

How Election Officials Respond to Law Enforcement Requests for Access to Election Equipment and Materials

Numerous laws and rules govern access to ballots, machines, and other sensitive election records.



Gowri Ramachandran



Marina Pino

Published **February 10, 2026**

Voting & Elections

In the past month, President Trump has [said](#) [\[link-1\]](#) that he regrets not ordering the National Guard to seize voting machines in certain states following the 2020 election and that he wants the Republican Party to “[nationalize](#) [\[link-2\]](#)” elections. A few days after the FBI seized 2020 election records in Georgia in late

January, the Office of the Director of National Intelligence [confirmed](#) [\[link-3\]](#) that election officials in Puerto Rico had voluntarily turned over voting systems for review.

The Trump administration is not the only entity that has sought to access sensitive voting equipment and ballots. In recent years, there

has been a deluge of requests from a variety of sources, including private actors, legislative committees, and law enforcement agents. While some are legitimate and important for transparency, other demands go far beyond what is legally authorized and what election officials are permitted to turn over. Beyond risks of violating state and federal laws, improper disclosure may pose security risks and undermine public trust in election processes.

This article outlines what legal procedures govern the authority of law enforcement and other parties to access election equipment, ballots, and other sensitive data in the custody of election officials.

Who is responsible for maintaining and securing voting machines and ballots?

Under the Constitution's [Elections Clause](#) ^[link-4], elections are

administered by state and local authorities in accordance with laws passed by the states and Congress. Those laws assign the duty of acquiring, maintaining, and securing voting machines and ballots to state and local election officials. While those officials are subject to law and oversight, no individual or entity is authorized to take over their duties, including by taking possession of their equipment and data, unless specifically authorized by statute. No statute provides such broad authority to the federal government.

Does the president have constitutional or statutory authority over elections that would allow him to seize or access voting machines or ballots?

The president has no constitutional authority over federal election administration. Instead, the [Constitution charges states and](#)

[Congress](#) [\[link-5\]](#) with setting the rules that govern elections, and all elections — including federal elections — are administered by state and local authorities. While the president has narrow power to shape the level of support and resources that the federal government provides to those officials who request support, such as threat intelligence briefings and cyber and physical [assessments](#) [\[link-6\]](#), for the states that choose to use them, this power does not permit the president to take over election administration and access voting equipment or records.

While the president has the authority to enforce election laws passed by Congress, those laws generally do not authorize the seizure of election infrastructure.

For example, the prohibition of noncitizen voting does not justify voting system or ballot seizures.

Under [federal law](#) [\[link-7\]](#), only U.S. citizens can vote in federal elections. Anyone who violates this law could face criminal prosecution and deportation. If an instance of noncitizen voting does occur, voting machines and marked ballots would not offer any evidence that would be necessary for an investigation because voting machines do not record or store any information about a voter's eligibility or citizenship status.

Likewise, the record retention and inspection requirements in the Civil Rights Act do not authorize records seizures. That law provides only limited, non-exclusive access for the attorney general to “inspect” or “copy” certain records, after providing a written “basis” and “purpose.” Under [52 U.S.C. Section 20701](#) [\[link-8\]](#), election officials must preserve records related to registration and other acts requisite to voting for at least 22 months

following a federal election. Crucially, election officials or other designees under state law must supervise custody of these materials. In recent months, courts have [rejected](#) [\[link-9\]](#) the use of these Civil Rights Act provisions to conduct fishing expeditions into voter rolls. What is more, it is unlikely that the retention requirement covers voting system hardware, which officials must reuse for elections that occur more frequently than every 22 months.

There are a range of other limits on what information the federal government may request or do within the narrow scope of its law enforcement authority. For instance, a request that would compromise the integrity or custody of election materials or interfere with the ability to meet state certification deadlines may be prohibited under state or federal law. And any deployment of federal law enforcement to interfere with

elections is [plainly illegal](#) [\[link-10\]](#) and in many cases a federal crime. For instance, federal [law](#) [\[link-11\]](#) bars ordering “armed men at any place where a general or special election is held,” with a sentence of up to five years in prison for violators. Crucially, [no emergency powers](#) [\[link-12\]](#) allow the president to override these laws.

