ACLU of Hawai'i Foundation
EMILY M. HILLS 11208
JONGWOOK "WOOKIE" KIM 11020
P.O. Box 3410
Honolulu, HI 96801
T: (808) 522-5905
F: (808) 522-5909
ehills@acluhawaii.org
wkim@acluhawaii.org

American Civil Liberties Union Foundation
THERESA J. LEE*
ETHAN HERENSTEIN*
WILLIAM HUGHES*
SOPHIA LIN LAKIN*
125 Broad St., 18th Floor
New York, NY 10004
T: (212) 549-2500
F: (332) 234-9285
tlee@aclu.org
eherenstein@aclu.org
whughes@aclu.org
slakin@aclu.org

**admitted pro hac vice*

Counsel for Amici Curiae

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF HAWAI'I

UNITED STATES OF AMERICA,

Plaintiff,

v.

SCOTT NAGO, in his official capacity as Chief Elections Officer for the State of Hawaii,

Defendant.

No. 1:25-cv-00522-LEK-RT

BRIEF OF AMICI CURIAE COMMON CAUSE, NEIL ABERCROMBIE, AND KATHERINE HAMMES IN SUPPORT OF DEFENDANTS' MOTIONS TO DISMISS AND IN OPPOSITION TO PLAINTIFF'S MOTION TO COMPEL; EXHIBIT 1

Hearing: April 3, 2026 at 11:00 a.m.
Judge: Hon. Leslie E. Kobayashi
Trial Date: TBD
Related: ECF Nos. 1, 5, 52, 53

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Other Authorities

INTRODUCTION

The right to vote is "of the most fundamental significance under our constitutional structure," *No Labels Party of Ariz. v. Fontes*, 142 F.4th 1226, 1231 (9th Cir. 2025), and "preservative of all [other] rights," *Yick Wo v. Hopkins*, 118 U.S. 356, 370 (1886). Against this backdrop, Congress has repeatedly legislated to protect the franchise, including through the Voting Rights Act, 52 U.S.C. § 10301 *et seq.*; the National Voter Registration Act ("NVRA"), 52 U.S.C. § 20501 *et seq.*; the Help America Vote Act ("HAVA"), 52 U.S.C. § 20901 *et seq.*; and the Civil Rights Act of 1960 ("CRA"), 52 U.S.C. § 20701 *et seq*. These statutes were all passed for the express purpose of ensuring that all eligible Americans—especially racial minorities and voters with disabilities—may participate in free, fair, and secure elections.

This case concerns the proper scope of one such statute: Title III of the CRA, the Act's election-records provision. As the Department of Justice itself has explained, Congress enacted Title III to "secure a more effective protection of the right to vote." U.S. Dep't of Just., C.R. Div., *Federal Law Constraints on Post-Election "Audits"* (July 28, 2021) (citing *Alabama ex rel. Gallion v. Rogers*, 187 F. Supp. 848, 853 (M.D. Ala. 1960); H.R. Rep. No. 86-956, at 7 (1959)). Yet in this action—like dozens of similar suits filed nationwide—the United States invokes that provision to demand disclosure of sensitive voter data to which it is not entitled.

Specifically, the federal government seeks Hawai'i's unredacted voter file,

which contains highly sensitive personal information, including full birth dates and driver's license numbers or partial Social Security numbers for every registered voter in the state. That demand conflicts with Title III's text and purpose. Rather than protecting voter access, disclosure of such information for reasons unrelated to enforcing voting rights would deter participation and undermine confidence in elections, especially here given that the United States has not fully or accurately stated "the basis and the purpose" of its request, as the statute expressly requires. 52 U.S.C. § 20703.

The United States' interpretation inverts Title III's function and frustrates the objectives of other federal election laws, as well as state protections for voter privacy. *Amici* Common Cause, Neil Abercrombie, and Katherine Hammes therefore respectfully submit this brief in support of dismissal.

INTEREST OF AMICI CURIAE

Amici Curiae are Common Cause, a nonpartisan, good-government organization dedicated to grassroots voter engagement both nationally and specifically in Hawai‘i, and Neil Abercrombie and Katherine Hammes, Hawai‘i voters. Common Cause has an interest in protecting the voting and privacy rights of its members and all Hawai‘i voters. It also has an organizational interest in encouraging Hawai‘i residents to register to vote and to participate in the political

process. Mr. Abercrombie and Ms. Hammes have a strong interest in the security of their personal, private data.

All of these interests would be harmed by the relief that the federal government seeks in this case. Disclosure of voters' personal information would invade the privacy of all Common Cause's members who are registered Hawai'i voters, as well as Mr. Abercrombie and Ms. Hammes, and could potentially chill their political speech. The United States' requested relief would also pose a particular risk to certain groups of voters, such as naturalized citizens (including Ms. Hammes), voters with prior felony convictions, and people who have recently moved, all of whom are more likely to get caught up in improper voter purges. The requested relief would also harm Common Cause as an organization, due to its work related to voter registration and political participation. This work requires trust, and voter trust would be imperiled by the disclosure the United States seeks.

