section@usdoj.gov](mailto:Voting.Section@usdoj.gov)> wrote:

Dear Lieutenant Governor Henderson,

Please see the attached correspondence. If you would like to send responsive materials via the Department's secure file-sharing platform, Justice Enterprise File Sharing (JEFS), please let us know and we will send you instructions. Thank you.

### **Voting Section**

Civil Rights Division

U.S. Department of Justice

950 Pennsylvania Ave NW- 4CON

Washington, D.C. 20530

1(800)253-3931

Civil Rights Division, Justice Enterprise File Sharing System (JEFS)  
 Account Request and Approval Form  
 Non-Civil Rights Division User

## JEFS Account Request Form for External non-DOJ Users

Account Type:	<input checked="" type="checkbox"/> User (JEFS - Application Users)	JEFS is strictly for Department of Justice (DOJ) official business.	
DOJ Staff Name (Sponsor)		Date of Request	
Request Type: User Account	<input type="checkbox"/> Grant or Modify Access	<input type="checkbox"/> Remove Access	
Request Type: Folder	<input type="checkbox"/> Grant or Modify Access	<input type="checkbox"/> Remove Access	

NOTE: Please include any additional information here. (special instructions, folder name(s), etc.)

External User Information			To be checked by Account User:	
First Name	Middle Initial	Last Name	<input type="checkbox"/> I have read and agree to abide by the Rules of Behavior as described in the attached pages.	
Organization / Company		Email Address		
Address (Street, City, State)		Zip code		
Sponsoring Component		Citizenship of (Country)	Phone Number	
Approving Official (Component DSO or Manager)				
Name (Print or Type)			Title	
Approver Signature				
Approving Official JEFS (To be signed by JEFS Support Team)				
Name (Print or Type)			Title	
Approver Signature				

## JEFS Account Request Form for External non-DOJ Users

### Terms and Conditions

Department of Justice (DOJ), Civil Rights Division Terms and Conditions for JEFs Users

#### Introduction

The intent of the Terms and Conditions is to summarize for you, a user of DOJ Information Technology resources, the applicable laws and requirements from various Federal and DOJ documents. These include, but are not limited to, the Office of Management and Budget (OMB) Circular A-130, OMB M-17-12, OMB M-16-24, DOJ Order 2640.2 (series), DOJ Order 2740.1 (series), and the DOJ Cybersecurity Standard.

To remain compliant with all applicable Federal laws, regulations, and DOJ Standards, the Department reserves the right to update these terms and conditions at any time. Please direct all questions relating to the terms and conditions to your Point of Contact (POC) or the Litigation Support Group Case Manager.

#### Who is covered by these rules?

These rules apply to Litigation Consultants, Expert Witnesses, Mediators, and Non-Civil Rights Division Users providing services to DOJ. They also apply to any other persons using DOJ Information Technology or accessing DOJ systems under formally established agreements. These rules are written for the vast majority of people for the vast majority of time. However, some people (e.g. Investigators) may be exempt from a specific item for a specific situation when performing their official duties and with proper authorization. In a similar manner, equipment and/or software limitations may prevent operation in accordance with some of these rules.

These situations must be documented, the risks accepted, and the applicable processes approved by the system Authorizing Official. All users are required to review and provide signature or electronic verification acknowledging compliance with these rules.

#### What are the penalties for noncompliance?

*Non-compliance with requirements will be enforced through sanctions commensurate with the infraction. Actions and penalties may include a verbal or written warning, temporary suspension of system access, permanent revocation, civil, criminal, financial, and imprisonment depending on the severity of the violation. (We will not deal with any classified information)*

Unauthorized browsing or inspection of Federal Taxpayer Information (Internal Revenue Code Sec. 7213A) is punishable with a fine of up to \$1,000 and/or up to one year imprisonment. Unauthorized disclosure of Tax Return information (Internal Revenue Code Sec. 7213) is a felony punishable with a fine of up to \$5,000 and/or up to five years in prison. In addition to these penalties, any Federal employee convicted under Sec. 7213 or Sec. 7213A will be dismissed from employment.

## JEFS Account Request Form for External non-DOJ Users

### User Security Guide

#### Your responsibilities as an external user:

- Comply with all Federal laws and Department and Component policies and requirements. Use DOJ information and information systems for lawful, official use, and authorized purposes only.
- Read and accept the DOJ security warning banner that appears prior to logging onto the system.
- Screen-lock or log off your computer when JEFS is no longer in use.
- Do not post Department information on cloud-based services unless approved.
- Do not post Department information for official business on public websites or social media unless explicitly authorized for your official duties. (e.g., Public Affairs Office)
- Do not post information on social media or public websites that allows unauthorized users to infer or obtain non-public information (system account information, personal identifiable information (PII), project status, etc.).
- Protect and safeguard all DOJ information commensurate with the sensitivity and value of the data at risk, including encrypting all PII being sent to third parties.
- Protect and safeguard all DOJ information and information systems from unauthorized access; unauthorized or inadvertent modification, disclosure, damage, destruction, loss, theft, denial of service; and improper sanitization or use.
- JEFS users shall ensure that all DOJ data are stored on authorized removable media (e.g., thumb drives, removable hard drives, and CD/DVD), laptops, tablets, and mobile devices (e.g., smartphones and netbooks) is encrypted with a Department-approved solution unless the Department's Chief Information Officer (CIO) or designee approves a waiver from the Department policy.
- Handle all Department data as Sensitive unless designated as non-Sensitive by your Attorney Point of Contact (POC) or the Litigation Support Group Case Manager.
- Report any anomalous or unusual behavior, and discovered or suspected security incidents to your appropriate point of contact (POC) (e.g., Civil Rights Attorney, Litigation Support Group (LSG) Case Manager, LSG Office at 202-514-4224, or Justice Security Operations Center [JSOC], DOJCert@usdoj.gov).
- The email address associated with your JEFS account should be attributable by another party or organization (e.g., .org, .com, .mil, .gov) controlled by only you and not shared with anyone, even family members.

Do not attempt to circumvent or test the security controls of the system.

## JEFS Account Request Form for External non-DOJ Users

### Passwords

- Change the default password upon receipt from a system administrator.
- Do not share account passwords with anyone.
- Avoid using the same password for multiple accounts.

### Software

- Do not copy or distribute intellectual property without permission or license from the copyright owner (e.g., music, software, documentation, and other copyrighted materials).
- Use DOJ-licensed and authorized software only.
- Do not install or update software on the File Sharing System unless specifically authorized.
- Do not attempt to access any electronic audit trails that may exist on the File Sharing System computer.

At the completion of your service, please properly dispose of any case related data Contact your Attorney Point of Contact (POC) or the Litigation Support Group Case Manager for more guidance.

### Mobile Computing & Remote Access

- When utilizing the Litigation Support System, connect to a secure wireless network (password protected) and take precautionary measures to prevent the compromise of DOJ data when insecure wireless networks must be used. **Never connect to open wireless networks that require no passwords.**
- Ensure the confidentiality of government information from a non-Government Furnished Equipment (GFE) client (public or private). This includes the following:
  - Non-GFE devices and computers must have updated antivirus, local firewall, updated Operating System security patches and software patched levels.
  - In addition, all wireless access to DOJ networks must be from a WI-FI Protected Access 2 (WPA2) or higher encrypted wireless network with password protection.
  - Do not download documents or files public computers.
  - Purge documents and files when finished on a non-GFE private will be held responsible for the compromise of Government information through negligence or a willful act.

## JEFS Account Request Form for External non-DOJ Users

### Personally Identifiable Information (PII)

Verify that each computer-readable data extract containing sensitive PII data has been erased within 90 days of origination or that its use is still required. Contact your Attorney Point of Contact (POC) or the Litigation Support Group Case Manager.

Safeguard against breaches of information involving PII, which refers to information that can be used alone or combined with other information that can distinguish or trace an individual's identity --such as a name, social security number, biometric records, the date and place of birth, mother's maiden name, etc.

Report all breaches of information involving PII to your Attorney Point of Contact (POC) or the Litigation Support Group Case Manager as soon as possible.

### Signature Block

I acknowledge receipt of, understand my responsibilities as identified in, and will comply with the DOJ Civil Rights Division Terms and Conditions for External Users. This includes my responsibility to ensure protection of PII that I may handle.

---

Your Signature

---

Date

---

Your Printed Name

---

Organization/Component

*[Note: For DOJ employees, statement of acknowledgement may be made by signature of the Terms and Conditions for General Users are provided in hard copy or by email.]*

## JEFS Account Request Form for External non-DOJ Users

### Confidentiality Agreement

In consideration of being provided access to the Department of Justice (DOJ), Civil Rights Division Justice Enterprise File Sharing System (JEFS), the User hereby agrees to the following:

The provisions of this agreement shall apply to and be binding upon the User, the User's company, business, employees, agents, officers, successors and assigns, and any person acting upon behalf of the User in relation to the DOJ case(s) or project(s) he or she is authorized to access.

Except as required by law, as otherwise provided in this agreement, or as directed in writing by the Department of Justice, no information obtained, developed, gathered, or created as a result of work performed in connection with this matter, including any training materials or guidance concerning the System, shall be provided or disclosed orally, in writing, or in any other form, including the transmission of electronic data, to any third party or person who is not a part of this agreement. In any case in which disclosure of such information is or may be appropriate, no disclosures shall be made without prior written approval of the Department of Justice. This prohibition includes, but is not limited to communications with any person representing the media, any industry representatives, and any colleagues or fellow researchers. Disclosures may be made to persons who have signed and filed Confidentiality Agreements with the Department of Justice in connection with this case or project, as well as your management, supervisory, or support personnel as they may be necessary to execute your role as an authorized User in connection with this case or project.

Except as required by law, as otherwise provided in this agreement, or as directed by the Department of Justice, all documents, information, electronic data, or other work obtained, developed, gathered, or created as a result of System access, including documents or other information provided by the United States or other parties, shall be treated as privileged Sensitive But Unclassified (SBU) information. The User shall not reveal such materials to any third party or person without prior written approval from the Department of Justice, except for those persons who have signed and filed Confidentiality Agreements with the Department of Justice in connection with this case or project.

Should any documents, information, or electronic data, provided, obtained, developed, gathered, or created in connection with this System be lost, discovered missing, or mistakenly or inadvertently turned over without DOJ consent to an unauthorized person or third party, the User shall immediately report the details of such incident to the lead Department of Justice attorney point of contact responsible for this case or matter and the Litigation Support Group (LSG) Case Manager assigned to this case or project. In the event the User receives any requests in any form for such information, the User shall immediately notify the lead Department of Justice attorney point of contact and LSG Case Manager and await and follow DOJ instructions on how to proceed.

The User is responsible for notifying the LSG Case Manager when his or her involvement in this case or matter has concluded, at which time the User will request termination of access to the System. The User shall deliver upon request, within 30 days of notification that System access has been terminated, all documents, electronic data, and other information provided, obtained, developed, gathered, or created in connection with System access and related to the case or project he or she was supporting to the Department of Justice.

Notwithstanding the terms of this agreement, documents created by third-parties and gathered as evidence in litigation that are stored as images on the System will not be deemed to be privileged or confidential by virtue of this agreement. Nothing in this agreement limits the authority of agents or attorneys assigned to the matters in which that evidence is, was or will be collected from disclosing that evidence to witnesses, courts, or other persons who are not parties to this agreement in any manner authorized by law as necessary for those assigned agents and attorneys to discharge their duties in investigating and prosecuting the matters.

Should you have any questions regarding these documents or your responsibilities, please contact your Litigation Support Group Case Manager.

### Acknowledgement Block

I acknowledge receipt of the "CIVIL RIGHTS DIVISION, JUSTICE ENTERPRISE FILE SHARING SERVER User Security Guide & Confidentiality Agreement" and understand my responsibilities as identified. This includes my responsibility to ensure the protection of PII that I may handle.

\_\_\_\_\_  
Your Signature

\_\_\_\_\_  
Date

\_\_\_\_\_  
Your Printed Name

\_\_\_\_\_  
Organization/Component

## JEFS Account Request Form for External non-DOJ Users

### Privacy Statement

In order for the Department of Justice Civil Rights Division to provide you with access to its document review system, please complete the attached form. Information gathered from this form will be used solely to confirm the identity and eligibility of the individuals requesting access to the system owned by the Civil Rights Division of the United States Department of Justice. Email, phone and computer information gathered will be used solely to create an account that will let the individuals requesting access view, process and/or store electronic information that is the property of the Civil Rights Division.

Failure to provide this information will result in denial of access to the document review system.

This form is not an application for Government employment. Information collected by this form will not be used for or affect any subsequent application for employment with the Federal Government.

The Department of Justice does not collect or use information for commercial marketing.

Information gathered in this form will not be disclosed outside of the Civil Rights Division except where contractors are acting on behalf of the Civil Rights Division, and where the Division may be required by law to disclose information you submit with other agencies for law enforcement purposes in accordance with the Civil Rights Division's routine uses published at 68 Fed. Reg. 47610 (Aug. 11, 2003, <http://edocket.access.gpo.gov/2003/pdf/03-20342.pdf>) or to protect the Division from security threats.

Electronically submitted information is maintained and destroyed according to the principles of the Federal Records Act and the regulations and records schedules of the National Archives and Records Administration, and in some cases may be covered by the Privacy Act and subject to the Freedom of Information Act (FOIA). A discussion of the FOIA can be found at [http://www.justice.gov/oip/foia\\_guide09.htm](http://www.justice.gov/oip/foia_guide09.htm) and a discussion about the Privacy Act can be found at <http://www.justice.gov/opcl/privacyact1974.htm>.

I acknowledge receipt of these Terms and Conditions and understand my responsibilities as identified in the DOJ Terms and Conditions. This includes my responsibility to ensure protection of PII that I may handle.

---

Signature

Date

---

Printed Name

---

Component and Office

Clear Form

Print Form

---

**From:** Neff, Eric (CRT) [Eric.Neff@usdoj.gov]  
**Sent:** 12/2/2025 3:37:03 PM  
**To:** ryancowley@utah.gov  
**CC:** deidrehenderson@utah.gov  
**Subject:** Full Voter Roll List with MOU  
**Attachments:** VRLData Sharing Agreement DOJ-UT.pdf; 20250829 Owsley to CRT.pdf; 20250814 Henderson from CRT.pdf

Dear Mr. Crowley,

I am the new point of contact for Voter Roll Maintenance communication. Please see the attached proposed MOU from the Department of Justice. This MOU in our opinion satisfies all reasonable concerns regarding privacy and data security, which you raised in your August 29 letter (attached). This MOU includes a request for compliance within 7 days of receipt of this communication. Compliance requires providing all records requested in previous communications with your Department, most notably our August 14 letter (attached).

Please do not hesitate to contact me with any questions or concerns.

Best,  
Eric

**Eric Neff**

Trial Attorney  
Civil Rights Division  
Department of Justice  
150 M St. NE, Ste. 8-139  
Washington, DC 20002  
Eric.Neff@usdoj.gov  
Cell: 202-532-3628





**U.S. Department of Justice**  
Civil Rights Division

---

**CONFIDENTIAL MEMORANDUM OF UNDERSTANDING**

**I. PARTIES & POINTS OF CONTACT.**

Requester

Federal Agency Name: Civil Rights Division, U.S. Department of Justice

VRL/Data User:

Title:

Address:

Phone:

VRL/Data Provider

State Agency Name:

Custodian:

Title:

Address:

Phone:

The parties to this Memorandum of Understanding (“MOU” or “Agreement”) are the Department of Justice, Civil Rights Division (“Justice Department” or “Department”), and the State of Utah (“You” or “your state”).

**II. AUTHORITY.**

By this Agreement, the State of Utah (“You” or “your state”) has agreed to, and will, provide an electronic copy of your state’s complete statewide Voter Registration List (“VRL” or “VRL/Data”) to the Civil Rights Division of the U.S. Department of Justice (at times referred to as the “Department”). The VRL/Data must include, among other fields of data, the voter registrant’s full name, date of birth, residential address, his or her state driver’s license number or

the last four digits of the registrant's social security number as required under the HAVA to register individuals for federal elections. *See* 52 U.S.C. § 21083(a)(5)(A).

The authorities by which this information is requested by the Department of Justice are:

- National Voter Registration Act of 1993, 52 U.S.C. § 20501, *et seq.*
- Attorney General's authority under Section 11 of the NVRA to bring enforcement actions. *See* 52 U.S.C. § 20510(a).
- Help America Vote Act of 2002, 52 U.S.C. § 20901, *et seq.*
- Attorney General's authority to enforce the Help America Vote Act under 53 U.S.C. § 21111.
- Attorney General authority to request records pursuant to Title III of the Civil Rights Act of 1960 ("CRA"), codified at 52 U.S.C. § 20701, *et seq.*
- The Privacy Act of 1974, 5 U.S.C. § 552a, as amended.

### **III. PURPOSE.**

A VRL is a Voter Registration List pursuant to the NVRA and HAVA, commonly referred to as "voter roll," compiled by a state – often from information submitted by counties – containing a list of all the state's *eligible* voters. Regardless of the basis for ineligibility, ineligible voters do not appear on a state's VRL when proper list maintenance is performed by states. The Justice Department is requesting your state's VRL to test, analyze, and assess states' VRLs for proper list maintenance and compliance with federal law. In the event the Justice Department's analysis of a VRL results in list maintenance issues, insufficiency, inadequacy, anomalies, or concerns, the Justice Department will notify your state's point of contact of the issues to assist your state with curing.

