

# The Justice Department's Security Measures for Collecting Voter Rolls Are Inadequate

Federal and state law requires that sensitive voter registration information be kept secure.



Lisa J. Danetz

February 25, 2026

Voting & Elections

Since spring of 2025, the Department of Justice has been attempting to [sweep up voter rolls](#) [\[link-1\]](#) across the nation. That fight has extended to the courts, where the DOJ has filed [lawsuits](#) [\[link-2\]](#) against 24 states since September. Notably, most of those states have already provided publicly available voter registration information, but the DOJ has demanded full, unredacted rolls, which include sensitive, personally identifiable information like driver's licenses and Social Security numbers.

Much of the discussion of this issue has [focused](#) [\[link-3\]](#) on various legal arguments — including the basis and purpose requirement under the Civil Rights Act, the Privacy Act, and violations of state law —

for why the DOJ is not entitled to such information. There is another, lesser-known reason: The DOJ has provided no detailed assurances about how it will protect U.S. citizens' sensitive private information and seems to be ignoring federal law that requires it to do so.

Under federal law and many state laws, state officials must protect the security of their citizens' voter registration information. At the federal level, the [Help America Vote Act](#) [\[link-4\]](#) (HAVA) requires state and local election officials to ensure “[adequate technological security measures](#) [\[link-5\]](#)” to protect statewide voter registration databases. States [determine](#) [\[link-6\]](#) how to do so and can

also require [stricter protection](#) [\[link-7\]](#) than that specified by HAVA's minimum standards.

Federal law also requires the federal government to take certain steps to secure any sensitive information it collects and holds. The [Federal Information Security Modernization Act](#) [\[link-8\]](#) (FISMA) stipulates that [U.S. government agencies and their contractors](#) [\[link-9\]](#) develop and implement information security programs to protect their computer systems and the information stored in them. The level of protection the law requires varies based on the level of risk posed by the information at issue and must be based on [mandatory](#) [\[link-10\]](#) federal standards. FISMA also requires that federal agencies regularly monitor their and their contractors' information security programs.

In theory, HAVA, FISMA, and state law should make sure any sensitive voter registration information remains secure. Unfortunately, the reality appears different. The DOJ's proposed [agreement](#) [\[link-11\]](#) governing the transfer of voter registration data with sensitive information from the states is simultaneously vague as to its security plans and, to the extent it lists them, woefully deficient. A recent

[analysis](#) [\[link-12\]](#) details the information-security shortcomings. The lack of protection is scary.

The security shortfalls include the following:

- There is inadequate data encryption, or the converting of voter registration information into unreadable code. Inadequate encryption means hackers can easily access voters' personal data.
- There are insufficient access and data minimization controls. The agreement permits password-only access to the data, rather than requiring multifactor authentication. It also fails to limit any sharing of the data beyond the stated purpose of the collection.
- The DOJ has not explained how it will ensure that contractors, with whom it explicitly plans to share the data, are vetted and that they safeguard voters' private information, as required by federal law.
- There is no audit log analysis or defined reporting process. No one will review or analyze who accesses the data, so no one will detect any problems that occur. In the event the DOJ does detect any problems, such as unauthorized access to information or other data breaches, there

is no required timeframe to report problems back to the states.

- The DOJ plans to “archive” and store data after its analysis rather than destroy it. Archiving data will create a permanent federal registry of voters’ sensitive information that will always be available.

These cybersecurity failures exacerbate what is known as the [mosaic effect](#) [\[link-13\]](#). Voter registration lists include significant amounts of information about each voter — some combination of name, residential address, date of birth, driver’s license number, full or partial Social Security number, email address, telephone number, registration date, registration status, voting history, and political party. Aggregation of so much voter registration data, combined with other available information from commercial data brokers, financial leaks, and federal databases, offers an easy centralized target for bad actors.

Potential breaches of this data raise at least three concerns. First, the mosaic effect would allow a bad actor to use a voter’s information for identity theft. Second, by leaking information about a successful security breach, an adverse nation state could exploit the accumulated data to create fear, assert power, and

undermine confidence in our government. Third, a bad actor could use this information to remove targeted names from voter registration lists without quick or easy detection.

Given recent examples of poor information security and data handling by federal agencies, it is not safe to blindly trust the DOJ’s processes. In 2025, federal employees inappropriately [uploaded](#) [\[link-14\]](#) confidential Social Security Administration data to an unapproved private server and entered into a “voter data agreement” to transfer that information to a political advocacy group aimed at finding evidence of alleged voter fraud and overturning election results. The interim director of the Cybersecurity and Infrastructure Security Agency, an agency created to “defend and secure cyberspace,” [uploaded](#) [\[link-15\]](#) sensitive agency files into the public version of ChatGPT, thereby allowing OpenAI to use that information to answer questions from any of more than 700 million active users. And the head of the DOJ’s own Weaponization Working Group, [established](#) [\[link-16\]](#) under the current attorney general to [review](#) [\[link-17\]](#) the activities of people who previously investigated or prosecuted the president

and his businesses, [leaked](#) [\[link-18\]](#) grand jury materials.