BACKGROUND

In May 2025, Plaintiff United States, through its Department of Justice ("DOJ"), began sending letters to election officials in at least 40 states, making escalating demands for production of statewide voter registration databases, with plans to gather data from all 50 states. *See* Kaylie Martinez-Ochoa, Eileen O'Connor, & Patrick Berry, Tracker of Justice Department Requests for Voter Information, Brennan Ctr. for Just. (updated Feb. 27, 2026), https://perma.cc/8YMZ-AD97.

In September 2025, DOJ requested a copy of Hawai‘i’s entire, unredacted statewide voter registration list that “contain[s] *all fields*,” including “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.” Ex. 1 to U.S. Mot. to Compel, Letter from Harmeet K. Dhillon, DOJ Assistant Attorney General, to Scott T. Nago, Hawai‘i Chief Election Officer, at 2-3 (Sept. 8, 2025), Dkt. No. 5-2 (“DOJ Ltr.”); *see also* Compl. ¶ 20. DOJ cited three sources of authority—the NVRA, HAVA, and CRA—for its records request, and stated without explanation that “[t]he purpose of this request is to ascertain Hawaii’s compliance with the list maintenance requirements of the NVRA and HAVA.” DOJ Ltr. at 3; *see* Compl. ¶¶ 19-21. It waved away any privacy issues, claiming that the federal prohibition on sharing voter information obtained under the CRA with the public was sufficient to assuage concerns. DOJ Ltr. 3 (citing 52 U.S.C. § 20704).

Officer Nago’s office responded on September 22, 2025, declining to transmit the requested information. Ex. 2 to U.S. Mot. to Compel, Letter from Thomas J. Hughes, Hawai‘i Deputy Solicitor General, to Harmeet K. Dhillon at 6-8 (Sept. 22, 2025), Dkt. No. 5-2 (“HI Ltr.”); *see* Compl. ¶ 22. The Officer responded that the cited authorities did not permit its demand for a full, unredacted copy of Hawai‘i’s voter list and asserted that DOJ had not explained why the data was needed to assess

NVRA or HAVA compliance. HI Ltr. at 7. He also raised concerns about whether the request complied with the Privacy Act. *Id.* at 7-8.

On December 1, 2025, DOJ's "new contact for the Voting Section," Eric Neff, sent a follow-up email, indicating that he was "not aware of" the Officer's September 22 letter and seeking a position on DOJ's September 8 letter. Ex. 3 to U.S. Mot. to Compel, Email from Eric Neff to elections@hawaii.gov at 10 (Dec. 1, 2025), Dkt. No. 5-2 ("DOJ Email"). DOJ also attached a proposed memorandum of understanding for Hawai'i's consideration to address "potential concerns a state might rightfully raise regarding its citizens' private data and identifying information." *Id.*; Compl. ¶ 25; *see also, e.g.*, Ex. 2, U.S. Dep't of Just., Civ. Div., Confidential Mem. of Understanding ("MOU").[1] One of Hawai'i's Deputy Solicitors General responded, attaching the Officer's September 22 letter and clarifying that Hawai'i's basis for declining to produce the requested records was outlined in the September 22 letter. Ex. 4 to U.S. Mot. to Compel, Emails from Thomas J. Hughes to Eric Neff at 12 (Dec. 2, 2025), Dkt. No. 5-2 ("HI Emails").

[1] In addition to incorporating the MOU by reference in its Complaint, Compl. ¶ 25, the United States has represented in court that it intended for a number of states to sign MOUs as to its requests for state voter files, Ex. 6 to Mot. to Intervene, Hr'g Tr. at 72-73, 90, *United States v. Weber*, No. 2:25-cv-09149 (C.D. Cal. Dec. 4, 2025), Dkt. No. 24-6 (DOJ attorney discussing MOU), and a version of the MOU signed by Texas and the United States has become publicly available. *See* Ex. 1 ("MOU"). This Court can take judicial notice of the MOU as a government document produced by DOJ. *See Tia v. Suzuki*, No. 13-cv-00157, 2013 WL 2009031, at *1 (D. Haw. May 10, 2013).

The United States responded by filing this lawsuit, which is one of at least thirty that DOJ has initiated recently to compel states and election officials to disclose sensitive voter data.[2] DOJ's request for private, sensitive voter data appears to be in connection with never-before-seen efforts by the United States to construct a national voter database, and to otherwise use untested forms of database matching to scrutinize voter rolls—in short, as part of President Trump's self-described efforts to "nationalize" elections.[3]

According to reporting, DOJ employees "have been clear that they are interested in a central, federal database of voter information." Devlin Barrett & Nick Corasaniti, *Trump Administration Quietly Seeks to Build National Voter Roll*, N.Y.