What operational tools are available for election officials to prepare for requests to access election records and equipment?

Preparation remains one of the most valuable tools available to election officials.

Election officials should review internal policies and protocols on physical building security, as well as public access to voter data or other election materials, to mitigate any unauthorized access or breach.

- All voting system components and ballots should be kept in a secure

location with access controls, alarm systems, and procedures to log every entry. Measures such as appointment policies and signage in public areas to indicate employee-only spaces can help maintain order and protect secure environments. Some states [forbid](#) [\[link-13\]](#) election officials from turning over sensitive information absent a court order.

Some [require](#) [\[link-14\]](#) requesters to certify that data will be stored securely, not shared with unauthorized individuals and parties, and used only for expressly permitted purposes.

- Voting equipment and election material storage areas should be monitored with video surveillance. If permissible, election workers and voting system vendors should require background checks of those with access to voting systems.
- Election offices should review training materials for staff to

ensure protocols cover requests for access scenarios, including contact information for retained counsel.

- Officials should use resiliency measures so that no request or encounter will prevent a voter from casting their ballot or having their vote counted. Offices should, as always, have [enough backup materials](#) [\[link-15\]](#) in place to keep polling places operational in the event of an equipment breach, including backup paper ballots in case touchscreen voting machines are not available, paper backup copies of digital records such as check-in lists of voters, voter registration files, and precinct and district maps. If permitted by state law, contingency plans for tabulation may include arrangements with neighboring jurisdictions or the state's chief election official.

Election officials should consult counsel and, when appropriate,

other trusted election officials, including a state's election official association if available.

- As explained below, attorneys can help assess the legal authority behind a request, advise on any limits in state or federal law, and move for court intervention and oversight.
- Officials should also share information and any interactions with law enforcement with other officials, as appropriate. This communication can help other jurisdictions prepare for similar situations.

Election officials should plan a public communications strategy in the event of requests for access to election equipment or sensitive data.

- Officials should include their retained counsel in their planning to provide clear, timely explanations about legal obligations, procedures, and how

election materials are being secured, via both traditional and social media.

- A comprehensive plan may include options to respond to emergent developments, such as notifications to all voters of any remedial action taken and the remaining opportunities to securely cast their ballot.

What rules and restrictions govern law enforcement officials who are requesting access to sensitive materials?

All requests — from any requester at all levels of government and private actors — must respect the constitutional and statutory framework that preserves state and local control. No federal agency or official has blanket authority to intervene in or access election systems without legal process or specific statutory authorization. Notably, the Department of Justice has

longstanding [policies](#) [\[link-16\]](#) restricting enforcement activity that could be perceived as interfering with elections, particularly [close](#) [\[link-17\]](#) to voting periods.

What legal responses are available if election officials are faced with requests or demands for access by law enforcement or other governmental authorities?

Election officials can take both preparatory and, with advice of counsel, legal steps to preserve to the best of their ability the security of sensitive materials and equipment, as well as the public's interest in timely certification of elections.

The election official can ask to see a badge or other identification and ask what office the individual represents to ensure they are a law enforcement officer.

- Private parties have [impersonated](#) [\[link-18\]](#) law enforcement or claimed government affiliation without authorization. Legitimate law enforcement will be willing to make formal requests (e.g., presenting a search warrant signed by a judge).
- Federal law does not require an election official to immediately provide any information based on an informal request, such as an oral request or letter, by a law enforcement official to obtain election information. Such requests can be reviewed by counsel to determine the appropriate and lawful response.