The purpose of this MOU is to establish the parties' understanding as to the security protections for data transfer and data access by the Department of Justice of the electronic copy of the statewide voter registration list, including all fields requested by the Department of Justice.

#### **IV. TIMING OF AGREEMENT – TIME IS OF ESSENCE.**

Although the Justice Department is under no such obligation as a matter of law, because this Agreement is proposed, made, and to be entered into at your state's request as part of your state's transmission of its VRL to the Justice Department, this Agreement is to be fully executed within seven (7) days of the Justice Department presenting this Agreement to you. Both parties agree that no part of this Agreement or execution is intended to, or will, cause delay of the transmission of your state's VRL to the Justice Department for analysis.

#### **V. TIMING OF VRL/DATA TRANSFER.**

You agree to transfer an electronic copy of your state's complete statewide VRL/Data to the Civil Rights Division of the U.S. Department of Justice as described in Section III of this Agreement no later than five (5) business days from the execution of this Agreement, which is counted from the last day of the last signatory.

#### **VI. METHOD OF VRL/DATA ACCESS OR TRANSFER.**

The VRL will be submitted by your state via the Department of Justice's secure file-sharing system, i.e., Justice Enterprise File Sharing (JEFS"). A separate application to use JEFS must be completed and submitted by your state through the Civil Rights Help Desk. JEFS implements strict access controls to ensure that each user can only access their own files. All files and folders are tied to a specific user, and each user has defined permissions that govern how they may interact with those files (e.g., read, write, or read-only).

Whenever a user attempts to access a file or folder, JEFS validates the request against the assigned permissions to confirm that the user is explicitly authorized. This process guarantees that users can only access files and folders only where they have permission. Users are also limited to the authorized type of interaction with each file or folder. Within the Department of Justice, access to JEFS is restricted to specific roles: Litigation Support, IT staff, and Civil Rights Division staff.

## **VII. LOCATION OF DATA AND CUSTODIAL RESPONSIBILITY.**

The parties mutually agree that the Civil Rights Division (also “Department”) will be designated as “Custodian” of the file(s) and will be responsible for the observance of all conditions for use and for establishment and maintenance of security agreements as specified in this agreement to prevent unauthorized use. The information that the Department is collecting will be maintained consistent with the Privacy Act of 1974, 5 U.S.C. § 552a. The full list of routine uses for this collection of information can be found in the Systems of Record Notice (“SORN”) titled, JUSTICE/CRT – 001, “Central Civil Rights Division Index File and Associated Records,” 68 Fed. Reg. 47610-01, 611 (August 11, 2003); 70 Fed. Reg. 43904-01 (July 29, 2005); and 82 Fed. Reg. 24147-01 (May 25, 2017). It should be noted that the statutes cited for routine use include NVRA, HAVA, and the Civil Rights Act of 1960, and the Justice Department is making our request pursuant to those statutes. The records in the system of records are kept under the authority of 44 U.S.C. § 3101 and in the ordinary course of fulfilling the responsibility assigned to the Civil Rights Division under the provisions of 28 C.F.R. §§ 0.50, 0.51.

VRL/Data storage is similar to the restricted access provided on JEFS and complies with the SORN: Information in computer form is safeguarded and protected in accordance with applicable Department security regulations for systems of records. Only a limited number of staff members who are assigned a specific identification code will be able to use the computer to access

the stored information. However, a section may decide to allow its employees access to the system in order to perform their official duties.

All systems storing the VRL data will comply with all security requirements applicable to Justice Department systems, including but not limited to all Executive Branch system security requirements (e.g., requirements imposed by the Office of Management and Budget [OMB] and National Institute of Standards and Technology [NIST]), Department of Justice IT Security Standards, and Department of Justice Order 2640.2F.

#### **VIII. NVRA/HAVA COMPLIANT VOTER REGISTRATION LIST.**

After analysis and assessment of your state's VRL, the Justice Department will securely notify you or your state of any voter list maintenance issues, insufficiencies, inadequacies, deficiencies, anomalies, or concerns, the Justice Department found when testing, assessing, and analyzing your state's VRL for NVRA and HAVA compliance, i.e., that your state's VRL only includes eligible voters.

You agree therefore that within forty-five (45) days of receiving that notice from the Justice Department of any issues, insufficiencies, inadequacies, deficiencies, anomalies, or concerns, your state will clean its VRL/Data by removing ineligible voters and resubmit the updated VRL/Data to the Civil Rights Division of the Justice Department to verify proper list maintenance has occurred by your state pursuant to the NVRA and HAVA.

#### **IX. CONFIDENTIALITY & DEPARTMENT SAFEGUARDS.**

Any member of the Justice Department in possession of a VRL/Data will employ reasonable administrative, technical, and physical safeguards designed to protect the security and confidentiality of such data. Compliance with these safeguards will include secure user authentication protocols deploying either: (i) Two-Factor Authentication ("2FA"), which requires users to go through two layers of security before access is granted to the system; or (ii) the

assignment of unique user identifications to each person with computer access plus unique complex passwords, which are not vendor supplied default passwords.

The Department will activate audit logging for the records, files, and data containing the state's VRL/Data in order to identify abnormal use, as well as to track access control, on computers, servers and/or Devices containing the VRL/Data.

For all devices storing records, files, and data containing the VRL/Data: there is (i) up-to-date versions of system security agent software that includes endpoint protection and malware protection and reasonably up-to-date patches and virus definitions, or a version of such software that can still be supported with up-to-date patches and virus definitions, and is set to receive the most current security updates on a regular basis; and (ii) up-to-date operating system security patches designed to maintain the integrity of the personal information.

For all devices storing records, files, and data containing the VRL/Data: there is (i) controlled and locked physical access for the Device; and (ii) the prohibition of the connection of the Device to public or insecure home networks.

There will be no copying of records, files, or data containing the VRL/Data to unencrypted USB drives, CDs, or external storage. In addition, the use of devices outside of moving the records, files, or data to the final stored device location shall be limited.

Any notes, lists, memoranda, indices, compilations prepared or based on an examination of VRL/Data or any other form of information (including electronic forms), that quote from, paraphrase, copy, or disclose the VRL/Data with such specificity that the VRL/Data can be identified, or by reasonable logical extension can be identified will not be shared by the Department. Any summary results, however, may be shared by the Department.

In addition to the Department's enforcement efforts, the Justice Department may use the information you provide for certain routine, or pre-litigation or litigation purposes including:

present VRL/Data to a court, magistrate, or administrative tribunal; a contractor with the Department of Justice who needs access to the VRL/Data information in order to perform duties related to the Department's list maintenance verification procedures. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. § 552a(m).

**X. LOSS OR BREACH OF DATA.**

If a receiving party discovers any loss of VRL/Data, or a breach of security, including any actual or suspected unauthorized access, relating to VRL/Data, the receiving party shall, at its own expense immediately provide written notice to the producing party of such breach; investigate and make reasonable and timely efforts to remediate the effects of the breach, and provide the producing party with assurances reasonably satisfactory to the producing party that such breach shall not recur; and provide sufficient information about the breach that the producing party can reasonably ascertain the size and scope of the breach. The receiving party agrees to cooperate with the producing party or law enforcement in investigating any such security incident. In any event, the receiving party shall promptly take all necessary and appropriate corrective action to terminate unauthorized access.

**XI. DESTRUCTION OF DATA.**

The Department will destroy all VRL/Data associated with actual records as soon as the purposes of the list maintenance project have been accomplished and the time required for records retention pursuant to applicable law has passed. When the project is complete and such retention requirements by law expires, the Justice Department will:

1. Destroy all hard copies containing confidential data (e.g., shredding);
2. Archive and store electronic data containing confidential information offline in a secure location; and

3. All other data will be erased or maintained in a secured area.

## **XII. OTHER PROVISIONS.**

- A. Conflicts. This MOU constitutes the full MOU on this subject between the Department and your state. Any inconsistency or conflict between or among the provisions of this MOU, will be resolved in the following order of precedence: (1) this MOU and (2) other documents incorporated by reference in this MOU (e.g., transaction charges).
- B. Severability. Nothing in this MOU is intended to conflict with current law or regulation or the directives of Department, or the your state. If a term of this MOU is inconsistent with such authority, then that term shall be invalid but, to the extent allowable, the remaining terms and conditions of this MOU shall remain in full force and effect.
- C. Assignment. Your state may not assign this MOU, nor may it assign any of its rights or obligations under this MOU. To the extent allowable by law, this MOU shall inure to the benefit of, and be binding upon, any successors to the Justice Department and your state without restriction.
- D. Waiver. No waiver by either party of any breach of any provision of this MOU shall constitute a waiver of any other breach. Failure of either party to enforce at any time, or from time to time, any provision of this MOU shall not be construed to be a waiver thereof.
- E. Compliance with Other Laws. Nothing in this MOU is intended or should be construed to limit or affect the duties, responsibilities, and rights of the User Agency under the National Voter Registration Act, 52 U.S.C. § 20501 *et seq.*, as amended; the Help America Vote Act, 52 U.S.C. § 20901 *et seq.*, as amended; the Voting Rights Act, 52 U.S.C. § 10301 *et seq.*, as amended; and the Civil Rights Act, 52 U.S.C. § 10101 *et seq.*, as amended.
- F. Confidentiality of MOU. To the extent allowed by applicable law, this MOU, its contents, and the drafts and communications leading up to the execution of this MOU are deemed

by the parties as “confidential.” Any disclosures therefore could be made, if at all, pursuant to applicable laws or court orders requiring such disclosures.

**SIGNATURES**

VRL/Data Provider

State Agency Name:

Signature: \_\_\_\_\_ Date of Execution: \_\_\_\_\_

Authorized Signatory Name Printed: \_\_\_\_\_

Title: \_\_\_\_\_

Requester

Federal Agency Name: Civil Rights Division, U.S. Department of Justice

Signature: \_\_\_\_\_ Date of Execution: \_\_\_\_\_

Authorized Signatory Name Printed: \_\_\_\_\_

Title: \_\_\_\_\_



State of Utah

SPENCER J. COX  
Governor

DEIDRE M. HENDERSON  
Lieutenant Governor

## Office of the Lieutenant Governor

RYAN COWLEY  
*Director of Elections*

SHELLY JACKSON  
*Deputy Director of Elections*

August 29, 2025

Michael E. Gates  
Deputy Assistant Attorney General  
U.S. Department of Justice Civil Rights Division

Sent via email: [Michael.Gates@usdoj.gov](mailto:Michael.Gates@usdoj.gov)

Mr. Gates:

This letter is in response to the Department of Justice's (DOJ) request to the Lieutenant Governor for sensitive voter information, dated August 14, 2025, and follow up email on August 22, 2025. We are grateful for the additional time to prepare a response. To facilitate a clear and constructive dialogue, we kindly request clarification regarding the purpose of these requests and how the records might be utilized by the DOJ.

### Background

Utah's statewide voter-registration list ("VRL") contains highly sensitive and personally identifiable voter information. On July 15, you requested "all fields" of the VRL. We responded on July 31 with an offer to produce certain publicly available voter data. But in your August 14 letter, you indicated that our initial offer to produce this publicly available information was insufficient. Instead, you renewed your request for the entire VRL and specified that our production should include voters' full names, dates of birth, and residential addresses, as well as their state driver's license numbers or the last four digits of their social security numbers. You have asked us to respond by today.

### Purpose

We seek to better understand some aspects of the requests. Notably, the initial letter referenced the National Voter Registration Act's ("NVRA") requirement for public inspection of certain records to verify the accuracy of Utah's official list of eligible voters. But the second letter outlined a different focus, this time requesting the VRL under the Civil Rights Act ("CRA")—to

ascertain Utah’s compliance with the list maintenance requirements of the NVRA and HAVA.” The second letter also referenced DOJ’s confidentiality obligations under the CRA, but those confidentiality obligations are imposed only by the CRA, not by any statute mentioned in the first letter.

Given these variations in purpose and authority, we kindly request clarification on the specific objectives behind these requests and the applicable legal authority. Our goal is to ensure that we fully understand and address the DOJ’s concerns while respecting all relevant state and federal legal requirements.

### Intended Use

We also request clarity regarding how the requested information may be used or shared. Initially, the authority cited for the request was a statute allowing inspection of individual records. We’d like to understand whether our entire VRL—containing highly sensitive personally identifiable information—will be made available to the public, as implied by the references in the first letter. And if the DOJ considers the VRL to have been produced under the CRA (as the second letter suggests), we would appreciate clarification on which government agencies might receive the VRL from the DOJ. If any groups, agencies, or entities outside of the DOJ may have, or will be given, access to this data, we’d like clarification on both the authority and purpose for that access, as well as how the private information will be protected in accordance with the Privacy Act.

### Request for Clarification

As demonstrated above, the DOJ has not clearly articulated the specific legal authority supporting its request for Utah’s VRL containing personal identifying information of all Utah voters. Additionally, it remains unclear whether the VRL, if provided, would be maintained as strictly confidential and not disseminated to other governmental agencies or outside entities. Before proceeding with further legal analysis regarding the appropriateness of releasing the VRL, we kindly request clarification on the following points:

- What explicit authority does the DOJ rely on to request the entire VRL, including all personal identifying information of Utah voters? If this authority is based on the NVRA, should we be concerned that the NVRA does not appear to impose strict confidentiality requirements on the DOJ? Conversely, if the authority is based on the CRA, which does impose confidentiality obligations on the DOJ, under what circumstances might the DOJ share the VRL with other governmental agencies?
- Will the DOJ share the VRL with any non-governmental individuals or entities, such as advocacy organizations?

- Does the DOJ intend to match any information in the VRL against any other databases, whether federal, state, or non-governmental? If so, please specify which databases and the purposes of such comparisons.
- What is the relevant timeframe for this request? The initial communication specified a period from the close of registration for the November 2022 general election through the close of registration for the November 2024 election. This timeframe begins approximately 36 months ago. But the CRA—cited in the second letter as the authority for this request—imposes recordkeeping obligations for only 22 months following the date of any election in which a federal race is involved. Since the November 2022 election falls outside this 22-month period, we'd appreciate assistance identifying the relevant timeframe.

We are committed to working together to address these questions effectively. We appreciate your assistance in clarifying these matters to ensure compliance and mutual understanding. Please contact me with questions.

Sincerely,

Ryan Cowley  
Director of Elections



U.S. Department of Justice

Civil Rights Division

---

Office of the Assistant Attorney General

Washington, D.C. 20530

August 14, 2025

Via Mail and Email

The Honorable Deidre Henderson  
Lieutenant Governor  
P.O. Box 142220  
Salt Lake City, UT 84114-2220  
[deidrehenderson@utah.gov](mailto:deidrehenderson@utah.gov)

Re: **Complete Utah's Voter Registration List with All Fields**

Lieutenant Governor Henderson:

We have received Utah's statewide voter registration list ("VRL"). However, as the Attorney General requested, the electronic copy of the statewide VRL must contain *all fields*, including the registrant's full name, date of birth, residential address, his or her state driver's license number or the last four digits of the registrant's social security number as required under the Help America Vote Act ("HAVA")<sup>1</sup> to register individuals for federal elections. *See* 52 U.S.C. § 21083(a)(5)(A)(i).

We have requested Utah's VRL to assess your state's compliance with the statewide VRL maintenance provisions of the National Voter Registration Act ("NVRA"), 52 U.S.C. § 20501, *et seq.* Our request is pursuant to the Attorney General's authority under Section 11 of the NVRA to bring enforcement actions. *See* 52 U.S.C. § 20501(a).

The Help America Vote Act ("HAVA"), 52 U.S.C. § 20501, *et seq.*, also provides authority for the Justice Department to seek the State's VRL via Section 401, which makes the Attorney General solely responsible for actions to enforce HAVA's computerized statewide Voter Registration List requirements. *See* 52 U.S.C. § 21111; *see also Brunner v. Ohio Republican Party*, 555 U.S. 5, 6 (2008) (*per curiam*) (finding there is no private right of action to enforce those requirements in HAVA).

---

<sup>1</sup> In charging the Attorney General with enforcement of the voter registration list requirements in the HAVA and in the NVRA, Congress plainly intended that Justice Department be able to conduct an independent review of each state's list. Any statewide prohibitions are clearly preempted by federal law.

In addition to those authorities, the Attorney General is also empowered by Congress to request records pursuant to Title III of the Civil Rights Act of 1960 (“CRA”), codified at 52 U.S.C. § 20701, *et seq.* Section 301 of the CRA requires state and local officials to retain and preserve records related to voter registration and other acts requisite to voting for any federal office for a period of 22 months after any federal general, special or primary election. *See* 52 U.S.C. § 20701.

Section 303 of the CRA provides, in pertinent part, “Any record or paper required by section 20701 of this title to be retained and preserved shall, upon demand in writing by the Attorney General or his representative directed to the person having custody, possession, or control of such record or paper, be made available for inspection, reproduction, and copying at the principal office of such custodian by the Attorney General or his representative...” 52 U.S.C. § 20703.

Pursuant to the foregoing authorities, including the CRA, the Attorney General is demanding an electronic copy of Utah’s complete and current VRL. The purpose of the request is to ascertain Utah’s compliance with the list maintenance requirements of the NVRA and HAVA.

When providing the electronic copy of the statewide VRL, Utah must ensure that it contains *all fields*, which includes the registrant’s full name, date of birth, residential address, his or her state driver’s license number or the last four digits of the registrant’s social security number as required under the Help America Vote Act (“HAVA”)<sup>2</sup> to register individuals for federal elections. *See* 52 U.S.C. § 21083(a)(5)(A)(i).