---

[2] *See* Press Release, U.S. Dep't of Just., *Justice Department Sues Five Additional States for Failure to Produce Voter Rolls* (Feb. 26, 2026), https://perma.cc/67UZ-KJFY; Press Release, U.S. Dep't of Just., *Justice Department Sues Virginia for Failure to Produce Voter Rolls* (Jan. 16, 2026), https://perma.cc/3L8Q-SJM5; Press Release, U.S. Dep't of Just., *Justice Department Sues Arizona and Connecticut for Failure to Produce Voter Rolls* (Jan. 6, 2026), https://perma.cc/6QP2-8ZXC; Press Release, U.S. Dep't of Just., *Justice Department Sues Four States for Failure to Produce Voter Rolls* (Dec. 18, 2025), https://perma.cc/HHJ7-JWQQ; Press Release, U.S. Dep't of Just., *Justice Department Sues Four Additional States and One Locality for Failure to Comply with Federal Elections Laws* (Dec. 12, 2025), https://perma.cc/TQ5T-FB2A; Press Release, U.S. Dep't of Just., *Justice Department Sues Six Additional States for Failure to Provide Voter Registration Rolls* (Dec. 2, 2025), https://perma.cc/F5MD-NWHD; Press Release, U.S. Dep't of Just., *Justice Department Sues Six States for Failure to Provide Voter Registration Rolls* (Sept. 25, 2025), https://perma.cc/7J99-WGBA; Press Release, U.S. Dep't of Just., *Justice Department Sues Oregon and Maine for Failure to Provide Voter Registration Rolls* (Sept. 16, 2025), https://perma.cc/M69P-YCVC.

[3] Reid J. Epstein & Nick Corasniti, Trump, in an Escalation, Calls for Republicans to "Nationalize" Elections, N.Y. Times (Feb. 2, 2026), https://www.nytimes.com/2026/02/02/us/politics/trump-nationalize-elections.html

Times, Sept. 9, 2025, https://www.nytimes.com/2025/09/09/us/politics/trump-voter-registration-data.html. DOJ is coordinating these efforts with the federal Department of Homeland Security ("DHS"), according to reported statements from DOJ and DHS. *Id.*[4] A recent article quoted a former lawyer in DOJ's Civil Rights Division stating that leadership directed attorneys to obtain state voter rolls through litigation so the data could be cross-matched with records from the Department of Homeland Security and the Social Security Administration.[5]

Additional reporting reveals self-proclaimed "election integrity" advocates who have previously sought to disenfranchise voters and overturn elections are involved in these efforts. *See* Mot. to Intervene at 6 & nn.4-5, Dkt. 24. The Administration has also confirmed that it was sharing the requested information with DHS.[6] And DOJ's actions also indicate that it may target specific groups of voters in its use of the requested data. In its letters requesting private voter data from other states, DOJ has also requested information about how elections officials, among other things, identify and remove duplicate registrations and verify that registered

[4] *See also, e.g.*, Sarah Lynch, *US Justice Dept Considers Handing over Voter Roll Data for Criminal Probes, Documents Show*, REUTERS (Sept. 9, 2025), https://www.reuters.com/legal/government/us-justice-dept-considers-handing-over-voter-roll-data-criminal-probes-documents-2025-09-09/.

[5] Emily Bazelon & Rachel Poser, *The Unraveling of the Justice Department*, N.Y. TIMES MAG. (Nov. 16, 2025), https://www.nytimes.com/interactive/2025/11/16/magazine/trump-justice-department-staff-attorneys.html.

[6] Jonathan Shorman, *DOJ is Sharing State Voter Roll Lists with Homeland Security*, Stateline, Sept. 12, 2025, https://stateline.org/2025/09/12/doj-is-sharing-state-voter-roll-lists-with-homeland-security.

voters are not ineligible to vote, such as due to a felony conviction, citizenship status, or having moved out of state.[7]

Notably, the United States' own representations to states tend to confirm suspicions of federal overreach that could disenfranchise voters. Far from indicating a purpose of ensuring compliance with the NVRA and HAVA, the United States' proposed MOU seeks to place authority to identify supposed ineligible voters in the hands of the federal government, and requires removal of supposedly ineligible voters within 45 days—directly contrary to those statutes' text. *Compare* MOU at 2, 5, *with* 52 U.S.C. § 21085 (methods of complying with HAVA "left to the discretion of the State"), and, *e.g.*, 52 U.S.C. § 20507 (protecting voters from removal under certain circumstances).

Recent events have further highlighted the abnormal nature of the United States' request. On January 24, 2026, Attorney General Pamela Bondi wrote a letter to Minnesota Governor Tim Walz, purporting to discuss DHS's "Operation Metro Surge" activities in the Twin Cities amidst ongoing violence against the civilian population there.[8] Like Hawai'i, Minnesota has been sued by the federal government

[7] *See, e.g.*, Ltr. from M. Riordan to Sec'y of State A. Schmidt (June 23, 2025), *United States v. Pennsylvania*, No. 25-cv-01481 (W.D. Pa. Oct. 9, 2025), Dkt. No. 37-1.

