STATE OF COLORADO
Department of State
1700 Broadway, Suite 550
Denver, CO 80290

Jena M. Griswold
Secretary of State
Christopher P. Beall
Deputy Secretary of State

Office of the Secretary of State
Election Rules
8 CCR 1505-1

Colorado Secretary of State Comment to Proposed Rules

Supplemental Memorandum on Proposed Permanent Adoption of Temporary Rule Amendments to Rules 20.5.4, 21.7.3, 21.7.4

Introduction

The Department continually analyzes our election rules to ensure that the use of voting systems in Colorado is up to date, secure, and follows best practices. After review of current election rules and considering conditions on the ground, the Department determined that several rules related to voting systems needed revisions or additions to clarify the security and chain of custody requirements for those systems. In particular, the Department determined that the temporary rules adopted on June 17, 2021 should be considered for permanent adoption. The following comment is intended to provide some additional detail and context to the reasoning and necessity for these proposed changes.

Background

The Help America Vote Act, a federal law passed in 2002, requires that every state certify and maintain electronic voting equipment. Colorado law also requires that those systems meet certain criteria for usability, accessibility, and security. Colorado statute requires the Secretary of State to create a certification process for that equipment. Bi-partisan Secretaries of State have overseen the adoption and implementation of this process. With these requirements in mind, the Secretary of State's office has developed a complex process to certify and install voting equipment around the state. That process is described below.

5-Step Certification Overview

The first step to use of a voting system in the State of Colorado is certification. Certification of voting systems in Colorado is a five-phase process that involves the Secretary of State, the voting system vendor, and a voting system test lab that is nationally accredited by the Election Assistance Commission (EAC).

The first phase of certification is the **Application.** When a voting systems provider applies for certification to the Department, it lists both software and hardware that is part of the voting system, including part and version numbers. The application is updated throughout the certification process to reflect any changes that occur. The voting system provider and the Department arrange for a format and time for the provider to conduct a demonstration for the public to see and use the voting system under consideration.

The second phase is **Document Review**. In the application package the voting system provider also submits the technical data package, any test reports from testing for other jurisdictions, and a preliminary requirements matrix. During this phase, Department staff review these materials for compliance with requirements to determine what will be needed to be tested by the test lab.

The third phase is the **Test Plan**. The voting system provider works with the test lab to draft a test plan for the voting system. The provider then submits the draft plan to the Department. Department staff use the review of the materials from the Document Review phase to determine if the plan is acceptable. This phase is iterative, the provider may need to submit several revised versions of the test plan before staff determine it is acceptable for testing to begin.

The fourth phase is **Testing**. After Department staff approve the test plan, the test lab may commence testing. Throughout testing, if the test lab identifies deficiencies, the voting system provider may make slight modifications to the system so that the testing will be successful. The provider makes updates to the technical data package to address any changes made during testing, or if Department staff identify deficiencies in the documentation during the review.

The fifth phase is **Compliance Review**. After the completion of testing Department staff review the test report and completed final requirements matrix for compliance. For certification, the system must meet the major requirements and demonstrate that overall it complies with the intent of the law.

After the application for certification is approved or rejected following testing, the Department posts the documentation to the Secretary of State website within 30 days. The documentation posted includes: the technical data package; user guides; test reports; and documents from other certification campaigns, if applicable. Documentation with security or proprietary information is not posted.

Accept Software, Create Golden Image, Install Software (Trusted Build)

After the Department certifies a voting system, the certified version of the software is sent directly from the voting system test lab to the Department of State's office. The software does not come from the voting system provider. The software is copied on to one-write media (DVD-ROM) to ensure no changes can be made, and sent via overnight shipping. Separately, the test lab sends hash values for all of the certified applications so that the contents can be verified. This ensures the software being used in Colorado is the exact version of the software that was tested by the lab and certified by the Department of State.

Once the Department receives the certified software, background checked staff work directly with the voting system provider to install and configure the voting system software on components of the voting system. The components are completely fresh computers with no software installed, including an operating system, and have never been connected to the internet. The Department of State uses the Golden Image process when installing the voting system to make the installation process efficient, and to ensure that the same exact copy of the system is installed throughout the state. A Golden Image is a copy of a computer's memory that can be placed directly onto the hard drive of another computer so that the new computer's content directly mirrors the original computer's content.