To the extent there are privacy concerns, the voter registration list is subject to federal privacy protections. Section 304 of the CRA provides the answer:

Unless otherwise ordered by a court of the United States, neither the Attorney General nor any employee of the Department of Justice, nor any other representative of the Attorney General, shall disclose any record or paper produced pursuant to this chapter, or any reproduction or copy, except to Congress and any committee thereof, governmental agencies, and in the presentation of any case or proceeding before any court or grand jury.

Moreover, HAVA specifies that the “last 4 digits of a social security number . . . shall not be considered a social security number for purposes of section 7 of the Privacy Act of 1974” (5 U.S.C. § 552a note); 52 U.S.C. § 21083(c). In addition, any prohibition of disclosure of a motor vehicle record contained in the Driver’s License Protection Act, codified at 18 U.S.C. § 2721(b)(1), is exempted when the disclosure is for use by a government agency in carrying out the government agency’s function to accomplish its enforcement authority as the Justice Department is now doing. That said, all data received from you will be kept securely and treated consistently with the Privacy Act.

---

<sup>2</sup> In charging the Attorney General with enforcement of the voter registration list requirements in the HAVA and in the NVRA, Congress plainly intended that Justice Department be able to conduct an independent review of each state’s list. Any statewide prohibitions are clearly preempted by federal law.

In charging the Attorney General with enforcement of the voter registration list requirements in HAVA and in the NVRA, Congress plainly intended that DOJ be able to conduct an independent review of each state's list. Any statewide prohibitions are preempted by federal law.

To that end, please provide the requested electronic Voter Registration List<sup>3</sup> to the Justice Department within seven days or by August 21, 2025.

The information and materials may be sent by encrypted email to [voting.section@usdoj.gov](mailto:voting.section@usdoj.gov) or via the Department's secure file-sharing system, Justice Enterprise File Sharing ("JEFS"). Should further clarification be required, please contact Maureen Riordan at [maureen.riordan2@usdoj.gov](mailto:maureen.riordan2@usdoj.gov).

Regards,



Harmeet K. Dhillon  
Assistant Attorney General  
Civil Rights Division

cc: Ryan Cowley  
Director of Elections  
350 N. State Street, Suite 200  
Salt Lake City, UT 84114-2220  
[ryancowley@utah.gov](mailto:ryancowley@utah.gov)

---

<sup>3</sup> Containing *all fields*, which includes either the registrant's full name, date of birth, residential address, his or her state driver's license number or the last four digits of the registrant's social security number as required by HAVA.



U.S. Department of Justice

Civil Rights Division

---

Office of the Assistant Attorney General

Washington, D.C. 20530

September 8, 2025

Via Mail and Email

The Honorable Sarah Copeland Hanzas  
Secretary of State  
128 State Street  
Montpelier, VT 05633  
[Sarah.CopelandHanzas@vermont.gov](mailto:Sarah.CopelandHanzas@vermont.gov)

Re: **Request for Complete Vermont's Voter Registration List with All Fields**

Dear Secretary Copeland Hanzas:

We write to you as the chief election official for the State of Vermont concerning your State's compliance with the statewide voter registration list maintenance provisions of the National Voter Registration Act ("NVRA"), 52 U.S.C. § 20501 *et seq.*, and the Help America Vote Act ("HAVA"), 52 U.S.C. § 20901, *et seq.* Please provide a copy of Vermont's statewide voter registration list ("VRL") within fourteen days of the date of this letter.

The electronic copy of the statewide VRL should contain *all fields*, which means, your state's VRL must include the registrant's full name, date of birth, residential address, his or her state driver's license number or the last four digits of the registrant's social security number as required under HAVA<sup>1</sup> to register individuals for federal elections. *See* 52 U.S.C. § 21083(a)(5)(A)(i).

We request Vermont's VRL to assess your state's compliance with the statewide VRL maintenance provisions of the NVRA. Our request is pursuant to the Attorney General's authority under Section 11 of the NVRA to bring enforcement actions. *See* 52 U.S.C. § 20510(a).

HAVA also provides authority for the Justice Department to seek the State's VRL via Section 401, which makes the Attorney General solely responsible for actions to enforce HAVA's computerized statewide voter registration list requirements. *See* 52 U.S.C. § 21111; *see also Brunner*

---

<sup>1</sup> In charging the Attorney General with enforcement of the voter registration list requirements in the HAVA and in the NVRA, Congress plainly intended that DOJ be able to conduct an independent review of each state's list. Any statewide prohibitions are clearly preempted by federal law.

v. *Ohio Republican Party*, 555 U.S. 5, 6 (2008) (*per curiam*) (finding no private right of action to enforce HAVA requirements).

In addition to those authorities, the Attorney General is also empowered by Congress to request records pursuant to Title III of the Civil Rights Act of 1960 (“CRA”), codified at 52 U.S.C. § 20701, *et seq.* Section 301 of the CRA requires state and local officials to retain and preserve records related to voter registration and other acts requisite to voting for any federal office for a period of twenty-two months after any federal general, special or primary election. *See* 52 U.S.C. § 20701.

Section 303 of the CRA provides, in pertinent part, “Any record or paper required by section 20701 to be retained and preserved shall, upon demand in writing by the Attorney General or his representative directed to the person having custody, possession, or control of such record or paper, be made available for inspection, reproduction, and copying at the principal office of such custodian by the Attorney General or his representative...” *See* 52 U.S.C. § 20703.

Pursuant to the foregoing authorities, including the CRA, the Attorney General is requesting an electronic copy of Vermont’s complete and current VRL. The purpose of this request is to ascertain Vermont’s compliance with the list maintenance requirements of the NVRA and HAVA.

To the extent there are privacy concerns, the voter registration list is subject to federal privacy protections. Section 304 of the CRA provides the answer:

Unless otherwise ordered by a court of the United States, neither the Attorney General nor any employee of the Department of Justice, nor any other representative of the Attorney General, shall disclose any record or paper produced pursuant to this chapter, or any reproduction or copy, except to Congress and any committee thereof, governmental agencies, and in the presentation of any case or proceeding before any court or grand jury.

52 U.S.C. § 20704. HAVA specifies that the “last 4 digits of a social security number . . . shall not be considered to be a social security number for purposes of section 7 of the Privacy Act of 1974” (5 U.S.C. § 522a note); 52 U.S.C. § 21083(c). In addition, any prohibition of disclosure of a motor vehicle record contained in the Driver’s License Protection Act, codified at 18 U.S.C. § 2721(b)(1), is exempted when the disclosure is for use by a government agency in carrying out the government agency’s function to accomplish its enforcement authority as the Justice Department is now doing. That said, all data received from you will be kept securely and treated consistently with the Privacy Act explained at [Civil Rights Division - Department of Justice - Privacy Policy](#)<sup>2</sup>.

Please provide the requested electronic VRL<sup>3</sup> to the Justice Department fourteen days from the date of this letter. The information and materials may be sent by encrypted email to [voting.section@usdoj.gov](mailto:voting.section@usdoj.gov) or via the Department’s secure file-sharing system, Justice Enterprise File

---

<sup>2</sup> Available at: <https://civilrights.justice.gov/privacy-policy#:~:text=Our%20Statutes-Privacy%20Act%20Statement,the%20scope%20of%20our%20jurisdiction>.

<sup>3</sup> Containing *all fields*, which includes either the registrant’s full name, date of birth, residential address, his or her state driver’s license number or the last four digits of the registrant’s social security number as required by HAVA.

Sharing (“JEFS”). If Vermont would be interested in a data sharing agreement with the Civil Rights Division, please reply to [voting.section@usdoj.gov](mailto:voting.section@usdoj.gov) prior to the expiration of the fourteen-day response window. Upon receipt, we will send you an agreement template.

Should further clarification be required, please contact Maureen Riordan at [maureen.riordan2@usdoj.gov](mailto:maureen.riordan2@usdoj.gov).

Regards,

A handwritten signature in blue ink, appearing to read "Harmeet K. Dhillon".

Harmeet K. Dhillon  
Assistant Attorney General  
Civil Rights Division

cc: Seán Sheechan  
Director of Elections  
128 State Street  
Montpelier, VT 05633  
[Sean.Sheechan@vermont.gov](mailto:Sean.Sheechan@vermont.gov)



**U.S. Department of Justice**

Civil Rights Division

---

*Voting Section  
950 Pennsylvania Ave, NW – 4CON  
Washington, DC 20530*

July 15, 2025

Via Mail and Email

The Honorable Susan Beals  
Commissioner, Virginia Department of Elections  
1100 Bank Street, First Floor  
Richmond, Virginia 23219  
susan.beals@elections.virginia.gov

Dear Commissioner Beals:

We write to you as the chief election official for the Commonwealth of Virginia to request information regarding Virginia's procedures for complying with the statewide voter registration list maintenance provisions of the National Voter Registration Act ("NVRA"), 52 U.S.C. § 20501 *et seq.*

Please provide a list of the election officials who are responsible for implementing Virginia's general program of voter registration list maintenance from November 2022 through receipt of this letter, including those responsible officials not employed by your office (such as local election officials) who are also involved in that effort. Please also provide a description of the steps that you have taken, and when those steps were taken, to ensure that the Commonwealth's list maintenance program has been properly carried out in full compliance with the NVRA.

The NVRA requires each state and the District of Columbia to make available for inspection "all records concerning the implementation of programs and activities conducted for the purpose of ensuring the accuracy and currency of official lists of eligible voters." 52 U.S.C. § 20507(i)(1). Section 11 of the NVRA authorizes the Attorney General to bring NVRA enforcement actions. *See* 52 U.S.C. § 20510.

Pursuant to Section 20507(i) of the NVRA, the Attorney General requests that you produce for inspection the following records:

The current electronic copy of Virginia's computerized statewide voter registration list ("statewide voter registration list") as required by Section 303(a) of the Help America Vote Act. Please include all fields contained within the list. Please produce each list in a .xls, .csv, or delimited-text file format. Please specify what delimiter is used, if applicable, or provide a file layout along with a database user manual, coding list, or other materials that define or explain how a voter record is coded into the statewide voter registration list and reported in the electronic copy of the statewide voter registration list.

Additionally, please provide the following information in electronic form. The time period for these requests is close of registration for the November 2022 general election through the close of registration for the November 2024 general election, the same time period as the most recent report from the Election Assistance Commission's Election Administration and Voting Survey ("EAVS"). If you are unable to provide the data, please explain why the data is not available.

1. A review of the most recent report from EAVS report indicates that in response to Question A1b, there are nearly as many registered voters listed as active as the citizen voting age population in Virginia, with a registration rate in 2024 of 92.2 percent of the citizen voting age population. Please explain what actions Virginia is taking to ensure that voters who should not be on the voter roll are being removed.
2. In the EAVS data for Question A3d, Virginia had 1,074,543 voters (33.2 percent) with duplicate registrations, almost three times as high as the nationwide average of 12.7 percent. In response to the same question for the 2022 EAVS Report, Virginia had 1,226,754 duplicate registrations (36.3 percent). Please explain why duplicate registrations are such a high percentage of the total registration applications received. Please explain what actions Virginia is taking to identify duplicate registrations and to remove those duplicates from the voter registration list.
3. In the EAVS data for Question A10a, Virginia sent 521,339 confirmation notices, which is 8.8 percent of all active registered voters and well below the national average of 19.5 percent. Please explain why Virginia sent confirmation notices to so few registered voters.
4. In the EAVS data for Question A12b, Virginia had 536,460 voters (68.4 percent) removed because they moved out of the commonwealth, which was twice as high as the national average. Please explain how Virginia identifies voters who have moved out of the commonwealth and determines their removal from the voter registration list.
5. In the EAVS data for Question A12e, Virginia had 61,151 voters (7.8 percent) removed due to failure to respond to confirmation notices and did not vote in the two most recent federal elections, which was well below the national average. Based on the responses to Question A10f, 415,181 (79.6 percent) of the confirmation notices were unreturned. Please explain why so few voters are being removed in Question A12e. Please provide a list of all registrations that were cancelled because of failure to respond to confirmation notices and did not vote in the two most recent federal election cycles.
6. No data was listed in the EAVS survey for Question A12h for Virginia regarding duplicate registrants who were removed from the statewide voter registration database. Please provide a list of all duplicate registrants who were removed from the statewide voter registration list. If they were merged or linked with another record, please provide that information.

Please provide a description of the steps that Virginia has taken, and when those steps were taken, to identify registered voters who are ineligible to vote as well as the procedures the commonwealth used to remove those ineligible voters from the registration list. Please identify the number of registered voters identified as ineligible to vote for the time period of the close of registration for the November 2022 general election through present for each of the following reasons:

1. Non-citizen
2. Adjudicated incompetent
3. Felony conviction

For each of those voters identified in categories 1-3 above, provide their registration information on the statewide voter registration list, including their vote history.

Please provide this information within 14 days of the date of this letter. The information and materials may be sent by encrypted email to [voting.section@usdoj.gov](mailto:voting.section@usdoj.gov) or via the Department's secure file-sharing system, Justice Enterprise File Sharing (JEFS).

Should further clarification be required, please contact Maureen Riordan at [maureen.riordan2@usdoj.gov](mailto:maureen.riordan2@usdoj.gov). We look forward to your assistance in advance.

Sincerely,



Michael E. Gates  
Deputy Assistant Attorney General  
Civil Rights Division

Maureen Riordan  
Acting Chief, Voting Section  
Civil Rights Division



U.S. Department of Justice

Civil Rights Division

---

Office of the Assistant Attorney General

Washington, D.C. 20530

August 14, 2025

Via Mail and Email

The Honorable Susan Beals  
Commissioner, Virginia Department of Elections  
1100 Bank Street, First Floor  
Richmond, Virginia 23219  
[susan.beals@elections.virginia.gov](mailto:susan.beals@elections.virginia.gov)

Re: **Complete Virginia's Voter Registration List with All Fields**

Commissioner Beals:

We understand that the time the Justice Department has provided your state to respond to the request for a statewide voter registration list ("VRL") and other information has not reached its deadline.

Given responses from other states thus far, we want to clarify that the Justice Department's request to provide an electronic copy of the statewide VRL should contain *all fields*, which means, your state's VRL must include the registrant's full name, date of birth, residential address, his or her state driver's license number or the last four digits of the registrant's social security number as required under the Help America Vote Act ("HAVA")<sup>1</sup> to register individuals for federal elections. *See* 52 U.S.C. § 21083(a)(5)(A)(i).

We have requested Virginia's VRL to assess your state's compliance with the statewide VRL maintenance provisions of the National Voter Registration Act ("NVRA"), 52 U.S.C. § 20501, *et seq.* Our request is pursuant to the Attorney General's authority under Section 11 of the NVRA to bring enforcement actions. *See* 52 U.S.C. § 20501(a).

The Help America Vote Act ("HAVA"), 52 U.S.C. § 20501, *et seq.*, also provides authority for the Justice Department to seek the State's VRL via Section 401, which makes the Attorney

---

<sup>1</sup> In charging the Attorney General with enforcement of the voter registration list requirements in the HAVA and in the NVRA, Congress plainly intended that DOJ be able to conduct an independent review of each state's list. Any statewide prohibitions are clearly preempted by federal law.

General solely responsible for actions to enforce HAVA's computerized statewide voter registration list requirements. *See* 52 U.S.C. § 21111; *see also* *Brunner v. Ohio Republican Party*, 555 U.S. 5, 6 (2008) (*per curiam*) (finding there is no private right of action to enforce those requirements in HAVA).

In addition to those authorities, the Attorney General is also empowered by Congress to request records pursuant to Title III of the Civil Rights Act of 1960 ("CRA"), codified at 52 U.S.C. § 20701, *et seq.* Section 301 of the CRA requires state and local officials to retain and preserve records related to voter registration and other acts requisite to voting for any federal office for a period of 22 months after any federal general, special or primary election. *See* 52 U.S.C. § 20701.

Section 303 of the CRA provides, in pertinent part, "Any record or paper required by section 20701 of this title to be retained and preserved shall, upon demand in writing by the Attorney General or his representative directed to the person having custody, possession, or control of such record or paper, be made available for inspection, reproduction, and copying at the principal office of such custodian by the Attorney General or his representative..." 52 U.S.C. § 20703.

Pursuant to the foregoing authorities, including the CRA, the Attorney General is demanding an electronic copy of Virginia's complete and current VRL. The purpose of the request is to ascertain Virginia's compliance with the list maintenance requirements of the NVRA and HAVA.

When providing the electronic copy of the statewide VRL, Virginia must ensure that it contains *all fields*, which includes either the registrant's full name, date of birth, residential address, his or her state driver's license number, or the last four digits of the registrant's social security number as required under the Help America Vote Act ("HAVA")<sup>2</sup> to register individuals for federal elections. *See* 52 U.S.C. § 21083(a)(5)(A)(i).

To the extent there are privacy concerns, the voter registration list is subject to federal privacy protections. Section 304 of the CRA provides the answer:

Unless otherwise ordered by a court of the United States, neither the Attorney General nor any employee of the Department of Justice, nor any other representative of the Attorney General, shall disclose any record or paper produced pursuant to this chapter, or any reproduction or copy, except to Congress and any committee thereof, governmental agencies, and in the presentation of any case or proceeding before any court or grand jury.