[8] *Read Bondi's Letter to Minnesota's Governor*, N.Y. TIMES (Jan. 24, 2026), https://perma.cc/H5GY-ZKBS ("Bondi Letter"); *see also* Order, *Tincher v. Noem*, No. 25-cv-04669 (D. Minn. Jan. 16, 2026), Dkt. No. 85 (granting injunction against certain DHS practices in Minneapolis-St. Paul).

seeking access to its unredacted voter rolls. The letter sets out three actions the federal government wants Minnesota to take to "restore the rule of law, support ICE officers, and bring an end to the chaos in Minnesota," one of which is to "allow the Civil Rights Division of the Department of Justice to access voter rolls."[9]

ARGUMENT

I. THE UNITED STATES' DEMANDS EXCEED THE STATUTORY AUTHORITY OF THE CRA AND ARE CONTRARY TO LAW.

The United States' demand for Hawai'i's full and unredacted electronic voter file exceeds its statutory authority under the CRA. Against the backdrop of the turmoil of the Jim Crow era, Congress enacted the CRA, including the public records provisions in Title III, to facilitate investigations of civil rights violations preventing eligible citizens from voting due to discrimination. H.R. Rep. No. 86-956, at 7 (1959). But if the Attorney General makes a demand for records, she must provide "a statement of the basis and the purpose therefor." 52 U.S.C. § 20703.

The Complaint fails to adequately plead a claim for relief under the CRA for at least two distinct reasons. *First*, the United States fails to plausibly allege that it has offered a statutorily sufficient statement of "the basis and the purpose" of its sweeping demand for Hawai'i's full and unredacted state voter registration list, giving insufficient and pretextual explanations. *Second*, the United States does not

[9] Bondi Letter at 2-3.

make any showing that turning over *unredacted* records, replete with private voter information, is required under the CRA. Instead, producing this data would run directly contrary to the CRA, which exists to protect the right to vote.

A. The United States' Demand for Records Fails to Meet the Requisite Statutory Requirements of the CRA.

Title III of the CRA requires election officials to retain certain federal election records for 22 months, 52 U.S.C. § 20701, and authorizes the Attorney General, upon a written request that "contain[s] a statement of the basis *and* the purpose therefor" to inspect, reproduce, and copy those records, *id.* § 20703 (emphasis added).

The federal government's requests to Hawai'i fail to provide "a statement of the basis and the purpose" sufficient to support disclosure of the unredacted voter file. *Id*. Contemporaneous case law immediately following the enactment of Title III of the CRA shows that the "basis" and "purpose" were distinct concepts. *Kennedy v. Lynd*, 306 F.2d 222, 229 n.6 (5th Cir. 1962); *In re Coleman*, 208 F. Supp. 199, 199-200 (S.D. Miss. 1962), *aff'd sub nom*., *Coleman v. Kennedy*, 313 F.2d 867 (5th Cir. 1963). The "basis" is the statement for why the Attorney General believes there is a violation of federal civil rights law. *See Lynd*, 306 F.2d at 229 n.6; *United States v. Oregon*, No. 6:25-cv-01666, 2026 WL 318402, at *9 (D. Or. Feb. 5, 2026) (holding the basis prong requires "a factual basis for investigating a violation of a federal statute"); *United States v. Weber*, No. 2:25-cv-09149, 2026 WL 118807, at *9 (C.D. Cal. Jan. 15, 2026) ("The basis is the reasoning provided by the DOJ regarding the

evidence behind its investigation of a particular state and specific, articulable facts pointing to the violation of federal law."). The "purpose" explains how the requested records would help determine if there is a violation of the law. *See Lynd*, 306 F.2d at 229 n.6; *Oregon*, 2026 WL 318402, at *10 ("[T]he 'purpose' required in a demand for records under Title III must relate to a purpose of investigating violations of individuals' voting rights.").

The basis-and-purpose requirement under the CRA is a "critical safeguard that ensures the request is legitimately related to the purpose of the statute." *Weber*, 2026 WL 118807, at *9. It prevents the statute from being used for a "fishing expedition" to obtain records for reasons that are speculative, unrelated to the CRA's aims, or otherwise impermissible or contrary to law. *Id.* The statutory basis-and-purpose requirement therefore is not perfunctory but requires a specific statement as to the reason for requesting the information and how that information will aid in the investigatory analysis. *See Oregon*, 2026 WL 318402, at *9 ("If *any* purpose—regardless of its relationship to the purposes of the statute itself—would suffice, then the requirement of stating the demand's purpose would serve no function.").

For example, in addressing an analogous power by which the IRS obtains records for investigations via administrative subpoenas, courts have found that the test of judicial enforcement of such subpoenas includes an evaluation of whether the investigation is "conducted for a legitimate purpose," *Crystal v. United States*, 172

F.3d 1141, 1143 (9th Cir. 1999) (quoting *United States v. Powell*, 379 U.S. 48, 57-58 (1964)), and that the administrative subpoena "may not be so broad as to be in the nature of a fishing expedition." *Fed. Housing Fin. Agency v. SFR Invests. Pool 1, LLC*, No. 2:17-cv-00914, 2018 WL 1524440, at *7 (D. Nev. Mar. 27, 2018) (citation and quotation marks omitted)).

As set forth below, the United States failed to articulate in its demand and in the Complaint "the basis and purpose" for its request for Hawai'i voters' sensitive personal information. The DOJ Letter states that the "purpose" of its request for Hawai'i's complete and current voter registration list was to "ascertain Hawaii's compliance with the list maintenance requirements of the NVRA and HAVA." DOJ Ltr. 3. But neither the United States' Complaint nor its letter invoking the CRA supplies a "basis" for why the United States believes Hawai'i's list maintenance procedures might violate the NVRA, HAVA, or the CRA. Nor does the Complaint (or the DOJ Letter or emails) allege anomalies or anything inconsistent with reasonable list maintenance efforts in the data Hawai'i has reported to the U.S. Election Assistance Commission. *See* Compl. ¶¶ 9-26; DOJ Ltr.; DOJ Email.