The installation and configuration of the system is a complex process and takes a number of days to accomplish across all of the components and among the different types of computers that will be used in the state. At no time is any part left outside of the possession of Department staff, including meal breaks or overnight. At the end of each day interim images are created, sealed, and brought home with staff. Then those interim images are restored in the morning so that work may recommence.

When the installation process is complete and the system is thoroughly tested to make sure it is properly configured, images of all components across all computer models are created and saved onto a Root Drive. These image files are the Golden Images. The images on the Root Drive are copied onto other media to be taken by Department staff to be installed across the state. After the copies are made, the Root Drive, which is encrypted, is deposited in a safe at the Secretary of State's office (along with an exact backup of the Root Drive in case the data on the Root becomes corrupted).

In Colorado, voting systems are prohibited by rule from being connected to the internet. Because of this, installation of new software must be done with physical media. To ensure that the system is installed correctly, and to safeguard the security of the tabulation software, only a limited number of Department staff may possess and install the Golden Images that contain the certified voting system software on the voting system computers throughout the state. After the Root Drive is used to create the media to be used by Department staff, the new media is secured in locked cases. The cases are sealed with serialized tamper evident seals. When Department staff arrive in a county to install the Golden Images, a member of county staff and Department staff verify the seal number on the case is the same as what was written down when it was last sealed. This process is to ensure no one accessed any media.

During the in-county voting system installation Department staff and voting system provider staff perform different roles throughout the process. Department staff is responsible for the integrity of the tabulation software, including installing the images, ensuring security measures are intact, and hardening components. Voting system provider staff with training of Colorado election law and under the supervision of Department of State and county staff, are onsite to ensure that the newly installed system performs properly.

The final action in the installation process is county Acceptance Testing. In most cases this involves going through steps normally undertaken during a real election, but on a much smaller scale. It includes creating or loading a test election on all devices, using ballot marking devices

to mark ballots, running ballots through tabulation scanners, and verifying that the results match the count from the ballots.

Why are these proposed rules necessary?

Over the last several months, the Department and county clerks around the State of Colorado have been pressured to turn over voting systems and their components to unaccredited third parties. A holistic review of Colorado statutes and rules revealed that the security and chain of custody requirements for these systems did not fully contemplate the security issues that could arise in turning those systems over to third parties outside the normal course of certification.

As laid out in detail in this comment, the Department of State's office takes many steps to ensure that the chain of custody of a voting system is not broken from the time that system is certified for use. These detailed certification and installation steps help to ensure that the systems used in Colorado count the votes of Colorado voters accurately. Both the Department of State and counties throughout the state take the maintenance of the integrity of each election very seriously; a major component of this involves maintaining chain of custody from certification through final use. The U.S. Department of Justice has also indicated that maintaining documented chain of custody on voting systems is required under federal law.[1]

The proposed amendments to these rules ensure that the chain of custody on voting systems is not compromised with the use of unaccredited third-party access to voting systems. Chain of custody is a critical security measure that county clerks must maintain to ensure voting systems and their components function without error. In the event that chain of custody of a voting system is lost to a third party, the Secretary of State's office would not have confidence in the security of that system. The proposed amendments solve this issue by restricting use of those systems or removing their certification when the security of the system can no longer be established.

Supplemental Memorandum Regarding Other Misconceptions and Falsehoods concerning Proposed Rule Amendments

Introduction

During the written comment period and at the rulemaking hearing held on August 3, 2021, for these proposed amendments, the Department received a significant number of questions and comments regarding proposed amendments. These comments have, in many cases, misunderstood the purpose and effect of these proposed changes. To further clarify why these changes are being made, the Department is submitting the additional comments below.

False Claim #1: Proposed changes to Rule 2.13.2 decrease clerk authority to inactivate or otherwise process election records.

Truth: Changes to Rule 2.13.2 will not change clerk processing of voter records in any way.

[1] Attached as Exhibit A.

Authority for Change: Sections 1-1-107 (2)(a), 1-7.5-107(6), C.R.S.

Explanation: The proposed changes to Rule 2.13.2 only relate to cancelling records that meet the criteria for cancellation under Section 1-2-605(7), C.R.S. The changes suggested in the proposed rule amendment reflect practice that has been followed in the State of Colorado since 2018. In lieu of requiring every county to manually cancel those records, the statewide voter file (SCORE) has been developed to process these cancellations automatically. This development was completed under a prior administration and has been a significant cost and time savings for county clerks around the state. This proposed change will not take away or alter the responsibility or authority for county clerks to otherwise update, inactivate, or process voter registration records in Colorado.