The election official can ask if the officer has a warrant signed by a federal or state judge as opposed to an administrative warrant, which is issued by a federal agency. If the officer has a warrant signed by a judge, the official can ask to see it

but must provide access to the items in the warrant.

- A warrant signed by a judge must be honored without delay. A judicial warrant may authorize search or seizure and is based on allegations that, if true, constitute probable cause that a crime has been committed.
- Like any other individual, an election official should never obstruct the execution of a judicial warrant. The official can let the officer know that they would like to consult their attorney or ask the law enforcement officer to speak with their attorney to make sure they are properly complying with the warrant and that the warrant is executed as quickly and with the least disruption possible. Note, however, that agents are not required to wait for an election official to reach their attorney before accessing the materials listed in the warrant.
- Election officials may be subject to state privacy and other laws that require they *only* provide access to what is listed in the warrant. They can consult counsel to ensure they comply with these laws while also complying with the warrant. Unless there is a separate court order prohibiting it, taking photographs or video of the activity to serve or execute a search warrant is permitted in the federal and most state systems. If a law enforcement official objects to such recording, the election official may ask if there is any judicial order prohibiting it.
- Law enforcement officials executing a proper warrant should make an inventory of what was seized, and a copy of that inventory should be left or provided at the end of the search. There is no prohibition on election officials making their own inventory of what was taken (e.g., a description of the material,

room or place taken from, file names or document titles).

- Notably, whether an officer has a warrant or not, nothing in [federal law](#) [\[link-19\]](#) or in typical state election laws would require an election official to answer any questions on the spot, such as questions about a memorized password or other sensitive information. Like any person presented with a search warrant, an election official can seek legal advice first before answering questions.

The election official should remain in contact with counsel after the officer executes the warrant to discuss the availability and applicability of legal procedures for challenging the legality of the warrant.

In most states and in the federal system, there are [procedures](#) [\[link-20\]](#) for challenging the legality of a warrant and [for](#)

[potentially](#) [\[link-21\]](#)

[returning](#) [\[link-22\]](#) items seized, as well as for restricting attempts at breaking through passwords or taking other measures to mitigate the potential for tampering or inadvertent damage to sensitive election records and equipment.

- For some voting systems, a copy of software and memory, as opposed to the original, could be provided in lieu of an original system over which the election official must maintain custody and access records under state law, or under the terms of a lease agreement with an election system vendor.
- In the case of ballots and other highly sensitive paper records, a federal court could be moved to consider principles of comity and abstain from a dispute that is essentially an election contest, so that it may be deferred to the appropriate state venue where

these contests are normally heard. State courts that hear election contests more regularly may have existing procedures for securely storing ballots. Courts may also be moved to secure materials and make them available for inspection only under bipartisan and nonpartisan observation.

- The public, voters, and candidates all have a strong interest in on-time, accurate certification of elections, and thus, in the preservation of election records and equipment from potential tampering or interference that could occur in the absence of nonpartisan and bipartisan observation and transparency. When appearing before a judge, the election official and their attorney can convey these and other factors relevant to any legal analysis.

If the officer has an “administrative warrant” not signed by a judge, the

official should immediately consult with counsel to determine the appropriate response.

In some states, state law or guidance governs the custody of election materials and may require a court order before any records — including copies — can be turned over to third parties. If consistent with state law and internal regulations, the election official can calmly state that they are not authorized to provide access to any records without a judicial warrant.

If the election official receives a subpoena for the materials sought, they should immediately consult counsel on appropriate next steps.

In some instances, officials may receive a subpoena for the materials sought. Subpoenas typically do not require immediate compliance but instead provide a deadline, and they may seek to quash the subpoena on certain grounds, such as confidentiality

laws or various other privileges, overbreadth, improper purpose, or risk to sensitive information. Election officials who receive a [grand jury subpoena](#) [link-23] may petition the court overseeing the proceeding to quash it or to request specific procedures for protecting sensitive records.