Even if the United States had provided a proper "basis" for its demand—and it did not—it fails to explain any connection between its purported "purpose" and the vast scope of its records request here. The Complaint does not attempt to explain why the full and unredacted Hawai'i statewide voter file is necessary to determine

whether Hawai‘i has "conduct[ed] a general program that makes a reasonable effort to remove the names of ineligible voters" by virtue of "death" or "a change in the residence of the registrant," 52 U.S.C. § 20507(a)(4); *see* Compl. ¶ 12. And in fact, such records are not necessary: A single snapshot of a state's voter list does not and could not provide the information needed to determine if the state has made a "reasonable effort" to remove ineligible voters under Section 8 of the NVRA. Compl. ¶ 12; 52 U.S.C. § 20507(a)(4)(A)-(B). The NVRA and HAVA both leave the mechanisms for conducting list maintenance within the discretion of the State. *See* 52 U.S.C. §§ 20507(a)(4) & (c)(1), 21083(a)(2)(A), 21085. The *procedures* carried out by a state or locality establish its compliance; the unredacted voter file does not. Even were the United States to use voter file data to identify voters who had moved or died on Hawai‘i's voter list at a single point in time, that would not amount to Hawai‘i failing to comply with the "reasonable effort" required by the NVRA or HAVA. *See, e.g.*, *Pub. Int. Legal Found. v. Benson*, 136 F.4th 613, 624-27 (6th Cir. 2025) (describing a "reasonable effort" as "a serious attempt that is rational and sensible" and rejecting any "quantifiable, objective standard" in this context), *petition for cert. filed* (U.S. Oct. 7, 2025) (No. 25-437). Accordingly, the United States' demand failed on its face to meet the CRA's basis and purpose requirements.

Moreover, even if some portion of the voter file were necessary to investigate "Hawaii's compliance with federal election law," Compl. ¶ 19, the United States has

not provided any justification for why the full unredacted voter file is necessary to carry out this purported purpose. For decades, DOJ has neither sought nor required a full and unredacted voter file in its investigations regarding NVRA compliance. *See, e.g.*, Press Release, U.S. Dep't of Just., *United States Announces Settlement with Kentucky Ensuring Compliance with Voter Registration List Maintenance Requirements* (July 5, 2018), https://perma.cc/G2EZUUA5 (describing letters to all 44 states covered by the NVRA with requests for list maintenance information, but without demanding voter files). The United States' failure to articulate the basis and the purpose for demanding the full and unredacted voter file is ground to hold its demand insufficient as a matter of law.

The government's statement is not just insufficient as a matter of law; it is also pretextual. Section 303 of the CRA requires a statement of "*the* basis and *the* purpose" of a records request, and by twice using the definite article, the statute requires not just *a* basis or purpose among many, but *the* complete basis and purpose underlying the request. *See Niz-Chavez v. Garland*, 593 U.S. 155, 165-66 (2021); *see also, e.g.*, *Corner Post, Inc. v. Bd. of Governors of the Fed. Rsrv. Sys.*, 603 U.S. 799, 817 (2024) (emphasizing distinction between the definite and the indefinite article). But the United States has not disclosed the actual purpose for its requests, and this Court "is not obliged to accept a contrived statement and purpose" in place of an accurate one. *Weber*, 2026 WL 118807, at *10.

Public reporting and public, judicially-noticeable documents confirm that the United States' *actual* purpose is not to ensure compliance with the NVRA and HAVA, but to build an unprecedented national voter file through novel, error-prone, forms of data-matching, and then to use this tool to identify ostensibly ineligible voters and challenge their right to vote. *See supra* 6-8 & nn.3-7. As *Weber* characterized it, considering the same robust set of public reporting and documents, "[i]t appears that the DOJ is on a nationwide quest to gather the sensitive, private information of millions of Americans for use in a centralized federal database." 2026 WL 118807, at *10; *accord Oregon*, 2026 WL 318402, at *11, *13.

Such a database would be unlawful in multiple ways. The creation of any national voter database—much less one designed for targeting and mass-challenging voters—has never been authorized by Congress, and would violate (among other provisions of federal law) the federal Privacy Act's prohibition on the creation or maintenance of any database "describing how any individual exercises rights guaranteed by the First Amendment," which necessarily includes exercising the right to vote. *See* 5 U.S.C. § 552a(e)(7).

Consider also the MOU that the United States has recently pushed a number of states to sign in connection with its requests for statewide voter files. *See supra* 5 & n.1. The NVRA and HAVA require a state to conduct a "reasonable effort" to remove ineligible voters from the rolls, 52 U.S.C. §§ 20507(a)(4), 21083(a)(4)(A),

and the NVRA includes safeguards to protect voters from erroneous removal. The government's proposed MOU indicates multiple contemplated violations of those statutory requirements. First, it seeks to place authority to identify supposed ineligible voters in the hands of the federal government, contrary to statutory text, 52 U.S.C. § 21085 (leaving methods of complying with HAVA "to the discretion of the State"). MOU at 2, 5. Second, the MOU's substantive terms seek to compel states to remove supposedly ineligible voters "within forty-five (45) days," *id.* at 5, in a way that would violate multiple protections of the NVRA, 52 U.S.C. § 20507.