--

False Claim #2: Proposed changes to Rule 7.7 (renumbered as 7.6) will alter the process for voters with a disability to receive and return an electronic ballot. The changes would allow voters who qualify to return a ballot without affirming they have a disability and without signing or returning an ID.

Truth: The proposed changes to Rule 7.7 are required by SB 21-188 and do not alter the process for voters with a disability to receive and return a ballot beyond the changes made in that legislation. A voter with a disability must still return a handwritten signature or copy of an ID with their ballot.

Authority for Change: Sections 1-1-107 (2)(a), 1-5-706, C.R.S.

Explanation: With the passage of SB 21-188, the Department of State is required to implement two specific changes. First, the Department is required to allow voters with a qualifying disability to return a ballot electronically. Second, the Department is required to allow voters with a disability to return an acceptable form of ID in lieu of a handwritten signature for the purpose of identifying the voter. The changes made to this rule clarify that if a ballot is returned from a voter with a disability who received their ballot electronically, that ballot must contain the application (which includes an affirmation that the voter was qualified to receive their ballot electronically under this section) and either a signature or an acceptable form of ID. If either of those requirements are missing, the rule requires the county clerk to send a letter to the voter to "cure" their ballot by providing the missing information. If the missing information is not provided by 8 days after election day, the ballot would not be counted.

--

False Claim #3: Proposed changes to Rule 7.8.1 (renumbered as 7.7.1) alter the signature verification process to reduce accountability.

Truth: The proposed changes clarify a practice that is already required by statute.

Authority for Change: Sections 1-1-107 (2)(a), 1-7.5-106 (2), 1-7.5-107(6), C.R.S.

Explanation: Section 1-7.5-107.3, C.R.S. describes a very specific process for the review of signatures on a mail ballot. That section of code states that the first review is to be conducted by "an election judge," who compares the signature on the envelope with the signature stored in SCORE. The proposed change to this rule clarifies in rule what is already required by statute. This rule does not alter the practice of using bipartisan teams of judges at any subsequent review level.

--

False Claim #4: Proposed changes to Rule 7.8.11 (renumbered as 7.7.13) remove the requirement for clerks to test a signature verification device before its use in an election

Truth: The proposed changes maintain and clarify the requirement that county clerks test signature verification devices before their use in an election.

Authority for Change: 1-7.5-107.3 (5) and (6), C.R.S.

Explanation: Over the last election cycle, it was brought to the Department's attention that the current rules regarding the testing of signature verification devices did not standardize how and when these devices should be tested. In response, the Department has offered this proposed change. The change would require the county clerk to test the devices on the first 150 ballot envelopes received before deploying them for full use. The test would involve the use of a bipartisan team of election judges who would review the same signatures as the machine to determine if the machine is accepting signatures it should not. In the event that a discrepancy is identified, the clerk is required to cease use of that device until any issues are identified and a solution is offered.

During the public hearing, several members of the public offered that testing these devices with the first 150 signatures received in an election had the potential to undermine those ballots tested. This is false. As explained above, each of these envelopes would be reviewed by human election judges. The inspection process called for in this rule change would increase, rather than diminish, the reliability of the review of the envelopes used to conduct it.

--

False Claim #5: Proposed changes to Rule 9.2.2 make it more difficult to remove deceased voters from voter roll.

Truth: The proposed changes relate to mail ballot challenges. Those challenges have never resulted in removing a voter from the voter rolls as these challenges would potentially lead to a ballot not being counted, not that voter's removal from the voter rolls. County clerks regularly remove deceased Coloradans from the rolls under Section 1-2-602, C.R.S. These proposed changes do not alter that process in any way.

Authority for Change: Sections 1-7.5-106 (2), 1-7.5-107 (6), 1-9-210, C.R.S.

Explanation: In Colorado, voter records are cancelled due to the death of the registrant under Section 1-2-602, C.R.S. That section of the code allows county clerks to cancel a voter record if they receive information from the Colorado Department of Public Health and Environment that the registrant is deceased. County clerks may also cancel a record for a registrant if they receive written notice from a family member that the voter is dead. Challenging a mail ballot due to the death of the voter does not, and never did, result in removing that voter from the rolls. It can, however, result in that mail ballot not being counted, and this proposed rule change does not alter that fact.