HAVA specifies that the "last 4 digits of a social security number . . . shall not be considered a social security number for purposes of section 7 of the Privacy Act of 1974" (5 U.S.C. § 552a note); 52 U.S.C. § 21083(c). In addition, any prohibition of disclosure of a motor vehicle record contained in the Driver's License Protection Act, codified at 18 U.S.C. § 2721(b)(1), is exempted when the disclosure is for use by a government agency in carrying out the government agency's function to

---

<sup>2</sup> In charging the Attorney General with enforcement of the voter registration list requirements in HAVA and in the NVRA, Congress plainly intended that DOJ be able to conduct an independent review of each state's list. Any statewide prohibitions are clearly preempted by federal law.

accomplish its enforcement authority as the Justice Department is now doing. That said, all data received from you will be kept securely and treated consistently with the Privacy Act.

To that end, please provide the requested electronic Voter Registration List<sup>3</sup> to the Justice Department by the date set for your delivery by our original letter, or by August 21, 2025, whichever is later.

The information and materials may be sent by encrypted email to [voting.section@usdoj.gov](mailto:voting.section@usdoj.gov) or via the Department's secure file-sharing system, Justice Enterprise File Sharing ("JEFS"). Should further clarification be required, please contact Maureen Riordan at [maureen.riordan2@usdoj.gov](mailto:maureen.riordan2@usdoj.gov).

Regards,

A handwritten signature in blue ink, appearing to read "Harmeet K. Dhillon".

Harmeet K. Dhillon  
Assistant Attorney General  
Civil Rights Division

---

<sup>3</sup> Containing *all fields*, which includes either the registrant's full name, date of birth, residential address, his or her state driver's license number or the last four digits of the registrant's social security number as required by HAVA.



U.S. Department of Justice

Civil Rights Division

---

Office of the Assistant Attorney General

Washington, D.C. 20530

September 8, 2025

Via Mail and Email

The Honorable Steve Hobbs  
Secretary of State  
PO Box 40220  
Olympia, WA 98504-0220  
[steve.hobbs@sos.wa.gov](mailto:steve.hobbs@sos.wa.gov);  
[secretaryofstate@sos.wa.gov](mailto:secretaryofstate@sos.wa.gov)

Re: **Request for Complete Washington's Voter Registration List with All Fields**

Dear Secretary Hobbs:

We write to you as the chief election official for the State of Washington concerning your State's compliance with the statewide voter registration list maintenance provisions of the National Voter Registration Act ("NVRA"), 52 U.S.C. § 20501 *et seq.*, and the Help America Vote Act ("HAVA"), 52 U.S.C. § 20901, *et seq.* Please provide a copy of Washington's statewide voter registration list ("VRL") within fourteen days of the date of this letter.

The electronic copy of the statewide VRL should contain *all fields*, which means, your state's VRL must include the registrant's full name, date of birth, residential address, his or her state driver's license number or the last four digits of the registrant's social security number as required under HAVA<sup>1</sup> to register individuals for federal elections. *See* 52 U.S.C. § 21083(a)(5)(A)(i).

We request Washington's VRL to assess your state's compliance with the statewide VRL maintenance provisions of the NVRA. Our request is pursuant to the Attorney General's authority under Section 11 of the NVRA to bring enforcement actions. *See* 52 U.S.C. § 20510(a).

HAVA also provides authority for the Justice Department to seek the State's VRL via Section 401, which makes the Attorney General solely responsible for actions to enforce HAVA's

---

<sup>1</sup> In charging the Attorney General with enforcement of the voter registration list requirements in the HAVA and in the NVRA, Congress plainly intended that DOJ be able to conduct an independent review of each state's list. Any statewide prohibitions are clearly preempted by federal law.

computerized statewide voter registration list requirements. *See* 52 U.S.C. § 21111; *see also Brunner v. Ohio Republican Party*, 555 U.S. 5, 6 (2008) (*per curiam*) (finding no private right of action to enforce HAVA requirements).

In addition to those authorities, the Attorney General is also empowered by Congress to request records pursuant to Title III of the Civil Rights Act of 1960 (“CRA”), codified at 52 U.S.C. § 20701, *et seq.* Section 301 of the CRA requires state and local officials to retain and preserve records related to voter registration and other acts requisite to voting for any federal office for a period of twenty-two months after any federal general, special or primary election. *See* 52 U.S.C. § 20701.

Section 303 of the CRA provides, in pertinent part, “Any record or paper required by section 20701 to be retained and preserved shall, upon demand in writing by the Attorney General or his representative directed to the person having custody, possession, or control of such record or paper, be made available for inspection, reproduction, and copying at the principal office of such custodian by the Attorney General or his representative...” *See* 52 U.S.C. § 20703.

Pursuant to the foregoing authorities, including the CRA, the Attorney General is requesting an electronic copy of Washington’s complete and current VRL. The purpose of this request is to ascertain Washington’s compliance with the list maintenance requirements of the NVRA and HAVA.

To the extent there are privacy concerns, the voter registration list is subject to federal privacy protections. Section 304 of the CRA provides the answer:

Unless otherwise ordered by a court of the United States, neither the Attorney General nor any employee of the Department of Justice, nor any other representative of the Attorney General, shall disclose any record or paper produced pursuant to this chapter, or any reproduction or copy, except to Congress and any committee thereof, governmental agencies, and in the presentation of any case or proceeding before any court or grand jury.

52 U.S.C. § 20704. HAVA specifies that the “last 4 digits of a social security number . . . shall not be considered to be a social security number for purposes of section 7 of the Privacy Act of 1974” (5 U.S.C. § 522a note); 52 U.S.C. § 21083(e). In addition, any prohibition of disclosure of a motor vehicle record contained in the Driver’s License Protection Act, codified at 18 U.S.C. § 2721(b)(1), is exempted when the disclosure is for use by a government agency in carrying out the government agency’s function to accomplish its enforcement authority as the Justice Department is now doing. That said, all data received from you will be kept securely and treated consistently with the Privacy Act explained at [Civil Rights Division - Department of Justice - Privacy Policy](#)<sup>2</sup>.

Please provide the requested electronic VRL<sup>3</sup> to the Justice Department fourteen days from the date of this letter. The information and materials may be sent by encrypted email to

<sup>2</sup> Available at: <https://civilrights.justice.gov/privacy-policy#:~:text=Our%20Statutes-Privacy%20Act%20Statement,the%20scope%20of%20our%20jurisdiction>.

<sup>3</sup> Containing *all fields*, which includes either the registrant’s full name, date of birth, residential address, his or her state driver’s license number or the last four digits of the registrant’s social security number as required by HAVA.

[voting.section@usdoj.gov](mailto:voting.section@usdoj.gov) or via the Department's secure file-sharing system, Justice Enterprise File Sharing ("JEFS"). If Washington would be interested in a data sharing agreement with the Civil Rights Division, please reply to [voting.section@usdoj.gov](mailto:voting.section@usdoj.gov) prior to the expiration of the fourteen-day response window. Upon receipt, we will send you an agreement template.

Should further clarification be required, please contact Maureen Riordan at [maureen.riordan2@usdoj.gov](mailto:maureen.riordan2@usdoj.gov).

Regards,

A handwritten signature in blue ink, appearing to read "Harmeet K. Dhillon".

Harmeet K. Dhillon  
Assistant Attorney General  
Civil Rights Division

cc: Stuart Holmes  
Director of Elections  
416 Sid Snyder Ave SW  
Olympia, WA 98501  
[stuart.holmes@sos.wa.gov](mailto:stuart.holmes@sos.wa.gov)

---

**From:** Neff, Eric (CRT) [/O=EXCHANGELABS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=5BA4FD2878EA45EAAD98FC2FC41CC8E5-ENEFF]  
**Sent:** 12/19/2025 6:18:21 PM  
**To:** wvsos@wvsos.com  
**Subject:** Follow Up  
**Attachments:** 9.8.2025 Letter to West Virginia Final.pdf; VRLData Sharing Agreement MOU.pdf

This email is a follow up to our previous requests for West Virginia's Voter Registration List. We have received no response as of this date.

Does your office have a reply? No response by COB today will be treated as a refusal.

Thanks,  
Eric

**Eric Neff**  
Acting Chief  
Civil Rights Division, Voting Section  
Department of Justice  
150 M St. NE, Ste. 8-139  
Washington, DC 20002  
[Eric.Neff@usdoj.gov](mailto:Eric.Neff@usdoj.gov)  
Cell: 202-532-3628





U.S. Department of Justice

Civil Rights Division

---

Office of the Assistant Attorney General

Washington, D.C. 20530

September 8, 2025

Via Mail and Email

The Honorable Kris Warner  
Secretary of State  
1900 Kanawha Blvd.  
Bldg. 1, Suite 157-K  
Charleston, WV 25305  
[wvsos@wvsos.com](mailto:wvsos@wvsos.com)

Re: **Request for Complete West Virginia's Voter Registration List with All Fields**

Dear Secretary Warner:

We write to you as the chief election official for the State of West Virginia concerning your State's compliance with the statewide voter registration list maintenance provisions of the National Voter Registration Act ("NVRA"), 52 U.S.C. § 20501 *et seq.*, and the Help America Vote Act ("HAVA"), 52 U.S.C. § 20901, *et seq.* Please provide a copy of West Virginia's statewide voter registration list ("VRL") within fourteen days of the date of this letter.

The electronic copy of the statewide VRL should contain *all fields*, which means, your state's VRL must include the registrant's full name, date of birth, residential address, his or her state driver's license number or the last four digits of the registrant's social security number as required under HAVA<sup>1</sup> to register individuals for federal elections. *See* 52 U.S.C. § 21083(a)(5)(A)(i).

We request West Virginia's VRL to assess your state's compliance with the statewide VRL maintenance provisions of the NVRA. Our request is pursuant to the Attorney General's authority under Section 11 of the NVRA to bring enforcement actions. *See* 52 U.S.C. § 20510(a).

HAVA also provides authority for the Justice Department to seek the State's VRL via Section 401, which makes the Attorney General solely responsible for actions to enforce HAVA's

---

<sup>1</sup> In charging the Attorney General with enforcement of the voter registration list requirements in the HAVA and in the NVRA, Congress plainly intended that DOJ be able to conduct an independent review of each state's list. Any statewide prohibitions are clearly preempted by federal law.

computerized statewide voter registration list requirements. *See* 52 U.S.C. § 21111; *see also Brunner v. Ohio Republican Party*, 555 U.S. 5, 6 (2008) (*per curiam*) (finding no private right of action to enforce HAVA requirements).

In addition to those authorities, the Attorney General is also empowered by Congress to request records pursuant to Title III of the Civil Rights Act of 1960 (“CRA”), codified at 52 U.S.C. § 20701, *et seq.* Section 301 of the CRA requires state and local officials to retain and preserve records related to voter registration and other acts requisite to voting for any federal office for a period of twenty-two months after any federal general, special or primary election. *See* 52 U.S.C. § 20701.

Section 303 of the CRA provides, in pertinent part, “Any record or paper required by section 20701 to be retained and preserved shall, upon demand in writing by the Attorney General or his representative directed to the person having custody, possession, or control of such record or paper, be made available for inspection, reproduction, and copying at the principal office of such custodian by the Attorney General or his representative...” *See* 52 U.S.C. § 20703.

Pursuant to the foregoing authorities, including the CRA, the Attorney General is requesting an electronic copy of West Virginia’s complete and current VRL. The purpose of this request is to ascertain West Virginia’s compliance with the list maintenance requirements of the NVRA and HAVA.

To the extent there are privacy concerns, the voter registration list is subject to federal privacy protections. Section 304 of the CRA provides the answer:

Unless otherwise ordered by a court of the United States, neither the Attorney General nor any employee of the Department of Justice, nor any other representative of the Attorney General, shall disclose any record or paper produced pursuant to this chapter, or any reproduction or copy, except to Congress and any committee thereof, governmental agencies, and in the presentation of any case or proceeding before any court or grand jury.

52 U.S.C. § 20704. HAVA specifies that the “last 4 digits of a social security number . . . shall not be considered to be a social security number for purposes of section 7 of the Privacy Act of 1974” (5 U.S.C. § 522a note); 52 U.S.C. § 21083(c). In addition, any prohibition of disclosure of a motor vehicle record contained in the Driver’s License Protection Act, codified at 18 U.S.C. § 2721(b)(1), is exempted when the disclosure is for use by a government agency in carrying out the government agency’s function to accomplish its enforcement authority as the Justice Department is now doing. That said, all data received from you will be kept securely and treated consistently with the Privacy Act explained at [Civil Rights Division - Department of Justice - Privacy Policy](#)<sup>2</sup>.

---

<sup>2</sup> Available at: <https://civilrights.justice.gov/privacy-policy#:~:text=Our%20Statutes-Privacy%20Act%20Statement,the%20scope%20of%20our%20jurisdiction.>

Please provide the requested electronic VRL<sup>3</sup> to the Justice Department fourteen days from the date of this letter. The information and materials may be sent by encrypted email to [voting.section@usdoj.gov](mailto:voting.section@usdoj.gov) or via the Department's secure file-sharing system, Justice Enterprise File Sharing ("JEFS"). If West Virginia would be interested in a data sharing agreement with the Civil Rights Division, please reply to [voting.section@usdoj.gov](mailto:voting.section@usdoj.gov) prior to the expiration of the fourteen-day response window. Upon receipt, we will send you an agreement template.

Should further clarification be required, please contact Maureen Riordan at [maureen.riordan2@usdoj.gov](mailto:maureen.riordan2@usdoj.gov).

Regards,



Harmeet K. Dhillon  
Assistant Attorney General  
Civil Rights Division

cc: Brittany Westfall  
Elections Director  
1900 Kanawha Blvd.  
Bldg. 1, Suite 157-K  
Charleston, WV 25305  
[bwestfall@wvsos.gov](mailto:bwestfall@wvsos.gov)

---

<sup>3</sup> Containing *all fields*, which includes either the registrant's full name, date of birth, residential address, his or her state driver's license number or the last four digits of the registrant's social security number as required by HAVA.



**U.S. Department of Justice**

Civil Rights Division

---

**CONFIDENTIAL MEMORANDUM OF UNDERSTANDING**

**I. PARTIES & POINTS OF CONTACT.**

Requester

Federal Agency Name: Civil Rights Division, U.S. Department of Justice

VRL/Data User:

Title:

Address:

Phone:

VRL/Data Provider

State Agency Name:

Custodian:

Title:

Address:

Phone:

The parties to this Memorandum of Understanding (“MOU” or “Agreement”) are the Department of Justice, Civil Rights Division (“Justice Department” or “Department”), and the **[Insert Entity/Agency Name]** (“You” or “your state”).

**II. AUTHORITY.**

By this Agreement, **[Insert Entity/Agency Name]** (“You” or “your state”) has agreed to, and will, provide an electronic copy of your state’s complete statewide Voter Registration List (“VRL” or “VRL/Data”) to the Civil Rights Division of the U.S. Department of Justice (at times referred to as the “Department”). The VRL/Data must include, among other fields of data, the voter registrant’s full name, date of birth, residential address, his or her state driver’s license

number or the last four digits of the registrant's social security number as required under the HAVA to register individuals for federal elections. *See* 52 U.S.C. § 21083(a)(5)(A).

The authorities by which this information is requested by the Department of Justice are:

- National Voter Registration Act of 1993, 52 U.S.C. § 20501, *et seq.*
- Attorney General's authority under Section 11 of the NVRA to bring enforcement actions. *See* 52 U.S.C. § 20501(a).
- Help America Vote Act of 2002, 52 U.S.C. § 20901, *et seq.*
- Attorney General's authority to enforce the Help America Vote Act under 53 U.S.C. § 21111.
- Attorney General authority to request records pursuant to Title III of the Civil Rights Act of 1960 ("CRA"), codified at 52 U.S.C. § 20701, *et seq.*
- The Privacy Act of 1974, 5 U.S.C. § 552a, as amended.

### **III. PURPOSE.**

A VRL is a Voter Registration List pursuant to the NVRA and HAVA, commonly referred to as "voter roll," compiled by a state – often from information submitted by counties – containing a list of all the state's *eligible* voters. Regardless of the basis for ineligibility, ineligible voters do not appear on a state's VRL when proper list maintenance is performed by states. The Justice Department is requesting your state's VRL to test, analyze, and assess states' VRLs for proper list maintenance and compliance with federal law. In the event the Justice Department's analysis of a VRL results in list maintenance issues, insufficiency, inadequacy, anomalies, or concerns, the Justice Department will notify your state's point of contact of the issues to assist your state with curing.

The purpose of this MOU is to establish the parties' understanding as to the security protections for data transfer and data access by the Department of Justice of the electronic copy of the statewide voter registration list, including all fields requested by the Department of Justice.

#### **IV. TIMING OF AGREEMENT – TIME IS OF ESSENCE.**

Although the Justice Department is under no such obligation as a matter of law, because this Agreement is proposed, made, and to be entered into at your state's request as part of your state's transmission of its VRL to the Justice Department, this Agreement is to be fully executed within seven (7) days of the Justice Department presenting this Agreement to you. Both parties agree that no part of this Agreement or execution is intended to, or will, cause delay of the transmission of your state's VRL to the Justice Department for analysis.

#### **V. TIMING OF VRL/DATA TRANSFER.**

You agree to transfer an electronic copy of your state's complete statewide VRL/Data to the Civil Rights Division of the U.S. Department of Justice as described in Section III of this Agreement no later than five (5) business days from the execution of this Agreement, which is counted from the last day of the last signatory.

#### **VI. METHOD OF VRL/DATA ACCESS OR TRANSFER.**

The VRL will be submitted by your state via the Department of Justice's secure file-sharing system, i.e., Justice Enterprise File Sharing (JEFS"). A separate application to use JEFS must be completed and submitted by your state through the Civil Rights Help Desk. JEFS implements strict access controls to ensure that each user can only access their own files. All files and folders are tied to a specific user, and each user has defined permissions that govern how they may interact with those files (e.g., read, write, or read-only).