Finally, there is the Attorney General's recent letter to Minnesota Governor Tim Walz, demanding that Minnesota turn over voters' private data in order to help "support ICE officers" and "bring an end to the chaos" being inflicted by DHS agents ostensibly enforcing the immigration laws. *See* Bondi Letter at 2-3. Attorney General Bondi's letter, which by its terms connects DOJ's request for state voter data with the Administration's draconian immigration-enforcement efforts, highlights DOJ's failure to disclose the true purpose of its request. *See Oregon*, 2026 WL 318402, at *11 ("The context of this demand within a letter about immigration enforcement casts serious doubt as to the true purposes for which Plaintiff is seeking voter registration lists in this and other cases, and what it intends to do with that data.").

The United States' failure to honestly disclose what it is doing and will do with voters' sensitive personal information—to state *the* true purpose for the demand

for Hawai‘i residents’ protected personal data—is independently fatal to the CRA claim. “Congress passed the NVRA, Civil Rights Act, and HAVA to protect voting rights. If the DOJ wants to instead use these statutes for more than their stated purpose, circumventing the authority granted to them by Congress, it cannot do so under the guise of a pretextual investigative purpose.” *Weber*, 2026 WL 118807, at *12; *accord Oregon*, 2026 WL 318402, at *11 (“The presumption of regularity that has been previously extended to [the United States] that it could be taken at its word—with little doubt about its intentions and stated purposes—no longer holds.”).

B. Any Records Disclosed Under the CRA Should Be Redacted to Protect the Constitutional Rights of the Voter, so the Court must Deny the United States’ Request.

Even if disclosure were appropriate, sensitive personal voter information—in this case, partial Social Security and full driver’s license numbers—would still be subject to redaction, which is not barred under Title III. Indeed, courts have found that redaction may be required to prevent the disclosure of sensitive personal information that would create an intolerable burden on the constitutional right to vote. The cases interpreting Section 8(i) of the NVRA are instructive, as courts have consistently permitted—and sometimes required—redaction of voters’ sensitive personal data before disclosure to protect voter privacy and ensure compliance with federal and state law and the Constitution.

Like the CRA, the NVRA is silent as to how sensitive personal information should be treated during disclosure. *See* 52 U.S.C. §§ 20703, 20507(i)(1). Courts must interpret the disclosure provisions in a manner that does not unconstitutionally burden the right to vote. *See United States v. Hernandez*, 322 F.3d 592, 594-95 (9th Cir. 2003) (noting "the fundamental principle of judicial restraint that ordinarily requires courts to construe statutes, if it is fairly possible to do so, in a way that avoids unnecessarily addressing constitutional questions").

Federal courts throughout the country have consistently struck this balance, interpreting the "all records concerning" language in Section 8(i) to permit—and sometimes require—redaction and the protection of confidential materials. As the First Circuit has noted, "nothing in the text of the NVRA prohibits the appropriate redaction of uniquely or highly sensitive personal information in the Voter File," and such redaction "can further assuage the potential privacy risks implicated by the public release of the Voter File." *Pub. Int. Legal Found., Inc. v. Bellows*, 92 F.4th 36, 56 (1st Cir. 2024); *see also Pub. Int. Legal Found., Inc. v. N.C. State Bd. of Elections*, 996 F.3d 257, 264 (4th Cir. 2021) (NVRA disclosure provisions "must be read in conjunction with the various statutes enacted by Congress to protect the privacy of individuals and confidential information held by certain governmental agencies" and protecting sensitive information from disclosure); *Pub. Int. Legal Found., Inc. v. Dahlstrom*, 673 F. Supp. 3d 1004, 1015-16 (D. Alaska 2023) (similar). And in

Hawai‘i, the state constitution likewise provides Hawai‘i residents with an informational right to privacy that protects against disclosure of their sensitive personal information. *See Civ. Beat L. Ctr. for the Pub. Int., Inc. v. City & Cnty. of Honolulu*, 445 P.3d 47, 61 (Haw. 2019).

