Statement of Objections to Proposed Rule Changes, 8 CCR 1505-1

Hearing Date: May 24th, 2022

Shawn Smith

In the legislative declaration at CRS § 24-4-101.5, the Title, Article, and Part which mandate this rulemaking hearing by the Secretary of State to not only afford, but heed, public comment regarding the Secretary's proposed rule changes, the General Assembly of Colorado states:

"The general assembly finds that an agency should not regulate or restrict the freedom of any person to conduct his or her affairs, use his or her property, or deal with others on mutually agreeable terms unless it finds, after a full consideration of the effects of the agency action, that the action would benefit the public interest and encourage the benefits of a free enterprise system for the citizens of this state."

Without question, the Secretary's proposed rule changes fail that simple test, by restricting local control and transparency to citizens of their own elections, de facto depriving them of any reasonable basis for trust in their elections, or any reason for their election of local chief election officials. Her proposed rules do not benefit the public interest; they only benefit her consolidation of power in her own office. In direct response to the revelations resulting from the exposure of Colorado voting system information to highly-qualified, independent computer experts, the Secretary of State has attempted in her Rules and in legislative changes she has promoted, not to address the revelations of vulnerability and criminal violation of statute themselves, but to prevent the public from ever again having the opportunity to hear from independent sources of expertise whether their elections truly are the "gold standard." Within the past two years, in particular, the Secretary of State has careened toward a restructuring of Colorado's election system, supported by a derelict General Assembly majority, which demands that citizens allow voting system vendors and the Secretary of State to decide what is true, and to do so without the opportunity for citizens to exercise the scrutiny which must be the citizens' right, as sovereign.

Furthermore, the Secretary's continued assertion of counterfactual claims regarding the requirement to preserve as election records the complete audit trail information from computer-based voting systems, prescribed by Federal Voting System Standards mandated by Colorado statute, and the Secretary's apparently willfully deceptive or unfathomably ignorant assumptions regarding the sufficiency of the "safeguards" she has required, as well as her prior and sustained certification of voting systems which do not and cannot meet those voting system standards, and her introduction of uncertified, untested software to those certified voting systems, in violation of Colorado statute, as well as her reliance upon an unaccredited Voting System Testing Lab, all point to a fundamental incapacity on her part and in her office to secure the purity of Colorado elections and to safeguard the elective franchise. Her talking points, with respect to protecting voting rights, are fantastic. Her conduct, with respect to protecting voting rights, is abysmal and criminal.

Specific objections to these rules:

With respect to Rule 1.1.1, “active ballot” presumes that the digital ballot record of and all scanned ballots represent a given eligible voter’s intent with a cast ballot, but Mesa forensic reports showed not only that the voting system does not comply with 2002 Voting System Standards, making the voting system illegal to certify for or use in Colorado elections, but that machine manipulation can change the results of adjudication, and canvassing showed that eligible voters’ cast ballots may not be counted, and that ineligible voters cast ballots may be counted.

With respect to 1.1.17, “County” or “County Clerk” cannot mean “others employed or appointed by the County Clerk to carry out the duties of the County Clerk in the administration of an election” because CRS § 1-1-110(2) is explicit in authorizing only the “deputy clerk in the absence of the county clerk and recorder or if the county clerk and recorder for any reason is unable to perform the required duties.” I.e., a County Clerk may task election officials, made so by their own declaration, within their respective County, but the Secretary of State may not authorize or empower any election official in a County in contradiction of CRS § 1-1-110.

With respect to Rule 1.1.21, the Secretary of State may not, in a Rule, expand the definition of “Secretary of State” to include “personnel employed by the Secretary of State,” because CRS 24-21-105 is explicit in restricting the authority of the Secretary of State to appoint and authorize others to exercise the Secretary of State’s authority, stating “The secretary of state may appoint a deputy to act for him if he deems it necessary, who shall have full authority to act in all things relating to the office. The secretary shall be responsible for all acts of such deputy.” In other words, the Secretary may task personnel within her department, but may not authorize them to act in her place, e.g. to approve the certification of voting systems for purchase or use in Colorado, without explicitly and officially designating each of those personnel as a “Deputy.”

With respect to Rule 1.1.23, the implicit assertion that the Secretary of State, or any other Election Official, has a right or the ability to “adjudicate” the intent of a voter who has mismarked, overmarked, or marked duplicate choices on a ballot, assumes the authority and capability of Election Officials in contradiction to CRS §1-7-309(1), which states “Votes cast for an office to be filled or a ballot issue to be decided shall not be counted if an elector marks more names than there are persons to be elected to an office or if for any reason it is impossible to determine the elector's choice of candidate or vote concerning the ballot issue.” The Secretary of State has approved voting systems for purchase and use which not only have a digital capability to alter the ballot record, but for which the criteria to do so are variable and unverifiable by election judges and electors; no voting system may be used which enables or allows “adjudication” that includes the counting of votes from a ballot on which a voter had overvoted or undervoted, but voting systems certified by the CO Secretary of State have that capability.