This rule change is being proposed because the current rule does not identify how a challenge should be processed in the event that two election judges disagree. The Department relied on other similar bipartisan judge provisions in Colorado statute when proposing the current version of the rule. *See e.g.* Section 1-7.5-107.3 (2)(a), C.R.S. (signature on envelope rejected if two judges agree it is discrepant). Like a disagreement over a signature on a mail ballot envelope, the proposed rule would accept the challenged ballot for processing in the event that election judges could not agree on the challenge. In the event that the challenge was rejected, it would still be forwarded on to the voter and the District Attorney following the election, as required by statute.

--

False Claim #6: Proposed repeal of rules 20.11.2 and 20.19.5 will eliminate or reduce chain-of-custody logs and other security measures.

Truth: None of the rule changes proposed will eliminate or reduce chain of custody logs and other security measures. The rules referenced for this claim are being removed because they refer to systems and machines that are no longer used in Colorado.

Authority: Sections 1-1-107(2)(a), 1-5-616(1), C.R.S.

Explanation: This false claim is premised on a basic misunderstanding of the applicability of rules 20.11.2 and 20.19.5.

Rule 20.11.2 put in place requirements for transporting memory cards or cartridges. The memory cards and cartridges referred to in this rule have not been in use in Colorado since at least 2019. The Department has proposed repealing this rule as a clean-up measure. The Department regularly reviews election rules for outdated references and removes those references when they are no longer needed.

Similarly, Rule 20.19.5 put in place chain of custody requirements for ballot scanners. As used in this rule, the term “ballot scanners” refers to precinct-based ballot scanners, which have not been used in Colorado since 2016. Like Rule 20.11.2, the Department has proposed this repeal as a clean-up measure.

The proposed rules do not alter the rules that are related to chain of custody logs and the secure transportation of equipment currently in use in Colorado. Those rules remain in place and are not part of this proposed rulemaking. *See* Election Rules 1.1.13, 1.1.39, 1.1.43, 11.3.2(e)(1), 18.4.6, 20.3, 20.11.1, 20.11.3, 20.11.4, 20.17, 20.19.3, 25.2.2(d), 25.2.3(a), 26.10.4(a).

Exhibit A

U.S Department of Justice Guidance:
Federal Law Constraints on Post-Election "Audits"

Federal Law Constraints on Post-Election "Audits"

Published July 28, 2021

The U.S. Department of Justice is committed to ensuring full compliance with all federal laws regarding elections. This includes those provisions of federal law that govern the retention and preservation of election records or that prohibit intimidation of, or interference with, any person's right to vote or to serve as an election official.

The Department is also committed to ensuring that American elections are secure and reflect the choices made on the ballots cast by eligible citizens. "The November 3rd election was the most secure in American history," according to a Joint Statement issued by federal and state officials and released by the federal Cybersecurity & Infrastructure Security Agency. In many jurisdictions, there were automatic recounts or canvasses pursuant to state law due to the closeness of the election results. None of those state law recounts produced evidence of either wrongdoing or mistakes that casts any doubt on the outcome of the national election results.

In recent months, in a number of jurisdictions around the United States, an unusual second round of examinations have been conducted or proposed. These examinations would look at certain ballots, election records, and election systems used to conduct elections in 2020. These examinations, sometimes referred to as "audits," are governed, in the first instance, by state law. In some circumstances, the proposed examinations may comply with state law; in others, they will not. But regardless of the relevant state law, federal law imposes additional constraints with which every jurisdiction must comply. This document provides information about those federal constraints, which are enforced by the Department of Justice.

Constraints Imposed by the Civil Rights Act of 1960

The Civil Rights Act of 1960, now codified at 52 U.S.C. §§ 20701-20706, governs certain "[f]ederal election records." Section 301 of the Act requires state and local election officials to "retain and preserve" all records relating to any "act requisite to voting" for twenty-two months after the conduct of "any general, special, or primary election" at which citizens vote for "President, Vice President, presidential elector, Member of the Senate, [or] Member of the House of Representatives," 52 U.S.C. § 20701. The materials covered by Section 301 extend beyond "papers" to include other "records." Jurisdictions must therefore also retain and preserve records created in digital or electronic form.