Redaction may also be affirmatively required if the disclosure would "create[] an intolerable burden on [the constitutional right to vote] as protected by the First and Fourteenth Amendments." *Project Vote/Voting for America, Inc. v. Long*, 682 F.3d 331, 339 (4th Cir. 2012) (quotation marks and citation omitted). The Fourth Circuit, even while granting access to voter registration applications, affirmed the importance of redacting Social Security numbers, which are "uniquely sensitive and vulnerable to abuse."[10] *Id.* The court emphasized that the NVRA reflected Congress's view that the right to vote was "fundamental," and that the unredacted release of records risked deterring citizens from registering to vote and thus created an "intolerable burden" on this fundamental right. *Id.* at 334, 339; *cf. In re Coleman*, 208 F. Supp. 199, 200 (S.D. Miss. 1962) (noting, in the context of a Title III records

[10] The United States itself has explained—on multiple occasions—that the NVRA does not prohibit the States from redacting "uniquely sensitive information" when disclosing voting records. *See, e.g.*, Br. for the United States as Amicus Curiae, *Pub. Int. Legal Found., Inc. v. Bellows*, No. 23-1361 (1st Cir. July 25, 2024), 2023 WL 4882397 at *27-28; Br. for the United States as Amicus Curiae, *Pub. Int. Legal Found. v. Schmidt*, No. 23-1590 (3d Cir. Nov. 6, 2023), https://perma.cc/3BQ9-36UJ ("States may redact certain information before disclosing Section 8(i) records."); Br. for the United States as Amicus Curiae, *Project Vote/Voting for Am., Inc. v. Long*, No. 11-1809 (4th Cir. Oct. 18, 2011), 2011 WL 4947283, at *11, 25-26.

request, multiple considerations which could be "[s]ignificant," including that "[i]t is not claimed that these official records are privileged, or exempt from discovery for any sound reason of public policy," or "that an inspection of these records would be oppressive, or any unlawful invasion of any personal constitutional right"). As such, public disclosure provisions such as those in the NVRA and Title III of the CRA must be interpreted to avoid this unconstitutional burden. *See Long*, 682 F.3d at 339; *Bellows*, 92 F.4th at 56. The danger of imposing those burdens on Hawai'i voters and civic organizations is present here. *See* Ex. 2 to Mot. to Intervene, Decl. of Camron Hurt ¶¶ 6, 10-13, Dkt. 24-2; Ex. 3 to Mot. to Intervene, Decl. of Neil Abercrombie ¶¶ 5-10, Dkt. 24-3; Ex. 4 to Mot. to Intervene, Decl. of Katherine Hammes ¶¶ 3-10, Dkt. 24-4.

The same privacy and constitutional concerns warranting redactions under the NVRA apply equally to requests under the CRA. No matter the statutory mechanism, conditioning the right to vote on the release of voters' sensitive private information "creates an intolerable burden on that right." *Long*, 682 F.3d at 339 (citation omitted); *cf. Sheetz v. Cnty. of El Dorado*, 601 U.S. 267, 281-82 (2024) (Gorsuch, J., concurring) ("[O]ur Constitution deals in substance, not form. However the government chooses to act, . . . it must follow the same constitutional rules."). And the limited case law considering CRA records requests acknowledge that courts retain the "power and duty to issue protective orders," *Lynd*, 306 F.2d at 230, such

as the redaction of sensitive fields that courts have consistently determined are entitled to protection from disclosure. *Accord Oregon*, 2026 WL 318402, at *12 ("[T]he vast array of cases cited above addressing the propriety of redaction in the context of the NVRA confirm that such redaction is appropriate and permissible.").

Thus, even had the United States provided a valid statement of the basis and the purpose for its records demand (which it failed to do here), sensitive personal identifying information should similarly be redacted.

II. THE UNITED STATES DEMAND WOULD IMPERIL THE PRIVACY INTERESTS OF AND CHILL DEMOCRATIC PARTICIPATION BY HAWAIʻI VOTERS

Even if the DOJ satisfied statutory requirements—which it does not—granting its request would still thwart the purposes of the CRA by chilling the voting rights of Hawaiʻi residents. Here, the United States seeks highly sensitive personal information, including full birth dates and driver's license numbers or partial Social Security numbers for every registered voter in the state. Disclosing this type of personal information to the federal government would sow seeds of doubt into the minds of voters and discourage democratic participation.

Allowing the DOJ access to voter information under the guise of election-fraud prevention would harm voters' interests and erode democracy. The federal government would be emboldened to endlessly challenge and undermine elections, leading voters to become disillusioned with the electoral process. *See Crawford v.*

Marion Cnty. Election Bd., 553 U.S. 181, 197 (2008) (plurality op.) (recognizing that "public confidence in the integrity of the electoral process . . . encourages citizen participation in the democratic process"). Some voters could be discouraged from registering to vote and voting out of fear that they will be subjected to baseless voter challenges or even improper prosecution. *See Weber*, 2026 WL 118807, at *20 ("The centralization of [confidential voter] information by the federal government would have a chilling effect on voter registration . . . lead[ing] to decreasing voter turnout as voters fear that their information is being used for some inappropriate or unlawful purpose."). Others could fear being subjected to public harassment by elected officials and the media making baseless claims of fraud. *See, e.g.*, *Andrews v. D'Souza*, 696 F. Supp. 3d 1332, 1348-49 (N.D. Ga. 2023) (holding that publication of a citizen's face and license plate in video falsely alleging he was engaged in election fraud constituted voter intimidation under the CRA); *League of United Latin Am. Citizens – Richmond Region Council 4614 v. Pub. Int. Legal Found.*, No. 1:18-cv-00423, 2018 WL 3848404, at *4 (E.D. Va. Aug. 13, 2018) (similar, for allegations of voter fraud accompanied by individual voters' personal information obtained from county registrars).