• • •

As new demands for access to election data and equipment escalate, election officials should be prepared to respond in a way that complies with the law, ensures transparency, protects sensitive information and staff safety, and guards the security of our election systems. By taking proactive steps now, officials will be better positioned to handle requests and maintain public confidence.

▢

Links

link-1: said <https://www.nytimes.com/2026/01/11/us/trump-voting-machines-2020-election.html?partner=slack&smid=sl-share>

link-2: nationalize [https://www.politico.com/news/2026/02/02/trump-nationalize-elections-2026-midterms-00760015?](https://www.politico.com/news/2026/02/02/trump-nationalize-elections-2026-midterms-00760015?utm_medium=twitter&utm_source=dlvr.it)

[utm_medium=twitter&utm_source=dlvr.it](https://www.politico.com/news/2026/02/02/trump-nationalize-elections-2026-midterms-00760015?utm_medium=twitter&utm_source=dlvr.it)

link-3: confirmed <https://www.reuters.com/world/americas/us-spy-chiefs-office-investigated-voting-machines-puerto-rico-2026-02-04/>

link-4: Elections Clause <https://constitution.congress.gov/browse/article-1/section-4/clause-1/>

link-5: Constitution charges states and Congress <https://statecourtreport.org/our-work/analysis-opinion/states-not-president-run-elections-america>

link-6: assessments <https://perma.cc/C45G-VWEK>

link-7: federal law [https://uscode.house.gov/view.xhtml?req=\(title:18%20section:611%20edition:prelim\)](https://uscode.house.gov/view.xhtml?req=(title:18%20section:611%20edition:prelim))

link-8: 52 U.S.C. Section 20701 <https://uscode.house.gov/view.xhtml?req=granuleid:USC-prelim-title52-section20701&num=0&edition=prelim>

link-9: rejected <https://storage.courtlistener.com/recap/gov.uscourts.cacd.988465/gov.uscourts.cacd.988465.128.0.pdf?inline=1>

link-10: plainly illegal <https://www.brennancenter.org/our-work/research-reports/voters-should-not-be-intimidated>

link-11: law <https://www.law.cornell.edu/uscode/text/18/592>

link-12: no emergency powers <https://www.brennancenter.org/our-work/research-reports/federal-and-state-election-laws-ban-federal-forces-polling-places>

link-13: forbid <https://codes.findlaw.com/co/title-24-government-state/co-rev-st-sect-24-30-2109/>

link-14: require <https://elections.cdn.sos.ca.gov/pdfs/voter-file-application.pdf?inline=1>

link-15: enough backup materials https://www.brennancenter.org/sites/default/files/2019-12/2019_12_ContingencyPlanning.pdf?inline=1

link-16: policies <https://www.justice.gov/jm/jm-9-85000-protection-government-integrity#9-85.500>

link-17: close <https://www.justice.gov/jm/jm-9-85000-protection-government-integrity#9-85.300>

link-18: impersonated <https://www.theguardian.com/us-news/2025/jul/24/colorado-election-clerks-voting-machines>

link-19: federal law https://www.law.cornell.edu/constitution/fifth_amendment

link-20: procedures https://www.law.cornell.edu/rules/frcmp/rule_41

link-21: for potentially <https://sdlawlibrary.libguides.com/c.php?g=1290776&p=9477489>

link-22: returning [https://www.nacdl.org/getattachment/c969375c-3447-472a-ade8-fdd88e960d4a/wilson-rule-41-g-motion-4ac.pdf?](https://www.nacdl.org/getattachment/c969375c-3447-472a-ade8-fdd88e960d4a/wilson-rule-41-g-motion-4ac.pdf?inline=1)

[inline=1](#)

link-23: grand jury subpoena [https://www.justice.gov/archives/usam/eousa-resource-manual-156-information-security-grand-jury-](https://www.justice.gov/archives/usam/eousa-resource-manual-156-information-security-grand-jury-information-guidelines-handling)

[information-guidelines-handling](#)