Whenever a user attempts to access a file or folder, JEFS validates the request against the assigned permissions to confirm that the user is explicitly authorized. This process guarantees that users can only access files and folders only where they have permission. Users are also limited to the authorized type of interaction with each file or folder. Within the Department of Justice, access to JEFS is restricted to specific roles: Litigation Support, IT staff, and Civil Rights Division staff.

## **VII. LOCATION OF DATA AND CUSTODIAL RESPONSIBILITY.**

The parties mutually agree that the Civil Rights Division (also “Department”) will be designated as “Custodian” of the file(s) and will be responsible for the observance of all conditions for use and for establishment and maintenance of security agreements as specified in this agreement to prevent unauthorized use. The information that the Department is collecting will be maintained consistent with the Privacy Act of 1974, 5 U.S.C. § 552a. The full list of routine uses for this collection of information can be found in the Systems of Record Notice (“SORN”) titled, JUSTICE/CRT – 001, “Central Civil Rights Division Index File and Associated Records,” 68 Fed. Reg. 47610-01, 611 (August 11, 2003); 70 Fed. Reg. 43904-01 (July 29, 2005); and 82 Fed. Reg. 24147-01 (May 25, 2017). It should be noted that the statutes cited for routine use include NVRA, HAVA, and the Civil Rights Act of 1960, and the Justice Department is making our request pursuant to those statutes. The records in the system of records are kept under the authority of 44 U.S.C. § 3101 and in the ordinary course of fulfilling the responsibility assigned to the Civil Rights Division under the provisions of 28 C.F.R. §§ 0.50, 0.51.

VRL/Data storage is similar to the restricted access provided on JEFS and complies with the SORN: Information in computer form is safeguarded and protected in accordance with applicable Department security regulations for systems of records. Only a limited number of staff members who are assigned a specific identification code will be able to use the computer to access

the stored information. However, a section may decide to allow its employees access to the system in order to perform their official duties.

All systems storing the VRL data will comply with all security requirements applicable to Justice Department systems, including but not limited to all Executive Branch system security requirements (e.g., requirements imposed by the Office of Management and Budget [OMB] and National Institute of Standards and Technology [NIST]), Department of Justice IT Security Standards, and Department of Justice Order 2640.2F.

#### **VIII. NVRA/HAVA COMPLIANT VOTER REGISTRATION LIST.**

After analysis and assessment of your state's VRL, the Justice Department will securely notify you or your state of any voter list maintenance issues, insufficiencies, inadequacies, deficiencies, anomalies, or concerns, the Justice Department found when testing, assessing, and analyzing your state's VRL for NVRA and HAVA compliance, i.e., that your state's VRL only includes eligible voters.

You agree therefore that within forty-five (45) days of receiving that notice from the Justice Department of any issues, insufficiencies, inadequacies, deficiencies, anomalies, or concerns, your state will clean its VRL/Data by removing ineligible voters and resubmit the updated VRL/Data to the Civil Rights Division of the Justice Department to verify proper list maintenance has occurred by your state pursuant to the NVRA and HAVA.

#### **IX. CONFIDENTIALITY & DEPARTMENT SAFEGUARDS.**

Any member of the Justice Department in possession of a VRL/Data will employ reasonable administrative, technical, and physical safeguards designed to protect the security and confidentiality of such data. Compliance with these safeguards will include secure user authentication protocols deploying either: (i) Two-Factor Authentication ("2FA"), which requires users to go through two layers of security before access is granted to the system; or (ii) the

assignment of unique user identifications to each person with computer access plus unique complex passwords, which are not vendor supplied default passwords.

The Department will activate audit logging for the records, files, and data containing the state's VRL/Data in order to identify abnormal use, as well as to track access control, on computers, servers and/or Devices containing the VRL/Data.

For all devices storing records, files, and data containing the VRL/Data: there is (i) up-to-date versions of system security agent software that includes endpoint protection and malware protection and reasonably up-to-date patches and virus definitions, or a version of such software that can still be supported with up-to-date patches and virus definitions, and is set to receive the most current security updates on a regular basis; and (ii) up-to-date operating system security patches designed to maintain the integrity of the personal information.

For all devices storing records, files, and data containing the VRL/Data: there is (i) controlled and locked physical access for the Device; and (ii) the prohibition of the connection of the Device to public or insecure home networks.

There will be no copying of records, files, or data containing the VRL/Data to unencrypted USB drives, CDs, or external storage. In addition, the use of devices outside of moving the records, files, or data to the final stored device location shall be limited.

Any notes, lists, memoranda, indices, compilations prepared or based on an examination of VRL/Data or any other form of information (including electronic forms), that quote from, paraphrase, copy, or disclose the VRL/Data with such specificity that the VRL/Data can be identified, or by reasonable logical extension can be identified will not be shared by the Department. Any summary results, however, may be shared by the Department.

In addition to the Department's enforcement efforts, the Justice Department may use the information you provide for certain routine, or pre-litigation or litigation purposes including:

present VRL/Data to a court, magistrate, or administrative tribunal; a contractor with the Department of Justice who needs access to the VRL/Data information in order to perform duties related to the Department's list maintenance verification procedures. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. § 552a(m).

#### **X. LOSS OR BREACH OF DATA.**

If a receiving party discovers any loss of VRL/Data, or a breach of security, including any actual or suspected unauthorized access, relating to VRL/Data, the receiving party shall, at its own expense immediately provide written notice to the producing party of such breach; investigate and make reasonable and timely efforts to remediate the effects of the breach, and provide the producing party with assurances reasonably satisfactory to the producing party that such breach shall not recur; and provide sufficient information about the breach that the producing party can reasonably ascertain the size and scope of the breach. The receiving party agrees to cooperate with the producing party or law enforcement in investigating any such security incident. In any event, the receiving party shall promptly take all necessary and appropriate corrective action to terminate unauthorized access.

#### **XI. DESTRUCTION OF DATA.**

The Department will destroy all VRL/Data associated with actual records as soon as the purposes of the list maintenance project have been accomplished and the time required for records retention pursuant to applicable law has passed. When the project is complete and such retention requirements by law expires, the Justice Department will:

1. Destroy all hard copies containing confidential data (e.g., shredding);
2. Archive and store electronic data containing confidential information offline in a secure location; and

3. All other data will be erased or maintained in a secured area.

## **XII. OTHER PROVISIONS.**

- A. Conflicts. This MOU constitutes the full MOU on this subject between the Department and your state. Any inconsistency or conflict between or among the provisions of this MOU, will be resolved in the following order of precedence: (1) this MOU and (2) other documents incorporated by reference in this MOU (e.g., transaction charges).
- B. Severability. Nothing in this MOU is intended to conflict with current law or regulation or the directives of Department, or the your state. If a term of this MOU is inconsistent with such authority, then that term shall be invalid but, to the extent allowable, the remaining terms and conditions of this MOU shall remain in full force and effect.
- C. Assignment. Your state may not assign this MOU, nor may it assign any of its rights or obligations under this MOU. To the extent allowable by law, this MOU shall inure to the benefit of, and be binding upon, any successors to the Justice Department and your state without restriction.
- D. Waiver. No waiver by either party of any breach of any provision of this MOU shall constitute a waiver of any other breach. Failure of either party to enforce at any time, or from time to time, any provision of this MOU shall not be construed to be a waiver thereof.
- E. Compliance with Other Laws. Nothing in this MOU is intended or should be construed to limit or affect the duties, responsibilities, and rights of the User Agency under the National Voter Registration Act, 52 U.S.C. § 20501 *et seq.*, as amended; the Help America Vote Act, 52 U.S.C. § 20901 *et seq.*, as amended; the Voting Rights Act, 52 U.S.C. § 10301 *et seq.*, as amended; and the Civil Rights Act, 52 U.S.C. § 10101 *et seq.*, as amended.
- F. Confidentiality of MOU. To the extent allowed by applicable law, this MOU, its contents, and the drafts and communications leading up to the execution of this MOU are deemed

by the parties as “confidential.” Any disclosures therefore could be made, if at all, pursuant to applicable laws or court orders requiring such disclosures.

**SIGNATURES**

VRL/Data Provider

State Agency Name:

Signature: \_\_\_\_\_ Date of Execution: \_\_\_\_\_

Authorized Signatory Name Printed: \_\_\_\_\_

Title: \_\_\_\_\_

Requester

Federal Agency Name: Civil Rights Division, U.S. Department of Justice

Signature: \_\_\_\_\_ Date of Execution: \_\_\_\_\_

Authorized Signatory Name Printed: \_\_\_\_\_

Title: \_\_\_\_\_

---

**From:** Neff, Eric (CRT) [/O=EXCHANGELABS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=5BA4FD2878EA45EAAD98FC2FC41CC8E5-ENEFF]  
**Sent:** 1/13/2026 3:46:07 PM  
**To:** 'wvsos@wvsos.com' [wvsos@wvsos.com]  
**Subject:** RE: Follow Up

Following up to this prior email. Does your office have a response?

---

**From:** Neff, Eric (CRT)  
**Sent:** Friday, December 19, 2025 1:18 PM  
**To:** wvsos@wvsos.com  
**Subject:** Follow Up

This email is a follow up to our previous requests for West Virginia's Voter Registration List. We have received no response as of this date.

Does your office have a reply? No response by COB today will be treated as a refusal.

Thanks,  
Eric

**Eric Neff**  
Acting Chief  
Civil Rights Division, Voting Section  
Department of Justice  
150 M St. NE, Ste. 8-139  
Washington, DC 20002  
[Eric.Neff@usdoj.gov](mailto:Eric.Neff@usdoj.gov)  
Cell: 202-532-3628



---

**From:** Bennett, Brittany (CRT) [/O=EXCHANGELABS/OU=EXCHANGE ADMINISTRATIVE GROUP (FYDIBOHF23SPDLT)/CN=RECIPIENTS/CN=29CCD32720BD43F59B29D43FC56E2F4E-BRBENNET]  
**Sent:** 12/10/2025 4:27:40 PM  
**To:** wvsos@wvsos.com  
**Subject:** Request for West Virginia's VRL  
**Attachments:** 9.8.2025 Letter to West Virginia Final.pdf; VRLData Sharing Agreement MOU.pdf

Good morning,

Please see attached.

Thank you.

**Brittany E. Bennett**  
Trial Attorney  
Civil Rights Division, Voting Section  
U.S. Department of Justice  
150 M Street NE  
Washington, D.C. 20002  
(202) 704-5430  
[brittany.bennett@usdoj.gov](mailto:brittany.bennett@usdoj.gov)





U.S. Department of Justice

Civil Rights Division

---

Office of the Assistant Attorney General

Washington, D.C. 20530

September 8, 2025

Via Mail and Email

The Honorable Kris Warner  
Secretary of State  
1900 Kanawha Blvd.  
Bldg. 1, Suite 157-K  
Charleston, WV 25305  
[wvsos@wvsos.com](mailto:wvsos@wvsos.com)

Re: **Request for Complete West Virginia's Voter Registration List with All Fields**

Dear Secretary Warner:

We write to you as the chief election official for the State of West Virginia concerning your State's compliance with the statewide voter registration list maintenance provisions of the National Voter Registration Act ("NVRA"), 52 U.S.C. § 20501 *et seq.*, and the Help America Vote Act ("HAVA"), 52 U.S.C. § 20901, *et seq.* Please provide a copy of West Virginia's statewide voter registration list ("VRL") within fourteen days of the date of this letter.

The electronic copy of the statewide VRL should contain *all fields*, which means, your state's VRL must include the registrant's full name, date of birth, residential address, his or her state driver's license number or the last four digits of the registrant's social security number as required under HAVA<sup>1</sup> to register individuals for federal elections. *See* 52 U.S.C. § 21083(a)(5)(A)(i).

We request West Virginia's VRL to assess your state's compliance with the statewide VRL maintenance provisions of the NVRA. Our request is pursuant to the Attorney General's authority under Section 11 of the NVRA to bring enforcement actions. *See* 52 U.S.C. § 20510(a).

HAVA also provides authority for the Justice Department to seek the State's VRL via Section 401, which makes the Attorney General solely responsible for actions to enforce HAVA's

---

<sup>1</sup> In charging the Attorney General with enforcement of the voter registration list requirements in the HAVA and in the NVRA, Congress plainly intended that DOJ be able to conduct an independent review of each state's list. Any statewide prohibitions are clearly preempted by federal law.

computerized statewide voter registration list requirements. *See* 52 U.S.C. § 21111; *see also Brunner v. Ohio Republican Party*, 555 U.S. 5, 6 (2008) (*per curiam*) (finding no private right of action to enforce HAVA requirements).

In addition to those authorities, the Attorney General is also empowered by Congress to request records pursuant to Title III of the Civil Rights Act of 1960 (“CRA”), codified at 52 U.S.C. § 20701, *et seq.* Section 301 of the CRA requires state and local officials to retain and preserve records related to voter registration and other acts requisite to voting for any federal office for a period of twenty-two months after any federal general, special or primary election. *See* 52 U.S.C. § 20701.

Section 303 of the CRA provides, in pertinent part, “Any record or paper required by section 20701 to be retained and preserved shall, upon demand in writing by the Attorney General or his representative directed to the person having custody, possession, or control of such record or paper, be made available for inspection, reproduction, and copying at the principal office of such custodian by the Attorney General or his representative...” *See* 52 U.S.C. § 20703.

Pursuant to the foregoing authorities, including the CRA, the Attorney General is requesting an electronic copy of West Virginia’s complete and current VRL. The purpose of this request is to ascertain West Virginia’s compliance with the list maintenance requirements of the NVRA and HAVA.

To the extent there are privacy concerns, the voter registration list is subject to federal privacy protections. Section 304 of the CRA provides the answer:

Unless otherwise ordered by a court of the United States, neither the Attorney General nor any employee of the Department of Justice, nor any other representative of the Attorney General, shall disclose any record or paper produced pursuant to this chapter, or any reproduction or copy, except to Congress and any committee thereof, governmental agencies, and in the presentation of any case or proceeding before any court or grand jury.

52 U.S.C. § 20704. HAVA specifies that the “last 4 digits of a social security number . . . shall not be considered to be a social security number for purposes of section 7 of the Privacy Act of 1974” (5 U.S.C. § 522a note); 52 U.S.C. § 21083(c). In addition, any prohibition of disclosure of a motor vehicle record contained in the Driver’s License Protection Act, codified at 18 U.S.C. § 2721(b)(1), is exempted when the disclosure is for use by a government agency in carrying out the government agency’s function to accomplish its enforcement authority as the Justice Department is now doing. That said, all data received from you will be kept securely and treated consistently with the Privacy Act explained at [Civil Rights Division - Department of Justice - Privacy Policy](#)<sup>2</sup>.

---

<sup>2</sup> Available at: <https://civilrights.justice.gov/privacy-policy#:~:text=Our%20Statutes-Privacy%20Act%20Statement,the%20scope%20of%20our%20jurisdiction.>

Please provide the requested electronic VRL<sup>3</sup> to the Justice Department fourteen days from the date of this letter. The information and materials may be sent by encrypted email to [voting.section@usdoj.gov](mailto:voting.section@usdoj.gov) or via the Department's secure file-sharing system, Justice Enterprise File Sharing ("JEFS"). If West Virginia would be interested in a data sharing agreement with the Civil Rights Division, please reply to [voting.section@usdoj.gov](mailto:voting.section@usdoj.gov) prior to the expiration of the fourteen-day response window. Upon receipt, we will send you an agreement template.

Should further clarification be required, please contact Maureen Riordan at [maureen.riordan2@usdoj.gov](mailto:maureen.riordan2@usdoj.gov).

Regards,



Harmeet K. Dhillon  
Assistant Attorney General  
Civil Rights Division

cc: Brittany Westfall  
Elections Director  
1900 Kanawha Blvd.  
Bldg. 1, Suite 157-K  
Charleston, WV 25305  
[bwestfall@wvsos.gov](mailto:bwestfall@wvsos.gov)

---

<sup>3</sup> Containing *all fields*, which includes either the registrant's full name, date of birth, residential address, his or her state driver's license number or the last four digits of the registrant's social security number as required by HAVA.



U.S. Department of Justice

Civil Rights Division

---

**CONFIDENTIAL MEMORANDUM OF UNDERSTANDING**

**I. PARTIES & POINTS OF CONTACT.**

Requester

Federal Agency Name: Civil Rights Division, U.S. Department of Justice

VRL/Data User:

Title:

Address:

Phone:

VRL/Data Provider

State Agency Name:

Custodian:

Title:

Address:

Phone:

The parties to this Memorandum of Understanding (“MOU” or “Agreement”) are the Department of Justice, Civil Rights Division (“Justice Department” or “Department”), and the **[Insert Entity/Agency Name]** (“You” or “your state”).

**II. AUTHORITY.**

By this Agreement, **[Insert Entity/Agency Name]** (“You” or “your state”) has agreed to, and will, provide an electronic copy of your state’s complete statewide Voter Registration List (“VRL” or “VRL/Data”) to the Civil Rights Division of the U.S. Department of Justice (at times referred to as the “Department”). The VRL/Data must include, among other fields of data, the voter registrant’s full name, date of birth, residential address, his or her state driver’s license

number or the last four digits of the registrant's social security number as required under the HAVA to register individuals for federal elections. *See* 52 U.S.C. § 21083(a)(5)(A).