With respect to Rule 1.1.29, the Secretary of State is attempting to establish a vendor-specific term, “Election Project Backup,” as a mechanism for backup and preservation of election records, but that mechanism does not preserve all log files and other artifacts (including all operating system log files for any “COTS”-based component of a voting system running voting system software) identified as mandatory standards for audit trails in the 2002 Voting System Standards, which are a statutory minimum standard for voting systems in Colorado under CRS § 1-5-601.5. Restricting and impeding County Clerks from conducting full or partial hard drive images interferes with the discharge of their duty with respect to 52 U.S.C. §20701 and CRS §

1-7-802, which require the preservation of election records for 22 and 25 months, respectively. Any rule or order by the Secretary of State which interferes with the discharge of duty by election officials to take adequate steps to preserve all election records explicitly or implicitly identified in the 2002 Voting System Standards is a de facto violation of CRS § 1-13-701.

With respect to Rule 1.1.38, in requiring that observers be only either appointed by the Secretary of State or by the Federal government and approved by the Secretary of State, the Secretary of State proposes to violate 52 U.S.C §10305, which prescribes that observers may be appointed by a court and also by several agencies of the Federal government, with no provision that the appointed observers be approved by the Secretary of State. The failure of both the Secretary of State and the Colorado Attorney General to either notice or respect the Federal statute is ample evidence that an outside special counsel should be appointed by a court to review all rules and procedures enacted by the Secretary of State, to determine the full extent to which the Secretary of State has failed to abide, flouted, or violated Federal statutes.

With respect to Rule 1.1.47, if "Secure Ballot Area" does not include all ballot drop boxes and all facilities, vehicles, and locations (e.g. the vehicles and containers used by individuals retrieving ballots from ballot drop boxes, or all USPS facilities and vehicles involved in conveying cast ballots) within which cast ballots may be present after being marked by an eligible elector and prior to verification of the affidavit signature of an eligible elector, then those areas must be considered "not secure" and therefore not suitable or approved for use in elections.

With respect to Rule 1.1.48, copying of election files to and from memory cards and flash media and programming of voting system components both occur in Voter Service and Polling Centers where ballot-marking devices are used by electors, as well as in the area where smartcards are programmed for use at the ballot-marking devices to provide to electors, therefore those areas must, by this rule, be designated as "secure equipment areas," however new Rule 20.4 requires that the Counties restrict access to these designated "secure equipment areas," and doing so would restrict the access of eligible electors. Therefore Rule 1.1.48 and Rule 20.4, as proposed, violate the Civil Rights Act of 1960 and violate the Equal Protection clause of the U.S. Constitution by restricting in-person voters.

With respect to Rule 1.1.39, renumbered to 1.1.51, the assumption and assertion that a serially-numbered tamper-evident seal is adequate to either prevent or reveal tampering is faulty and without evidence, as numerous tutorials are publicly available which illustrate methods of successfully bypassing the tamper-evident seals without revealing that tampering has, in fact, occurred.

With respect to Rule 1.1.45, the inclusion of "mechanical, electromechanical, or electronic equipment (including the software, firmware, and documentation…) that is used to: …(4) Maintain and produce any audit trail information" as part of a "voting system" is illogical, overly broad, and illegal, in that it interferes with County election officials' authority and responsibility to preserve election records in the form of copies of electronic files generated on the voting system but separate from it. If the voting system can be operated without the copies, then it stands to reason that the copies are not part of the voting system. If the copies can be destroyed without affecting the operation of the voting system, then it stands to reason that the copies are not part of the voting system. If the copies cannot be used, in and of themselves, to duplicate the function of the voting system, then it stands to reason that the copies are not part of the voting system.

With respect to Rule 2.15.5, the Secretary of State has no authority to redefine or issue rules which modify the legislative intent of Article 72 of Title 24; her attempted restriction of "custodian" with respect to County Clerks ignores the "authorized person" aspect of CRS §24-72-202(1.1) and thereby exceeds her authority and violates CRS. Also, there is no "Part 21, Article 72 of Title 24, C.R.S." This level of inattention to or disregard for the law disastrously characterizes the Secretary of State's conduct with respect to election law and the rights of citizens under our Constittuion.