Certain voters—especially those from historically marginalized communities—may fear that disclosure of their personal information could lead to them being swept up in fishing expeditions unrelated to voting. For example,

naturalized citizens or individuals who had their rights restored after a conviction may fear being subjected to challenges based on erroneous and outdated data. *See Weber*, 2026 WL 118807, at *2 ("The DOJ's request . . . stands to have a chilling effect on . . . political minority groups and working-class immigrants who may consider not registering to vote or skip casting a ballot because they are worried about how their information will be used.").

Voters must be assured that they will not be penalized for exercising their right to vote and that when they cast a ballot, their most sensitive information is protected from disclosure. Federal laws like the Privacy Act restrict access to any record that "contains [one's] name, or the identifying number, symbol, or other identifying particular assigned to [an] individual." *See* 5 U.S.C. § 552a(a)(4). Yet the federal government threatens voter privacy and trust by bypassing the appropriate procedures to pursue the State's unredacted voter registration list, which contains protected identifying information under the law. *See Carlborg v. Dep't of the Navy*, No. 18-cv-1881, 2020 WL 4583270, at *7 (D.D.C. Aug. 10, 2020) (concluding that the Navy "properly withheld personal identifying information [including names, *signatures*, and social security numbers] pertaining to third parties who had not provided their consent to disclose that information" to the requester). Furthermore, the federal government seemingly seeks this protected information to create a "centralized federal database" comprised of the "sensitive [and] private information

of millions of Americans," *Weber*, 2026 WL 118807, at *10, which is also unlawful under the Privacy Act. *See* 5 U.S.C. § 552a(e)(7) (prohibiting the creation or maintenance of any database "describing how any individual exercises rights guaranteed by the First Amendment," which necessarily includes exercising the right to vote). Altogether, the federal government's quest threatens voters' bedrock understanding of the privacy protections they rely on. *Weber*, 2026 WL 118807, at *18.

These fishing expeditions would likely lead to the wrongful purging of eligible voters across Hawai'i. As explained above, the United States' proposed MOU seeks to place authority to identify supposed ineligible voters in the hands of the federal government, and requires removal of supposedly ineligible voters within 45 days—directly contrary to federal law.

This has significant implications for the rights of Hawai'i voters. As of 2023, 13.8% of adult Hawai'i residents were naturalized U.S. citizens (157,492 people).[11] And in 2023, an estimated 58,539 people moved to Hawai'i and at least 47,473 people intended to establish residency.[12] These groups are at higher risk of being erroneously purged from the voter rolls due to faulty data matching, as voters likely

[11] *The State of Hawaii Data Book 2024* 67, § 1.39, https://files.hawaii.gov/dbedt/economic/databook/db2024/section01.pdf.
[12] *The State of Hawaii Data Book 2024* 89-92, §§ 1.56, 1.59, https://files.hawaii.gov/dbedt/economic/databook/db2024/section01.pdf.

appear in databases of people who are ineligible to vote or are registered elsewhere, even if that data is outdated.

Once removed, affected voters could face significant barriers to re-registering, particularly in Hawai‘i, where geographic separation between islands can make in-person access to election offices overly burdensome. Indeed, some voters in Hawai‘i could even be forced to take plane rides in order to re-register if they miss the limited window of pop-up registration centers on their own islands.[13]

Exposing sensitive voter information opens the door to voter intimidation and fear, "threaten[ing] the right to vote which is the cornerstone of American democracy." *Weber*, 2026 WL 118807, at *20. To protect this fundamental right, the federal government must not be granted unlawful access to Hawai‘i voters' sensitive and personal information.

CONCLUSION

The United States' request for Hawai‘i's full and unredacted electronic voter file should be denied and the complaint dismissed.

---

[13] Gréta Bedekovics & Sydney Bryant, *The SAVE Act Would Force Many Rural Americans To Drive Hours To Register To Vote*, CENTER FOR AMERICAN PROGRESS, Feb. 28, 2025, https://www.americanprogress.org/article/the-save-act-would-force-many-rural-americans-to-drive-hours-to-register-to-vote/; State of Hawai‘i Office of Elections, *Voter Service Centers and Ballot Drop Boxes,* https://elections.hawaii.gov/voter-service-centers-and-places-of-deposit/ (last visited Feb. 27, 2026).

Dated: March 5, 2026

Respectfully submitted,

/s/ Emily M. Hills

THERESA J. LEE*
ETHAN HERENSTEIN*
WILLIAM HUGHES*
SOPHIA LIN LAKIN*
American Civil Liberties Union Foundation
125 Broad St., 18th Floor
New York, NY 10004
(212) 549-2500
tlee@aclu.org
eherenstein@aclu.org
whughes@aclu.org
slakin@aclu.org

**admitted pro hac vice*

EMILY M. HILLS 11208
JONGWOOK "WOOKIE" KIM 11020
ACLU of Hawaii Foundation
P.O. Box 3410
Honolulu, HI 96801
T: (808) 522-5905
F: (808) 522-5909
ehills@acluhawaii.org
wkim@acluhawaii.org

Attorneys for Amici Curiae Common Cause, Neil Abercrombie, and Katherine Hammes

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

EXHIBIT 1

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