The authorities by which this information is requested by the Department of Justice are:

- National Voter Registration Act of 1993, 52 U.S.C. § 20501, *et seq.*
- Attorney General's authority under Section 11 of the NVRA to bring enforcement actions. *See* 52 U.S.C. § 20501(a).
- Help America Vote Act of 2002, 52 U.S.C. § 20901, *et seq.*
- Attorney General's authority to enforce the Help America Vote Act under 53 U.S.C. § 21111.
- Attorney General authority to request records pursuant to Title III of the Civil Rights Act of 1960 ("CRA"), codified at 52 U.S.C. § 20701, *et seq.*
- The Privacy Act of 1974, 5 U.S.C. § 552a, as amended.

### **III. PURPOSE.**

A VRL is a Voter Registration List pursuant to the NVRA and HAVA, commonly referred to as "voter roll," compiled by a state – often from information submitted by counties – containing a list of all the state's *eligible* voters. Regardless of the basis for ineligibility, ineligible voters do not appear on a state's VRL when proper list maintenance is performed by states. The Justice Department is requesting your state's VRL to test, analyze, and assess states' VRLs for proper list maintenance and compliance with federal law. In the event the Justice Department's analysis of a VRL results in list maintenance issues, insufficiency, inadequacy, anomalies, or concerns, the Justice Department will notify your state's point of contact of the issues to assist your state with curing.

The purpose of this MOU is to establish the parties' understanding as to the security protections for data transfer and data access by the Department of Justice of the electronic copy of the statewide voter registration list, including all fields requested by the Department of Justice.

#### **IV. TIMING OF AGREEMENT – TIME IS OF ESSENCE.**

Although the Justice Department is under no such obligation as a matter of law, because this Agreement is proposed, made, and to be entered into at your state's request as part of your state's transmission of its VRL to the Justice Department, this Agreement is to be fully executed within seven (7) days of the Justice Department presenting this Agreement to you. Both parties agree that no part of this Agreement or execution is intended to, or will, cause delay of the transmission of your state's VRL to the Justice Department for analysis.

#### **V. TIMING OF VRL/DATA TRANSFER.**

You agree to transfer an electronic copy of your state's complete statewide VRL/Data to the Civil Rights Division of the U.S. Department of Justice as described in Section III of this Agreement no later than five (5) business days from the execution of this Agreement, which is counted from the last day of the last signatory.

#### **VI. METHOD OF VRL/DATA ACCESS OR TRANSFER.**

The VRL will be submitted by your state via the Department of Justice's secure file-sharing system, i.e., Justice Enterprise File Sharing (JEFS"). A separate application to use JEFS must be completed and submitted by your state through the Civil Rights Help Desk. JEFS implements strict access controls to ensure that each user can only access their own files. All files and folders are tied to a specific user, and each user has defined permissions that govern how they may interact with those files (e.g., read, write, or read-only).

Whenever a user attempts to access a file or folder, JEFS validates the request against the assigned permissions to confirm that the user is explicitly authorized. This process guarantees that users can only access files and folders only where they have permission. Users are also limited to the authorized type of interaction with each file or folder. Within the Department of Justice, access to JEFS is restricted to specific roles: Litigation Support, IT staff, and Civil Rights Division staff.

## **VII. LOCATION OF DATA AND CUSTODIAL RESPONSIBILITY.**

The parties mutually agree that the Civil Rights Division (also “Department”) will be designated as “Custodian” of the file(s) and will be responsible for the observance of all conditions for use and for establishment and maintenance of security agreements as specified in this agreement to prevent unauthorized use. The information that the Department is collecting will be maintained consistent with the Privacy Act of 1974, 5 U.S.C. § 552a. The full list of routine uses for this collection of information can be found in the Systems of Record Notice (“SORN”) titled, JUSTICE/CRT – 001, “Central Civil Rights Division Index File and Associated Records,” 68 Fed. Reg. 47610-01, 611 (August 11, 2003); 70 Fed. Reg. 43904-01 (July 29, 2005); and 82 Fed. Reg. 24147-01 (May 25, 2017). It should be noted that the statutes cited for routine use include NVRA, HAVA, and the Civil Rights Act of 1960, and the Justice Department is making our request pursuant to those statutes. The records in the system of records are kept under the authority of 44 U.S.C. § 3101 and in the ordinary course of fulfilling the responsibility assigned to the Civil Rights Division under the provisions of 28 C.F.R. §§ 0.50, 0.51.

VRL/Data storage is similar to the restricted access provided on JEFS and complies with the SORN: Information in computer form is safeguarded and protected in accordance with applicable Department security regulations for systems of records. Only a limited number of staff members who are assigned a specific identification code will be able to use the computer to access

the stored information. However, a section may decide to allow its employees access to the system in order to perform their official duties.

All systems storing the VRL data will comply with all security requirements applicable to Justice Department systems, including but not limited to all Executive Branch system security requirements (e.g., requirements imposed by the Office of Management and Budget [OMB] and National Institute of Standards and Technology [NIST]), Department of Justice IT Security Standards, and Department of Justice Order 2640.2F.

#### **VIII. NVRA/HAVA COMPLIANT VOTER REGISTRATION LIST.**

After analysis and assessment of your state's VRL, the Justice Department will securely notify you or your state of any voter list maintenance issues, insufficiencies, inadequacies, deficiencies, anomalies, or concerns, the Justice Department found when testing, assessing, and analyzing your state's VRL for NVRA and HAVA compliance, i.e., that your state's VRL only includes eligible voters.

You agree therefore that within forty-five (45) days of receiving that notice from the Justice Department of any issues, insufficiencies, inadequacies, deficiencies, anomalies, or concerns, your state will clean its VRL/Data by removing ineligible voters and resubmit the updated VRL/Data to the Civil Rights Division of the Justice Department to verify proper list maintenance has occurred by your state pursuant to the NVRA and HAVA.

#### **IX. CONFIDENTIALITY & DEPARTMENT SAFEGUARDS.**

Any member of the Justice Department in possession of a VRL/Data will employ reasonable administrative, technical, and physical safeguards designed to protect the security and confidentiality of such data. Compliance with these safeguards will include secure user authentication protocols deploying either: (i) Two-Factor Authentication ("2FA"), which requires users to go through two layers of security before access is granted to the system; or (ii) the

assignment of unique user identifications to each person with computer access plus unique complex passwords, which are not vendor supplied default passwords.

The Department will activate audit logging for the records, files, and data containing the state's VRL/Data in order to identify abnormal use, as well as to track access control, on computers, servers and/or Devices containing the VRL/Data.

For all devices storing records, files, and data containing the VRL/Data: there is (i) up-to-date versions of system security agent software that includes endpoint protection and malware protection and reasonably up-to-date patches and virus definitions, or a version of such software that can still be supported with up-to-date patches and virus definitions, and is set to receive the most current security updates on a regular basis; and (ii) up-to-date operating system security patches designed to maintain the integrity of the personal information.

For all devices storing records, files, and data containing the VRL/Data: there is (i) controlled and locked physical access for the Device; and (ii) the prohibition of the connection of the Device to public or insecure home networks.

There will be no copying of records, files, or data containing the VRL/Data to unencrypted USB drives, CDs, or external storage. In addition, the use of devices outside of moving the records, files, or data to the final stored device location shall be limited.

Any notes, lists, memoranda, indices, compilations prepared or based on an examination of VRL/Data or any other form of information (including electronic forms), that quote from, paraphrase, copy, or disclose the VRL/Data with such specificity that the VRL/Data can be identified, or by reasonable logical extension can be identified will not be shared by the Department. Any summary results, however, may be shared by the Department.

In addition to the Department's enforcement efforts, the Justice Department may use the information you provide for certain routine, or pre-litigation or litigation purposes including:

present VRL/Data to a court, magistrate, or administrative tribunal; a contractor with the Department of Justice who needs access to the VRL/Data information in order to perform duties related to the Department's list maintenance verification procedures. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. § 552a(m).

#### **X. LOSS OR BREACH OF DATA.**

If a receiving party discovers any loss of VRL/Data, or a breach of security, including any actual or suspected unauthorized access, relating to VRL/Data, the receiving party shall, at its own expense immediately provide written notice to the producing party of such breach; investigate and make reasonable and timely efforts to remediate the effects of the breach, and provide the producing party with assurances reasonably satisfactory to the producing party that such breach shall not recur; and provide sufficient information about the breach that the producing party can reasonably ascertain the size and scope of the breach. The receiving party agrees to cooperate with the producing party or law enforcement in investigating any such security incident. In any event, the receiving party shall promptly take all necessary and appropriate corrective action to terminate unauthorized access.

#### **XI. DESTRUCTION OF DATA.**

The Department will destroy all VRL/Data associated with actual records as soon as the purposes of the list maintenance project have been accomplished and the time required for records retention pursuant to applicable law has passed. When the project is complete and such retention requirements by law expires, the Justice Department will:

1. Destroy all hard copies containing confidential data (e.g., shredding);
2. Archive and store electronic data containing confidential information offline in a secure location; and

3. All other data will be erased or maintained in a secured area.

## **XII. OTHER PROVISIONS.**

- A. Conflicts. This MOU constitutes the full MOU on this subject between the Department and your state. Any inconsistency or conflict between or among the provisions of this MOU, will be resolved in the following order of precedence: (1) this MOU and (2) other documents incorporated by reference in this MOU (e.g., transaction charges).
- B. Severability. Nothing in this MOU is intended to conflict with current law or regulation or the directives of Department, or the your state. If a term of this MOU is inconsistent with such authority, then that term shall be invalid but, to the extent allowable, the remaining terms and conditions of this MOU shall remain in full force and effect.
- C. Assignment. Your state may not assign this MOU, nor may it assign any of its rights or obligations under this MOU. To the extent allowable by law, this MOU shall inure to the benefit of, and be binding upon, any successors to the Justice Department and your state without restriction.
- D. Waiver. No waiver by either party of any breach of any provision of this MOU shall constitute a waiver of any other breach. Failure of either party to enforce at any time, or from time to time, any provision of this MOU shall not be construed to be a waiver thereof.
- E. Compliance with Other Laws. Nothing in this MOU is intended or should be construed to limit or affect the duties, responsibilities, and rights of the User Agency under the National Voter Registration Act, 52 U.S.C. § 20501 *et seq.*, as amended; the Help America Vote Act, 52 U.S.C. § 20901 *et seq.*, as amended; the Voting Rights Act, 52 U.S.C. § 10301 *et seq.*, as amended; and the Civil Rights Act, 52 U.S.C. § 10101 *et seq.*, as amended.
- F. Confidentiality of MOU. To the extent allowed by applicable law, this MOU, its contents, and the drafts and communications leading up to the execution of this MOU are deemed

by the parties as “confidential.” Any disclosures therefore could be made, if at all, pursuant to applicable laws or court orders requiring such disclosures.

**SIGNATURES**

VRL/Data Provider

State Agency Name:

Signature: \_\_\_\_\_ Date of Execution: \_\_\_\_\_

Authorized Signatory Name Printed: \_\_\_\_\_

Title: \_\_\_\_\_

Requester

Federal Agency Name: Civil Rights Division, U.S. Department of Justice

Signature: \_\_\_\_\_ Date of Execution: \_\_\_\_\_

Authorized Signatory Name Printed: \_\_\_\_\_

Title: \_\_\_\_\_



U.S. Department of Justice

Civil Rights Division

Office of the Assistant Attorney General

Washington, D.C. 20530

June 4, 2025

Wisconsin Elections Commission  
201 W. Washington Avenue  
Madison, WI 53703  
elections@wi.gov

The U.S. Election Assistance Commission  
633 3rd Street NW, Suite 200  
Washington, DC 20001  
ckelliher@eac.gov

Re: State of Wisconsin elections violation under Help America Vote Act

Election Commissioners,

As the State of Wisconsin's chief election officials, you are required to follow federal laws, including the Help America Vote Act ("HAVA"). Ensuring election integrity is of the highest degree of importance for my administration at the Civil Rights Division of the Department of Justice. As the Supreme Court has recognized the preservation of the integrity of the election process is a compelling interest. *Brnovich v. Democratic Nat'l Comm.*, 594 U.S. 647, 647 (2021).

Section 21112 (Sec. 402) of HAVA requires that each state establish a state-based administrative complaint procedure to enable voters to file a complaint regarding a HAVA violation they may observe or experience while voting. Meeting this requirement is a condition of receiving HAVA funding from the federal government. Records indicate that to date, Wisconsin has received over \$77,000,000 in federal funding from the U.S. Election Assistance Commission.<sup>1</sup>

Under HAVA, the administrative process is required to be:

- (1) Uniform and nondiscriminatory,
- (2) Allow any person who believes that there is a violation of any provision of subchapter III of HAVA (including a violation which has occurred, is occurring, or is about to occur) to file a complaint,
- (3) If the complainant requests, there shall be a hearing on the record,
- (4) If the state determines that there is a violation, it shall provide an appropriate remedy, and

<sup>1</sup> <https://www.eac.gov/funding-levels-by-state>

- (5) If the state determines that there is no violation, the state shall dismiss the complaint and publish the results.

Quite surprisingly, we have learned that the Wisconsin Elections Commission has refused to provide any administrative complaint process or hearing regarding HAVA complaints against the Commission. Rather, Wisconsin has decided to rely on a 2022 state court case opining that the Commission cannot police itself. (See attached letter).

These very actions by the Commission have left complainants alleging HAVA violations by the Commission without any recourse. The consequences were summarized by a federal judge who opined that the Commission's failure to provide a hearing to those who allege a HAVA complaint against the Commission are left without any decision or interpretation of the law. With no opportunity or means to appeal, complainants are left stranded with their grievances. *See Wis. Voter All. v. Millis, 720 F. Supp. 3d 703.*

We are hereby notifying the U.S. Election Assistance Commission of Wisconsin's failure to follow federal elections laws. Your actions justify a bar against the Wisconsin Elections Commission receiving any future funding from the U.S. Election Assistance Commission.

In addition to this formal notification, we fully expect that Wisconsin's Election Commission will immediately come into compliance with all federal election laws, including HAVA, forthwith. If you have any questions about this letter, please contact Deputy Assistant Attorney General of the Civil Rights Division, Michael Gates, at [michael.gates2@usdoj.gov](mailto:michael.gates2@usdoj.gov).

Regards,



Harmeet K. Dhillon  
Assistant Attorney General  
Civil Rights Division

Michael E. Gates  
Deputy Assistant Attorney General  
Civil Rights Division

Attachment: 2022 WEC letter

Scott Johnson Commissioner  
CIF - Northern Section [sjohnson@cifns.org](mailto:sjohnson@cifns.org)

Ryan Tos Commissioner  
CIF - Central Section [ryantos@cifcs.org](mailto:ryantos@cifcs.org)

Mike Garrison Commissioner  
CIF - Sac-Joaquin Section [mgarrison@cifsjs.org](mailto:mgarrison@cifsjs.org)

Francisco Navarro Commissioner  
CIF - Oakland Section [francisco.navarro@ousd.org](mailto:francisco.navarro@ousd.org)

Joe Heinz Commissioner  
CIF - San Diego Section [jheinz@cifds.org](mailto:jheinz@cifds.org)



**U.S. Department of Justice**

**Civil Rights Division**

---

*Voting Section  
950 Pennsylvania Ave, NW – 4CON  
Washington, DC 20530*

June 17, 2025

The Honorable Meagan Wolfe  
Administrator, Wisconsin Elections Commission  
201 W Washington Ave  
Madison, WI. 53703  
[meagan.wolfe@wisconsin.gov](mailto:meagan.wolfe@wisconsin.gov)  
[elections@wi.gov](mailto:elections@wi.gov)

Re: Request for Information Related to HAVA Compliance

Dear Ms. Wolfe:

As you are already aware, we have received several complaints regarding the Wisconsin Election Commission's ("WEC") compliance with the Help America Vote Act ("HAVA") 52 U.S.C. 20901 - 21145. Many of these complaints allege that WEC is failing to comply with the list maintenance procedure requirements of Section 303 of HAVA. To enable the Attorney General to determine if WEC is complying with these requirements, we are requesting the following information:

- (1) Describe how Wisconsin's computerized statewide voter registration list ("voter registration list") is coordinated with the databases of other state agencies, as required by HAVA Section 303(a)(1)(A). Provide the name of each state database used for coordination, and describe the procedures used for coordination, as well as how often the databases are coordinated with the voter registration list;
- (2) Describe the process by which voters who have been deemed ineligible are removed from the voter registration list pursuant to the list maintenance procedures referenced in HAVA Section 303(a)(2), the number of the voters currently deemed ineligible that remain on the voter registration list, and the basis for not having already removed them from the voter registration list;
- (3) Describe how WEC determines who is an "inactive" voter, pursuant to the list maintenance procedures referenced in HAVA Section 303(a)(2), and explain the process for removal of inactive voters from the voter registration list;
- (4) Describe the process by which any duplicate voter registrations are identified, including how the State determines what constitutes a duplicate voter registration record, and the process for their removal from the voter registration list under HAVA Section 303(a)(2)(B)(iii);


- (5) Describe the process by which voters who have moved outside the state and subsequently registered to vote in another state are identified and removed from the voter registration list under HAVA Section 303(a)(4)(A);
- (6) Describe the process by which registrants who are ineligible due to non-citizenship are identified and removed from the voter registration list; and
- (7) Please send us the current voter registration list. Please include both active and inactive voters.