The ultimate purpose of the Civil Rights Act's preservation and retention requirements for federal elections records is 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) (citing H.R. Rep. 956, 86th Cong., 1st Sess. 7 (1959)), aff'd sub nom. Dinkens v. Attorney General, 285 F.2d 430 (5th Cir. 1961) (per curiam). The Act protects the right to vote by ensuring that federal elections records remain available in a form that allows for the Department to investigate and prosecute both civil and criminal elections matters under federal law. The Federal Prosecution of Election Offenses, Eighth Edition 2017 explains that "[t]he detection, investigation, and proof of election crimes – and in many instances Voting Rights Act violations – often depend[s] on documentation generated during the voter registration, voting, tabulation, and election certification processes." Id. at 75. It provides that "all documents and records that may be relevant to the detection or prosecution of federal civil rights or election crimes must be maintained if the documents or records were generated in connection with an election that included one or more federal candidates." Id. at 78.

The Department interprets the Civil Rights Act to require that covered elections records "be retained either physically by election officials themselves, or under their direct administrative supervision." Federal Prosecution of Elections Offenses at 79. "This is because the document retention requirements of this federal law place the retention and safekeeping duties squarely on the shoulders

of election officers." *Id.* If a state or local election authority designates some other individual or organization to take custody of the election records covered by Section 301, then the Civil Rights Act provides that the "duty to retain and preserve any record or paper so deposited shall devolve upon such custodian." 52 U.S.C. § 20701.

Therefore, if the original election official who has custody of records covered by the Act hands over those election records to other officials (for example, to legislators or other officeholders) or the official turns over the records to private parties (such as companies that offer to conduct "forensic examinations"), the Department interprets the Act to require that "administrative procedures be in place giving election officers ultimate management authority over the retention and security of those election records, including the right to physically access" such records. *Id.* In other words, the obligation to retain and preserve election records remains intact regardless of who has physical possession of those records. Jurisdictions must ensure that if they conduct post-election ballot examinations, they also continue to comply with the retention and preservation requirements of Section 301.

There are federal criminal penalties attached to willful failures to comply with the retention and preservation requirements of the Civil Rights Act. First, Section 301 itself makes it a federal crime for "[a]ny officer of election" or "custodian" of election records to willfully fail to comply with the retention and preservation requirements. 52 U.S.C. § 20701. Second, Section 302 provides that any "person, whether or not an officer of election or custodian, who willfully steals, destroys, conceals, mutilates, or alters any record or paper" covered by Section 301's retention and preservation requirement is subject to federal criminal penalties. *Id.* § 20702. Violators of either section can face fines of up to $1000 and imprisonment of up to one year for each violation.

Election audits are exceedingly rare. But the Department is concerned that some jurisdictions conducting them may be using, or proposing to use, procedures that risk violating the Civil Rights Act. The duty to retain and preserve election records necessarily requires that elections officials maintain the security and integrity of those records and their attendant chain of custody, so that a complete and

uncompromised record of federal elections can be reliably accessed and used in federal law enforcement matters. Where election records leave the control of elections officials, the systems for maintaining the security, integrity and chain of custody of those records can easily be broken. Moreover, where elections records are no longer under the control of elections officials, this can lead to a significant risk of the records being lost, stolen, altered, compromised, or destroyed. This risk is exacerbated if the election records are given to private actors who have neither experience nor expertise in handling such records and who are unfamiliar with the obligations imposed by federal law.

Constraints Imposed by the Federal Laws Prohibiting Intimidation

Federal law prohibits intimidating voters or those attempting to vote. For example, Section 11(b) of the Voting Rights Act of 1965 provides that "No person, whether acting under color of law or otherwise, shall intimidate, threaten, or coerce, or attempt to intimidate, threaten, or coerce any person for voting or attempting to vote, or intimidate, threaten, or coerce, or attempt to intimidate, threaten, or coerce any person for urging or aiding any person to vote or attempt to vote…." 52 U.S.C. § 10307(b). Similarly, Section 12 of the National Voter Registration Act of 1993 makes it illegal for any person, "including an election official," to "knowingly and willfully intimidate[], threaten[], or coerce[], or attempt to intimidate, threaten, or coerce, any person for . . . registering to vote, or voting, or attempting to register or vote" in any election for federal office. *Id.* § 20511(1)(A). Likewise, Section 131 of the Civil Rights Act of 1957 provides that "[n]o person, whether acting under color of law or otherwise, shall intimidate, threaten, coerce, or attempt to intimidate, threaten, or coerce any other person for the purpose of interfering with the right of such other person to vote or to vote as he may choose, or of causing such other person to vote for, or not to vote for, any candidate" for federal office. 52 U.S.C. § 10101(b).