Protecting citizens should be the hallmark of any government. Given state officials' obligation to protect their voters' sensitive

information, the DOJ's apparent lack of adequate security measures under federal law is yet one more reason for states to resist the attempt to amass nationwide voter registration data.

---

## MORE ON

[Election Integrity](#) [\[link-19\]](#)

---

## Links

**link-1:** sweep up voter rolls <https://www.brennancenter.org/our-work/research-reports/tracker-justice-department-requests-voter-information>

**link-2:** lawsuits <https://www.brennancenter.org/our-work/analysis-opinion/trump-administration-has-sued-more-20-states-refusing-turn-over-voter>

**link-3:** focused <https://www.brennancenter.org/our-work/analysis-opinion/justice-department-has-demanded-voter-files-least-21-states>

**link-4:** Help America Vote Act [https://www.eac.gov/sites/default/files/eac\\_assets/1/6/HAVA41.PDF](https://www.eac.gov/sites/default/files/eac_assets/1/6/HAVA41.PDF)

**link-5:** adequate technological security measures [https://uscode.house.gov/view.xhtml?req=\(title:52%20section:21083%20edition:prelim\)](https://uscode.house.gov/view.xhtml?req=(title:52%20section:21083%20edition:prelim))

**link-6:** determine <https://uscode.house.gov/view.xhtml?hl=false&edition=prelim&req=granuleid%3AUSC-prelim-title52-section21085&num=0&saved=%7CKHRpdGxIOjUyIHNIY3Rpb246MjEwODMgZWVpdGlvbWpwcmlVsaW0p%7C%7C0%7Cfalse%7Cprelim>

- link-7:** stricter protection <https://uscode.house.gov/view.xhtml?hl=false&edition=prelim&req=granuleid%3AUSC-prelim-title52-section21084&num=0&saved=%7CKHRpdGxIOjUyIHNIY3Rpb246MjEwODMgZWRpdGljbjpwcmVsaWOp%7C%7C%7C0%7Cfalse%7Cprelim>
- link-8:** Federal Information Security Modernization Act <https://uscode.house.gov/view.xhtml?req=granuleid%3AUSC-prelim-title44-chapter35-subchapter2&saved=%7CZ3JhbnVsZWlkOIVTQy1wcmVsaW0tdGI0bGU0NC1zZWNOaW9uMzU1MQ%3D%3D%7C%7C%7C0%7Cfalse%7Cprelim&edition=prelim>
- link-9:** U.S. government agencies and their contractors <https://uscode.house.gov/view.xhtml?hl=false&edition=prelim&req=granuleid%3AUSC-prelim-title44-section3554&num=0&saved=%7CZ3JhbnVsZWlkOIVTQy1wcmVsaW0tdGI0bGU0NC1zZWNOaW9uMzU1MQ%3D%3D%7C%7C%7C0%7Cfalse%7Cprelim>
- link-10:** mandatory [https://uscode.house.gov/view.xhtml?req=\(title:40%20section:11331%20edition:prelim\)](https://uscode.house.gov/view.xhtml?req=(title:40%20section:11331%20edition:prelim))
- link-11:** agreement <https://www.brennancenter.org/our-work/analysis-opinion/confidential-agreements-show-trump-administrations-plans-states-voter>
- link-12:** analysis <https://epic.org/documents/analyzing-doj-mou-for-voter-registration-list-data-for-fisma-compliance/>
- link-13:** mosaic effect <https://ostradecraft.medium.com/the-mosaic-effect-why-harmless-data-isnt-harmless-bc63bbd3d072>
- link-14:** uploaded <https://www.npr.org/2026/01/23/nx-s1-5684185/doge-data-social-security-privacy>
- link-15:** uploaded [https://www.politico.com/news/2026/01/27/cisa-madhu-gottumukkala-chatgpt-00749361?mc\\_cid=6f311a1887&mc\\_eid=2927a70260](https://www.politico.com/news/2026/01/27/cisa-madhu-gottumukkala-chatgpt-00749361?mc_cid=6f311a1887&mc_eid=2927a70260)
- link-16:** established <https://www.justice.gov/ag/media/1388506/dl?inline>
- link-17:** review <https://abcnews.com/US/bondi-new-ag-launches-weaponization-working-group-review/story?id=118501463>
- link-18:** leaked <https://www.cnn.com/2026/02/04/politics/ed-martin-review-improperly-handled-grand-jury>
- link-19:** Election Integrity <https://www.brennancenter.org/topics/voting-elections/election-integrity>