Please provide this information within 20 days of the date of this letter. The information and materials may be sent by email to [voting.section@usdoj.gov](mailto:voting.section@usdoj.gov) or by FedEx or UPS to:

U.S. Department of Justice, Civil Rights Division  
Voting Section  
4 Constitution Square  
150 M Street NE, Room 8.923  
Washington, DC 20002

If you have any questions, please contact Kevin Muench at [kevin.muench@usdoj.gov](mailto:kevin.muench@usdoj.gov). We very much appreciate your cooperation in our effort to monitor HAVA compliance.

Sincerely,



Maureen Riordan  
Voting Section, Acting Chief

Michael E. Gates  
Deputy Assistant Attorney General  
Civil Rights Division

**From:** [Neff, Eric \(CRT\)](#)  
**To:** [elections@wi.gov](mailto:elections@wi.gov)  
**Subject:** Demand for Full Voter Roll from DOJ CRT  
**Date:** Tuesday, December 2, 2025 10:54:00 AM  
**Attachments:** [VRLData Sharing Agreement DOJ-WI.pdf](#)  
[image001.png](#)

---

To the Wisconsin Elections Commission:

Please consider this email a demand to provide within 7 days:

- An electronic copy of the full Wisconsin statewide voter registration list
  - This list is to include, pursuant to the Help America Vote Act, either the last four digits of the social security number, the driver's license number, or both.

This request is for the purpose of ensuring compliance with minimum standards and routine voter registration list maintenance.

If you have any questions, do not hesitate to contact me.

Thanks,

**Eric Neff**

Trial Attorney

Civil Rights Division

Department of Justice

150 M St. NE, Ste. 8-139

Washington, DC 20002

[Eric.Neff@usdoj.gov](mailto:Eric.Neff@usdoj.gov)

Cell: 202-532-3628





**U.S. Department of Justice**

Civil Rights Division

---

**CONFIDENTIAL MEMORANDUM OF UNDERSTANDING**

**I. PARTIES & POINTS OF CONTACT.**

Requester

Federal Agency Name: Civil Rights Division, U.S. Department of Justice

VRL/Data User:

Title:

Address:

Phone:

VRL/Data Provider

State Agency Name:

Custodian:

Title:

Address:

Phone:

The parties to this Memorandum of Understanding (“MOU” or “Agreement”) are the Department of Justice, Civil Rights Division (“Justice Department” or “Department”), and the State of Wisconsin (“You” or “your state”).

**II. AUTHORITY.**

By this Agreement, the State of Wisconsin (“You” or “your state”) has agreed to, and will, provide an electronic copy of your state’s complete statewide Voter Registration List (“VRL” or “VRL/Data”) to the Civil Rights Division of the U.S. Department of Justice (at times referred to as the “Department”). The VRL/Data must include, among other fields of data, the voter registrant’s full name, date of birth, residential address, his or her state driver’s license number or

the last four digits of the registrant's social security number as required under the HAVA to register individuals for federal elections. *See* 52 U.S.C. § 21083(a)(5)(A).

The authorities by which this information is requested by the Department of Justice are:

- National Voter Registration Act of 1993, 52 U.S.C. § 20501, *et seq.*
- Attorney General's authority under Section 11 of the NVRA to bring enforcement actions. *See* 52 U.S.C. § 20510(a).
- Help America Vote Act of 2002, 52 U.S.C. § 20901, *et seq.*
- Attorney General's authority to enforce the Help America Vote Act under 53 U.S.C. § 21111.
- Attorney General authority to request records pursuant to Title III of the Civil Rights Act of 1960 ("CRA"), codified at 52 U.S.C. § 20701, *et seq.*
- The Privacy Act of 1974, 5 U.S.C. § 552a, as amended.

### **III. PURPOSE.**

A VRL is a Voter Registration List pursuant to the NVRA and HAVA, commonly referred to as "voter roll," compiled by a state – often from information submitted by counties – containing a list of all the state's *eligible* voters. Regardless of the basis for ineligibility, ineligible voters do not appear on a state's VRL when proper list maintenance is performed by states. The Justice Department is requesting your state's VRL to test, analyze, and assess states' VRLs for proper list maintenance and compliance with federal law. In the event the Justice Department's analysis of a VRL results in list maintenance issues, insufficiency, inadequacy, anomalies, or concerns, the Justice Department will notify your state's point of contact of the issues to assist your state with curing.

The purpose of this MOU is to establish the parties' understanding as to the security protections for data transfer and data access by the Department of Justice of the electronic copy of the statewide voter registration list, including all fields requested by the Department of Justice.

#### **IV. TIMING OF AGREEMENT – TIME IS OF ESSENCE.**

Although the Justice Department is under no such obligation as a matter of law, because this Agreement is proposed, made, and to be entered into at your state's request as part of your state's transmission of its VRL to the Justice Department, this Agreement is to be fully executed within seven (7) days of the Justice Department presenting this Agreement to you. Both parties agree that no part of this Agreement or execution is intended to, or will, cause delay of the transmission of your state's VRL to the Justice Department for analysis.

#### **V. TIMING OF VRL/DATA TRANSFER.**

You agree to transfer an electronic copy of your state's complete statewide VRL/Data to the Civil Rights Division of the U.S. Department of Justice as described in Section III of this Agreement no later than five (5) business days from the execution of this Agreement, which is counted from the last day of the last signatory.

#### **VI. METHOD OF VRL/DATA ACCESS OR TRANSFER.**

The VRL will be submitted by your state via the Department of Justice's secure file-sharing system, i.e., Justice Enterprise File Sharing (JEFS"). A separate application to use JEFS must be completed and submitted by your state through the Civil Rights Help Desk. JEFS implements strict access controls to ensure that each user can only access their own files. All files and folders are tied to a specific user, and each user has defined permissions that govern how they may interact with those files (e.g., read, write, or read-only).

Whenever a user attempts to access a file or folder, JEFS validates the request against the assigned permissions to confirm that the user is explicitly authorized. This process guarantees that users can only access files and folders only where they have permission. Users are also limited to the authorized type of interaction with each file or folder. Within the Department of Justice, access to JEFS is restricted to specific roles: Litigation Support, IT staff, and Civil Rights Division staff.

## **VII. LOCATION OF DATA AND CUSTODIAL RESPONSIBILITY.**

The parties mutually agree that the Civil Rights Division (also “Department”) will be designated as “Custodian” of the file(s) and will be responsible for the observance of all conditions for use and for establishment and maintenance of security agreements as specified in this agreement to prevent unauthorized use. The information that the Department is collecting will be maintained consistent with the Privacy Act of 1974, 5 U.S.C. § 552a. The full list of routine uses for this collection of information can be found in the Systems of Record Notice (“SORN”) titled, JUSTICE/CRT – 001, “Central Civil Rights Division Index File and Associated Records,” 68 Fed. Reg. 47610-01, 611 (August 11, 2003); 70 Fed. Reg. 43904-01 (July 29, 2005); and 82 Fed. Reg. 24147-01 (May 25, 2017). It should be noted that the statutes cited for routine use include NVRA, HAVA, and the Civil Rights Act of 1960, and the Justice Department is making our request pursuant to those statutes. The records in the system of records are kept under the authority of 44 U.S.C. § 3101 and in the ordinary course of fulfilling the responsibility assigned to the Civil Rights Division under the provisions of 28 C.F.R. §§ 0.50, 0.51.

VRL/Data storage is similar to the restricted access provided on JEFS and complies with the SORN: Information in computer form is safeguarded and protected in accordance with applicable Department security regulations for systems of records. Only a limited number of staff members who are assigned a specific identification code will be able to use the computer to access

the stored information. However, a section may decide to allow its employees access to the system in order to perform their official duties.

All systems storing the VRL data will comply with all security requirements applicable to Justice Department systems, including but not limited to all Executive Branch system security requirements (e.g., requirements imposed by the Office of Management and Budget [OMB] and National Institute of Standards and Technology [NIST]), Department of Justice IT Security Standards, and Department of Justice Order 2640.2F.

#### **VIII. NVRA/HAVA COMPLIANT VOTER REGISTRATION LIST.**

After analysis and assessment of your state's VRL, the Justice Department will securely notify you or your state of any voter list maintenance issues, insufficiencies, inadequacies, deficiencies, anomalies, or concerns, the Justice Department found when testing, assessing, and analyzing your state's VRL for NVRA and HAVA compliance, i.e., that your state's VRL only includes eligible voters.

You agree therefore that within forty-five (45) days of receiving that notice from the Justice Department of any issues, insufficiencies, inadequacies, deficiencies, anomalies, or concerns, your state will clean its VRL/Data by removing ineligible voters and resubmit the updated VRL/Data to the Civil Rights Division of the Justice Department to verify proper list maintenance has occurred by your state pursuant to the NVRA and HAVA.

#### **IX. CONFIDENTIALITY & DEPARTMENT SAFEGUARDS.**

Any member of the Justice Department in possession of a VRL/Data will employ reasonable administrative, technical, and physical safeguards designed to protect the security and confidentiality of such data. Compliance with these safeguards will include secure user authentication protocols deploying either: (i) Two-Factor Authentication ("2FA"), which requires users to go through two layers of security before access is granted to the system; or (ii) the

assignment of unique user identifications to each person with computer access plus unique complex passwords, which are not vendor supplied default passwords.

The Department will activate audit logging for the records, files, and data containing the state's VRL/Data in order to identify abnormal use, as well as to track access control, on computers, servers and/or Devices containing the VRL/Data.

For all devices storing records, files, and data containing the VRL/Data: there is (i) up-to-date versions of system security agent software that includes endpoint protection and malware protection and reasonably up-to-date patches and virus definitions, or a version of such software that can still be supported with up-to-date patches and virus definitions, and is set to receive the most current security updates on a regular basis; and (ii) up-to-date operating system security patches designed to maintain the integrity of the personal information.

For all devices storing records, files, and data containing the VRL/Data: there is (i) controlled and locked physical access for the Device; and (ii) the prohibition of the connection of the Device to public or insecure home networks.

There will be no copying of records, files, or data containing the VRL/Data to unencrypted USB drives, CDs, or external storage. In addition, the use of devices outside of moving the records, files, or data to the final stored device location shall be limited.

Any notes, lists, memoranda, indices, compilations prepared or based on an examination of VRL/Data or any other form of information (including electronic forms), that quote from, paraphrase, copy, or disclose the VRL/Data with such specificity that the VRL/Data can be identified, or by reasonable logical extension can be identified will not be shared by the Department. Any summary results, however, may be shared by the Department.

In addition to the Department's enforcement efforts, the Justice Department may use the information you provide for certain routine, or pre-litigation or litigation purposes including:

present VRL/Data to a court, magistrate, or administrative tribunal; a contractor with the Department of Justice who needs access to the VRL/Data information in order to perform duties related to the Department's list maintenance verification procedures. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. § 552a(m).

#### **X. LOSS OR BREACH OF DATA.**

If a receiving party discovers any loss of VRL/Data, or a breach of security, including any actual or suspected unauthorized access, relating to VRL/Data, the receiving party shall, at its own expense immediately provide written notice to the producing party of such breach; investigate and make reasonable and timely efforts to remediate the effects of the breach, and provide the producing party with assurances reasonably satisfactory to the producing party that such breach shall not recur; and provide sufficient information about the breach that the producing party can reasonably ascertain the size and scope of the breach. The receiving party agrees to cooperate with the producing party or law enforcement in investigating any such security incident. In any event, the receiving party shall promptly take all necessary and appropriate corrective action to terminate unauthorized access.

#### **XI. DESTRUCTION OF DATA.**

The Department will destroy all VRL/Data associated with actual records as soon as the purposes of the list maintenance project have been accomplished and the time required for records retention pursuant to applicable law has passed. When the project is complete and such retention requirements by law expires, the Justice Department will:

1. Destroy all hard copies containing confidential data (e.g., shredding);
2. Archive and store electronic data containing confidential information offline in a secure location; and

3. All other data will be erased or maintained in a secured area.

## **XII. OTHER PROVISIONS.**

- A. Conflicts. This MOU constitutes the full MOU on this subject between the Department and your state. Any inconsistency or conflict between or among the provisions of this MOU, will be resolved in the following order of precedence: (1) this MOU and (2) other documents incorporated by reference in this MOU (e.g., transaction charges).
- B. Severability. Nothing in this MOU is intended to conflict with current law or regulation or the directives of Department, or the your state. If a term of this MOU is inconsistent with such authority, then that term shall be invalid but, to the extent allowable, the remaining terms and conditions of this MOU shall remain in full force and effect.
- C. Assignment. Your state may not assign this MOU, nor may it assign any of its rights or obligations under this MOU. To the extent allowable by law, this MOU shall inure to the benefit of, and be binding upon, any successors to the Justice Department and your state without restriction.
- D. Waiver. No waiver by either party of any breach of any provision of this MOU shall constitute a waiver of any other breach. Failure of either party to enforce at any time, or from time to time, any provision of this MOU shall not be construed to be a waiver thereof.
- E. Compliance with Other Laws. Nothing in this MOU is intended or should be construed to limit or affect the duties, responsibilities, and rights of the User Agency under the National Voter Registration Act, 52 U.S.C. § 20501 *et seq.*, as amended; the Help America Vote Act, 52 U.S.C. § 20901 *et seq.*, as amended; the Voting Rights Act, 52 U.S.C. § 10301 *et seq.*, as amended; and the Civil Rights Act, 52 U.S.C. § 10101 *et seq.*, as amended.
- F. Confidentiality of MOU. To the extent allowed by applicable law, this MOU, its contents, and the drafts and communications leading up to the execution of this MOU are deemed

by the parties as “confidential.” Any disclosures therefore could be made, if at all, pursuant to applicable laws or court orders requiring such disclosures.

**SIGNATURES**

VRL/Data Provider

State Agency Name:

Signature: \_\_\_\_\_ Date of Execution: \_\_\_\_\_

Authorized Signatory Name Printed: \_\_\_\_\_

Title: \_\_\_\_\_

Requester

Federal Agency Name: Civil Rights Division, U.S. Department of Justice

Signature: \_\_\_\_\_ Date of Execution: \_\_\_\_\_

Authorized Signatory Name Printed: \_\_\_\_\_

Title: \_\_\_\_\_



---

**From:** Neff, Eric (CRT) [Eric.Neff@usdoj.gov]  
**Sent:** 12/2/2025 3:54:48 PM  
**To:** elections@wi.gov  
**Subject:** Demand for Full Voter Roll from DOJ CRT  
**Attachments:** VRLData Sharing Agreement DOJ-WI.pdf

To the Wisconsin Elections Commission:

Please consider this email a demand to provide within 7 days:

- An electronic copy of the full Wisconsin statewide voter registration list
  - o This list is to include, pursuant to the Help America Vote Act, either the last four digits of the social security number, the driver's license number, or both.

This request is for the purpose of ensuring compliance with minimum standards and routine voter registration list maintenance.

If you have any questions, do not hesitate to contact me.

Thanks,

**Eric Neff**

Trial Attorney  
Civil Rights Division  
Department of Justice  
150 M St. NE, Ste. 8-139  
Washington, DC 20002  
Eric.Neff@usdoj.gov  
Cell: 202-532-3628





**U.S. Department of Justice**

Civil Rights Division

---

**CONFIDENTIAL MEMORANDUM OF UNDERSTANDING**

**I. PARTIES & POINTS OF CONTACT.**

Requester

Federal Agency Name: Civil Rights Division, U.S. Department of Justice

VRL/Data User:

Title:

Address:

Phone:

VRL/Data Provider

State Agency Name:

Custodian:

Title:

Address:

Phone:

The parties to this Memorandum of Understanding (“MOU” or “Agreement”) are the Department of Justice, Civil Rights Division (“Justice Department” or “Department”), and the State of Wisconsin (“You” or “your state”).

**II. AUTHORITY.**

By this Agreement, the State of Wisconsin (“You” or “your state”) has agreed to, and will, provide an electronic copy of your state’s complete statewide Voter Registration List (“VRL” or “VRL/Data”) to the Civil Rights Division of the U.S. Department of Justice (at times referred to as the “Department”). The VRL/Data must include, among other fields of data, the voter registrant’s full name, date of birth, residential address, his or her state driver’s license number or

the last four digits of the registrant's social security number as required under the HAVA to register individuals for federal elections. *See* 52 U.S.C. § 21083(a)(5)(A).

The authorities by which this information is requested by the Department of Justice are:

- National Voter Registration Act of 1993, 52 U.S.C. § 20501, *et seq.*
- Attorney General's authority under Section 11 of the NVRA to bring enforcement actions. *See* 52 U.S.C. § 20510(a).
- Help America Vote Act of 2002, 52 U.S.C. § 20901, *et seq.*
- Attorney General's authority to enforce the Help America Vote Act under 53 U.S.C. § 21111.
- Attorney General authority to request records pursuant to Title III of the Civil Rights Act of 1960 ("CRA"), codified at 52 U.S.C. § 20701, *et seq.*
- The Privacy Act of 1974, 5 U.S.C. § 552a, as amended.

### **III. PURPOSE.**

A VRL is a Voter Registration List pursuant to the NVRA and HAVA, commonly referred to as "voter roll," compiled by a state – often from information submitted by counties – containing a list of all the state's *eligible* voters. Regardless of the basis for ineligibility, ineligible voters do not appear on a state's VRL when proper list maintenance is performed by states. The Justice Department is requesting your state's VRL to test, analyze, and assess states' VRLs for proper list maintenance and compliance with federal law. In the event the Justice Department's analysis of a VRL results in list maintenance issues, insufficiency, inadequacy, anomalies, or concerns, the Justice Department will notify your state's point of contact of the issues to assist your state with curing.