The Attorney General is authorized to file a civil action seeking preventative relief, including a temporary or permanent injunction, against any person who engages in actions that violate these statutes. See 52 U.S.C. §§ 10308(d); 20510(a). And there are criminal penalties as well. *See, e.g., id.* § 10308(a); 18 U.S.C. §§ 241, 242, 594; *see generally* Federal Prosecution of Election Offenses, at 33-38, 49-54, 56-58.

Judicial decisions have established that voter intimidation need not involve physical threats. In certain contexts, suggesting to individuals that they will face adverse social or legal consequences from voting can constitute an impermissible threat. Here are a few examples of the types of acts that may constitute intimidation:

- Sending a letter to foreign-born Latino registered voters warning them that "if they voted in the upcoming election their personal information would be collected … and … could be provided to organizations who are 'against immigration'" was potentially intimidating. *See United States v. Nguyen*, 673 F.3d 1259 (9th Cir. 2012).
- Having police officers take down the license plate numbers of individuals attending voter registration meetings contributed to intimidating prospective voters. *See United States v. McLeod*, 385 F.2d 734 (5th Cir. 1967).
- Sending robocalls telling individuals that if they voted by mail, their personal information would become part of a public database that could be used by police departments to track down old warrants and credit card companies to collect outstanding debts could constitute intimidation. *See Nat'l Coal. on Black Civic Participation v. Wohl*, 498 F. Supp. 3d 457 (S.D.N.Y. 2020).
- Linking individual voters to alleged illegalities in a way that might trigger harassment could constitute intimidation. *See League of United Latin Am. Citizens - Richmond Region Council 4614 v. Pub. Int. Legal Found.*, 2018 WL 3848404, at *4 (E.D. Va. Aug. 13, 2018).
- Conducting a "ballot security" program in which defendants stand near Native American voters discussing Native Americans who had been prosecuted for illegally voting, follow voters out of the polling places, and record their license plate numbers might constitute intimidation. *See Daschle v. Thune*, No. 4:04 Civ. 04177 (D.S.D. Nov. 1, 2004).

See also United States v. North Carolina Republican Party, No. 5:92-cv-00161 (E.D.N.C. Feb. 27, 1992) (approving a consent decree in a case where the United States alleged that it violated Section 11(b) to send postcards to voters in predominantly African American precincts falsely claiming that voters were required to have lived in the same precinct for thirty days prior to the election and stating that it is a "federal crime to knowingly give false information about your name, residence or period of residence to an election official").[1]

[1] While voter intimidation need not involve physical threats, federal law of course prohibits using "force or threat of force" to intimidate or interfere with, or attempt to intimidate or interfere with, any person's "voting or qualifying to vote" or serving "as a poll watcher, or any legally authorized election official, in any primary, special, or general election." 18 U.S.C. § 245(b)(1)(A). The Deputy Attorney General recently issued Guidance Regarding Threats Against Election Workers.

There have been reports, with respect to some of the post-2020 ballot examinations, of proposals to contact individuals face to face to see whether the individuals were qualified voters who had actually voted. *See, e.g.*, Cyber Ninjas Statement of Work ¶ 5.1 (proposing to select three precincts in a large urban county to collect information from individuals through "a combination of phone calls and physical canvassing").

This sort of activity raises concerns regarding potential intimidation of voters. For example, when such investigative efforts are directed, or are perceived to be directed, at minority voters or minority communities, they can have a significant intimidating effect on qualified voters that can deter them from seeking to vote in the future. Jurisdictions that authorize or conduct audits must ensure that the way those reviews are conducted has neither the purpose nor the effect of dissuading qualified citizens from participating in the electoral process. If they do not, the Department will act to ensure that all eligible citizens feel safe in exercising their right to register and cast a ballot in future elections.

If jurisdictions have questions about the constraints federal law places on the kinds of post-election audits they can conduct, they should contact the Voting Section of the Civil Rights Division. If citizens believe a jurisdiction has violated the Civil Rights Act's election record retention and preservation requirements, or believe they have been subjected to intimidation, they can use the Civil Rights Division's online complaint form to report their concerns or call (800) 253-3931.