The purpose of this MOU is to establish the parties' understanding as to the security protections for data transfer and data access by the Department of Justice of the electronic copy of the statewide voter registration list, including all fields requested by the Department of Justice.

#### **IV. TIMING OF AGREEMENT – TIME IS OF ESSENCE.**

Although the Justice Department is under no such obligation as a matter of law, because this Agreement is proposed, made, and to be entered into at your state's request as part of your state's transmission of its VRL to the Justice Department, this Agreement is to be fully executed within seven (7) days of the Justice Department presenting this Agreement to you. Both parties agree that no part of this Agreement or execution is intended to, or will, cause delay of the transmission of your state's VRL to the Justice Department for analysis.

#### **V. TIMING OF VRL/DATA TRANSFER.**

You agree to transfer an electronic copy of your state's complete statewide VRL/Data to the Civil Rights Division of the U.S. Department of Justice as described in Section III of this Agreement no later than five (5) business days from the execution of this Agreement, which is counted from the last day of the last signatory.

#### **VI. METHOD OF VRL/DATA ACCESS OR TRANSFER.**

The VRL will be submitted by your state via the Department of Justice's secure file-sharing system, i.e., Justice Enterprise File Sharing (JEFS"). A separate application to use JEFS must be completed and submitted by your state through the Civil Rights Help Desk. JEFS implements strict access controls to ensure that each user can only access their own files. All files and folders are tied to a specific user, and each user has defined permissions that govern how they may interact with those files (e.g., read, write, or read-only).

Whenever a user attempts to access a file or folder, JEFS validates the request against the assigned permissions to confirm that the user is explicitly authorized. This process guarantees that users can only access files and folders only where they have permission. Users are also limited to the authorized type of interaction with each file or folder. Within the Department of Justice, access to JEFS is restricted to specific roles: Litigation Support, IT staff, and Civil Rights Division staff.

## **VII. LOCATION OF DATA AND CUSTODIAL RESPONSIBILITY.**

The parties mutually agree that the Civil Rights Division (also “Department”) will be designated as “Custodian” of the file(s) and will be responsible for the observance of all conditions for use and for establishment and maintenance of security agreements as specified in this agreement to prevent unauthorized use. The information that the Department is collecting will be maintained consistent with the Privacy Act of 1974, 5 U.S.C. § 552a. The full list of routine uses for this collection of information can be found in the Systems of Record Notice (“SORN”) titled, JUSTICE/CRT – 001, “Central Civil Rights Division Index File and Associated Records,” 68 Fed. Reg. 47610-01, 611 (August 11, 2003); 70 Fed. Reg. 43904-01 (July 29, 2005); and 82 Fed. Reg. 24147-01 (May 25, 2017). It should be noted that the statutes cited for routine use include NVRA, HAVA, and the Civil Rights Act of 1960, and the Justice Department is making our request pursuant to those statutes. The records in the system of records are kept under the authority of 44 U.S.C. § 3101 and in the ordinary course of fulfilling the responsibility assigned to the Civil Rights Division under the provisions of 28 C.F.R. §§ 0.50, 0.51.

VRL/Data storage is similar to the restricted access provided on JEFS and complies with the SORN: Information in computer form is safeguarded and protected in accordance with applicable Department security regulations for systems of records. Only a limited number of staff members who are assigned a specific identification code will be able to use the computer to access

the stored information. However, a section may decide to allow its employees access to the system in order to perform their official duties.

All systems storing the VRL data will comply with all security requirements applicable to Justice Department systems, including but not limited to all Executive Branch system security requirements (e.g., requirements imposed by the Office of Management and Budget [OMB] and National Institute of Standards and Technology [NIST]), Department of Justice IT Security Standards, and Department of Justice Order 2640.2F.

#### **VIII. NVRA/HAVA COMPLIANT VOTER REGISTRATION LIST.**

After analysis and assessment of your state's VRL, the Justice Department will securely notify you or your state of any voter list maintenance issues, insufficiencies, inadequacies, deficiencies, anomalies, or concerns, the Justice Department found when testing, assessing, and analyzing your state's VRL for NVRA and HAVA compliance, i.e., that your state's VRL only includes eligible voters.

You agree therefore that within forty-five (45) days of receiving that notice from the Justice Department of any issues, insufficiencies, inadequacies, deficiencies, anomalies, or concerns, your state will clean its VRL/Data by removing ineligible voters and resubmit the updated VRL/Data to the Civil Rights Division of the Justice Department to verify proper list maintenance has occurred by your state pursuant to the NVRA and HAVA.

#### **IX. CONFIDENTIALITY & DEPARTMENT SAFEGUARDS.**

Any member of the Justice Department in possession of a VRL/Data will employ reasonable administrative, technical, and physical safeguards designed to protect the security and confidentiality of such data. Compliance with these safeguards will include secure user authentication protocols deploying either: (i) Two-Factor Authentication ("2FA"), which requires users to go through two layers of security before access is granted to the system; or (ii) the

assignment of unique user identifications to each person with computer access plus unique complex passwords, which are not vendor supplied default passwords.

The Department will activate audit logging for the records, files, and data containing the state's VRL/Data in order to identify abnormal use, as well as to track access control, on computers, servers and/or Devices containing the VRL/Data.

For all devices storing records, files, and data containing the VRL/Data: there is (i) up-to-date versions of system security agent software that includes endpoint protection and malware protection and reasonably up-to-date patches and virus definitions, or a version of such software that can still be supported with up-to-date patches and virus definitions, and is set to receive the most current security updates on a regular basis; and (ii) up-to-date operating system security patches designed to maintain the integrity of the personal information.

For all devices storing records, files, and data containing the VRL/Data: there is (i) controlled and locked physical access for the Device; and (ii) the prohibition of the connection of the Device to public or insecure home networks.

There will be no copying of records, files, or data containing the VRL/Data to unencrypted USB drives, CDs, or external storage. In addition, the use of devices outside of moving the records, files, or data to the final stored device location shall be limited.

Any notes, lists, memoranda, indices, compilations prepared or based on an examination of VRL/Data or any other form of information (including electronic forms), that quote from, paraphrase, copy, or disclose the VRL/Data with such specificity that the VRL/Data can be identified, or by reasonable logical extension can be identified will not be shared by the Department. Any summary results, however, may be shared by the Department.

In addition to the Department's enforcement efforts, the Justice Department may use the information you provide for certain routine, or pre-litigation or litigation purposes including:

present VRL/Data to a court, magistrate, or administrative tribunal; a contractor with the Department of Justice who needs access to the VRL/Data information in order to perform duties related to the Department's list maintenance verification procedures. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. § 552a(m).

#### **X. LOSS OR BREACH OF DATA.**

If a receiving party discovers any loss of VRL/Data, or a breach of security, including any actual or suspected unauthorized access, relating to VRL/Data, the receiving party shall, at its own expense immediately provide written notice to the producing party of such breach; investigate and make reasonable and timely efforts to remediate the effects of the breach, and provide the producing party with assurances reasonably satisfactory to the producing party that such breach shall not recur; and provide sufficient information about the breach that the producing party can reasonably ascertain the size and scope of the breach. The receiving party agrees to cooperate with the producing party or law enforcement in investigating any such security incident. In any event, the receiving party shall promptly take all necessary and appropriate corrective action to terminate unauthorized access.

#### **XI. DESTRUCTION OF DATA.**

The Department will destroy all VRL/Data associated with actual records as soon as the purposes of the list maintenance project have been accomplished and the time required for records retention pursuant to applicable law has passed. When the project is complete and such retention requirements by law expires, the Justice Department will:

1. Destroy all hard copies containing confidential data (e.g., shredding);
2. Archive and store electronic data containing confidential information offline in a secure location; and

3. All other data will be erased or maintained in a secured area.

## **XII. OTHER PROVISIONS.**

- A. Conflicts. This MOU constitutes the full MOU on this subject between the Department and your state. Any inconsistency or conflict between or among the provisions of this MOU, will be resolved in the following order of precedence: (1) this MOU and (2) other documents incorporated by reference in this MOU (e.g., transaction charges).
- B. Severability. Nothing in this MOU is intended to conflict with current law or regulation or the directives of Department, or the your state. If a term of this MOU is inconsistent with such authority, then that term shall be invalid but, to the extent allowable, the remaining terms and conditions of this MOU shall remain in full force and effect.
- C. Assignment. Your state may not assign this MOU, nor may it assign any of its rights or obligations under this MOU. To the extent allowable by law, this MOU shall inure to the benefit of, and be binding upon, any successors to the Justice Department and your state without restriction.
- D. Waiver. No waiver by either party of any breach of any provision of this MOU shall constitute a waiver of any other breach. Failure of either party to enforce at any time, or from time to time, any provision of this MOU shall not be construed to be a waiver thereof.
- E. Compliance with Other Laws. Nothing in this MOU is intended or should be construed to limit or affect the duties, responsibilities, and rights of the User Agency under the National Voter Registration Act, 52 U.S.C. § 20501 *et seq.*, as amended; the Help America Vote Act, 52 U.S.C. § 20901 *et seq.*, as amended; the Voting Rights Act, 52 U.S.C. § 10301 *et seq.*, as amended; and the Civil Rights Act, 52 U.S.C. § 10101 *et seq.*, as amended.
- F. Confidentiality of MOU. To the extent allowed by applicable law, this MOU, its contents, and the drafts and communications leading up to the execution of this MOU are deemed

by the parties as “confidential.” Any disclosures therefore could be made, if at all, pursuant to applicable laws or court orders requiring such disclosures.

**SIGNATURES**

VRL/Data Provider

State Agency Name:

Signature: \_\_\_\_\_ Date of Execution: \_\_\_\_\_

Authorized Signatory Name Printed: \_\_\_\_\_

Title: \_\_\_\_\_

Requester

Federal Agency Name: Civil Rights Division, U.S. Department of Justice

Signature: \_\_\_\_\_ Date of Execution: \_\_\_\_\_

Authorized Signatory Name Printed: \_\_\_\_\_

Title: \_\_\_\_\_



State of New Jersey

DEPARTMENT OF LAW AND PUBLIC SAFETY  
DIVISION OF LAW  
25 MARKET STREET  
PO BOX 0112  
TRENTON, NJ 08625-0112

PHILIP D. MURPHY  
Governor

TAHESHA L. WAY  
Lt. Governor

MATTHEW J. PLATKIN  
Attorney General

MICHAEL C. WALTERS  
Acting Director

August 21, 2025

Via Email (maureen.riordan2@usdoj.com)

Maureen Riordan  
Acting Chief, Voting Section  
Civil Rights Division  
U.S. Department of Justice  
950 Pennsylvania Avenue, NW – 4CON  
Washington, DC 20530

Re: Request for Voter Registration List

Dear Ms. Riordan:

On behalf of the Division of Elections (“DOE”) in the New Jersey Department of State, I write in response to Assistant Attorney General Harmeet K. Dhillon’s letter to Lieutenant Governor Way dated August 14, 2025, to respectfully seek clarification of the request.

By way of background, in response to the letter from you and Deputy Assistant Attorney General Michael E. Gates to Lieutenant Governor Way dated July 15, 2025, DOE provided the U.S. Department of Justice (“DOJ”) with a copy of New Jersey’s current voter registration list. That list contained the names, addresses, and other information about individual registered voters that may be disclosed consistent with New Jersey privacy laws, and without exposing certain especially sensitive, confidential personally identifiable information such as Social Security and driver license numbers. See, e.g., N.J. Stat. Ann. § 47:1A-5.3(b). This is the same version of the voter registration list that DOE regularly discloses in response to proper requests under the National Voter Registration Act (“NVRA”), see 52 U.S.C. § 20507(i)(1), and other legal authorities.

In her follow-up letter dated August 14, 2025, Assistant Attorney General Dhillon requests an “electronic copy of the statewide [voter registration list] ... contain[ing] *all fields*, including the registrant’s ... state driver’s license number or the last four digits of the registrant’s social security number” (emphasis in original). This request raises important legal questions, and the New Jersey Department of State and DOE take very seriously their responsibility to safeguard information that is protected under New Jersey law and entrusted to DOE by New Jersey residents in order to enable them to exercise their fundamental right to vote. Accordingly, and in light of the invitation in the August 14 letter to contact you “[s]hould further clarification [of the request] be required,” we would be grateful for additional information to enable us to sufficiently consider and respond to the request.



HUGHES JUSTICE COMPLEX · TELEPHONE: (609) 376-3232 FAX: (609) 292-7822  
New Jersey is an Equal Opportunity Employer · Printed on Recycled Paper and Recyclable



CRT-0003252

First, the August 14 letter states that the purpose of requesting New Jersey's entire voter registration list, including fields containing confidential personally identifiable information, is "to assess [New Jersey's] compliance with the statewide VRL maintenance provisions of the [NVRA]." The NVRA requires States to "conduct a general program that makes a reasonable effort to remove the names of ineligible voters from the official lists of eligible voters by reason of" death or a change in residence. 52 U.S.C. § 20507(a)(4); see also *Bellitto v. Snipes*, 935 F.3d 1192, 1202 (11th Cir. 2019) ("Nothing in HAVA [the Help America Vote Act] broadens the scope of the NVRA's list-maintenance obligations."). It is not clear that obtaining confidential personally identifiable information of individual registered voters is necessary to determine whether New Jersey is conducting a general program that makes a reasonable effort to remove the names of individuals who are deceased or have changed residence.<sup>1</sup> Nor is it apparent how the DOJ intends to use the requested information to make its compliance determination. Cf. *Chao v. Community Trust Co.*, 474 F.3d 75, 79 (3d Cir. 2007) ("To enforce an administrative subpoena, an agency must demonstrate" that "the inquiry [is] within the authority of the agency" and "the information sought [is] reasonably relevant to the authorized inquiry."). We would therefore appreciate clarification regarding the DOJ's need for and intended use of the information sought.

Second, the August 14 letter invokes the federal Civil Rights Act of 1960, a statute "designed to secure a more effective protection of the right to vote." *State of Ala. ex rel. Gallion v. Rogers*, 187 F. Supp. 848, 853 (M.D. Ala. 1960), *aff'd sub nom. Dinkens v. Att'y Gen. of U. S.*, 285 F.2d 430 (5th Cir. 1961). The Civil Rights Act of 1960 grants the U.S. Attorney General the authority to demand from state and local officials "records and papers" retained "for a period of twenty-two months from the date of any general, special, or primary [federal] election ... relating to any application, registration, payment of poll tax, or other act requisite to voting in such election," see 52 U.S.C. §§ 20701, 20703, to enable the Attorney General to investigate "question[s] concerning infringement or denial of [individuals'] constitutional voting rights," *Kennedy v. Lynd*, 306 F.2d 222, 228 (5th Cir. 1962); see also *id.* (The "purpose [of authorizing demands by the U.S. Attorney General for records under Title III of the Civil Rights Act of 1960] is to enable the Attorney General to determine whether [42 U.S.C.] § 1971 [currently codified as amended at 52 U.S.C. § 10101] suits or similar actions should be instituted."). Any such demand for records "shall contain a statement of the basis and the purpose therefor." *Id.* § 20703. The August 14 letter states that "[t]he purpose of [DOJ's] request" for New Jersey's complete voter registration list, including confidential personally identifiable information, "is to ascertain New Jersey's compliance with the list maintenance requirements of the NVRA and HAVA." But the letter does not provide the *basis* for the request pursuant to 52 U.S.C. § 20703, which is separate and distinct from the purpose of the request. *Id.* (requiring that a demand for records must contain "a statement of the basis *and* the purpose therefor" (emphasis added)). To aid our evaluation of the DOJ's request under the Civil Rights Act, we respectfully ask you to provide, pursuant to 52 U.S.C. § 20703, the basis for the request.

Third, as the August 14 letter appears to acknowledge, the request for New Jersey to transfer massive amounts of confidential personally identifying information to the DOJ raises issues regarding compliance with the federal Privacy Act, 5 U.S.C. § 552 *et seq.*, as well as the DPPA, as noted above. However, the August 14 letter does not address whether there is an existing System of Records Notice ("SORN") that adequately covers the requested records, or whether DOJ intends to publish a new SORN and the expected timeline for such publication. Nor does the letter address whether the DOJ anticipates

---

<sup>1</sup> Understanding how the information requested would further a proper law-enforcement function of the DOJ will also help my office assess the August 14 letter's assertion that the requested disclosure of driver license numbers falls within the exception set forth in the Drivers Privacy Protection Act ("DPPA") (described in the August 14 letter as the "Drivers License Protection Act") for use by a government agency "carrying out its functions." 18 U.S.C. § 2721(b)(1).

AAG Melissa D. Schaffer  
August 21, 2025


disclosing any of the records sought to other federal agencies or other entities or individuals, and if so, under what circumstances and for what purpose or purposes. See, e.g., 5 U.S.C. § 552a(b). We would be grateful for clarity on these points. Again, to ensure adequate protection of the requested personally identifiable information consistent with New Jersey law, the State would like to better understand how the information may be used and with whom it may be shared.

New Jersey's elections officials take extremely seriously their election duties. We appreciate the opportunity to seek clarification and thank you in advance for providing the information requested above.

Very truly yours,

MATTHEW J. PLATKIN  
ATTORNEY GENERAL OF NEW JERSEY

By:

  
\_\_\_\_\_  
Melissa Dutton Schaffer  
Assistant Attorney General

cc: Harmeet K. Dhillon  
Assistant Attorney General  
U.S. Department of Justice  
Civil Rights Division

Donna Barber, Director  
Department of State  
Division of Elections