With respect to Rules 1.1.53, 1.1.54, 1.1.56, and 1.1.57 the Secretary of State proposes to count votes cast by an eligible elector for a candidate to another candidate; this explicitly violates both Federal and State statute by counting the votes differently than the eligible elector's cast ballot. Furthermore, the use of fractional vote counts and totals and the machine-transfer of votes between candidates impedes transparency in elections, depriving citizens of the Constitutional rights to free and fair elections and the transparency necessary to verify that freeness and fairness for themselves.

With respect to Rule 4.1.2, the proposed imposition of a requirement that translation be "culturally appropriate" is overly broad and ambiguous, and cannot thus be within the authority of the Secretary of State to either regulate or mandate.

With respect to Rule 4.8.2, the proposed imposition of a restriction on nicknames which "contain a political slogan or other political speech" is overly broad and ambiguous, subject to arbitrary determination by public officials, and therefore invites bias, and also restricts the inherent freedom of individual candidates to express themselves in accordance with the First Amendment. The Secretary must either allow nicknames or disallow nicknames, but may not exercise any authority to approve some nicknames and not others.

With respect to Rule 4.8.8 (B), the Secretary proposes inappropriately to require that a translator or interpreter "produces translations that are …culturally appropriate." The Secretary herself has no basis of certification or expertise to make that determination and must be prohibited from the assertion or exercise of the arbitrary authority she describes.

With respect to Rule 6.9, that the County must immediately inform the Secretary of State's office in writing in the event that an election judge is removed from duty by the County, the Secretary of State cites no statutory authority or purpose for the Rule, and her assumption of the authority to require that County officials notify her ignores CRS § 1-6-119 and the will and intent of the legislature, which has prescribed procedures for election judge removal and saw fit to assign no related authorities whatsoever to the Secretary of State.

With respect to rule 7.2.14, the entire exercise of determining which party's ballot an elector returned is unnecessary except for the imposition of the open primary, which invites the fraud of non-members of a political party having the opportunity to select the candidates of that political party, and involves the conflation of party candidate selection with the government function of conducting elections. The government should have no involvement whatsoever in the conduct of a partisan primary election, and should expend no government funds, and use no government resources, to conduct or assist in a partisan primary election. Providing for the indication or means for a county to determine, before opening a ballot envelope, which party's primary election ballot the elector returned, also provides a means for discrimination against voters of a particular party. Since the Secretary has procedures for handling the determination of which party's primary ballot was returned by an elector without the means of determination

before opening the envelope, the pre-opening means represents an unnecessary opportunity for discrimination against the voters of a particular party, which might occur at anytime during which the ballot envelope for a cast ballot is out of the elector's possession and not yet opened to be counted.

With respect to Rule 7.4.1, the requirement to "use a video surveillance recording system" to monitor each ballot drop box location is meaningless without the requirements that the video be of sufficient quality, resolution, and angle to ensure that anyone committing a crime involving the drop box can be identified, and also that 100% of the surveillance video for any election cycle be reviewed by election officials in the respective political jurisdiction, and made available to the public for their review, without the need for a request of any kind. Like the asserted "safeguard" of having paper ballots, the "safeguard" of having video surveillance is meaningless without compulsory, comprehensive review of the video for abnormalities and illegality; these are not safeguards, they are placebos.

With respect to Rule 7.10.3, the security rules promulgated by the Secretary of State under Rule 2.17/20.9.1(B) are grossly inadequate to protect the security of SCORE and the voter registration data contained therein, and thus represent a breach of duty under Title 1, enacted to secure the purity of elections and safeguard the elective franchise. Specifically, there is no basis for confidence that "county-controlled access to networks" or "proper network security controls" are sufficient, and WPA2 wireless security is an inadequate and vulnerable security standard, and no password should be shared, and the use of numbers and mixed case letters instead of increasing password length reflects outdated and ineffective password security standards. Furthermore, the fact that vulnerabilities were discovered in SCORE, exposing SCORE data to compromise and manipulation, in both 2015 and 2020, and that the Secretary of State never directed a comprehensive independent forensic examination to determine the extent of SCORE data compromise, reveals a disturbing neglect of fundamentals for security and auditing. The internal security controls for SCORE failed and, having failed, an independent auditor should have been engaged to conduct a comprehensive independent audit of SCORE to determine the results and impact of those discovered vulnerabilities.

With respect to Rule 7.16.3, the Secretary of State's requirement that VSPCs be arranged to ensure that election officials and other voters may not observe how a BMD voter marks or casts their ballot also necessarily allows for undetected access to the BMD that would allow the compromise of the BMD to exploit the vulnerability identified by J. Alex Halderman in his declaration in the Curling case in Georgia, and thus, exposes the voting system and the elections in Colorado to fraud and compromise.

With respect to Rule 8.10.2(7), the Secretary of State's elimination of logic and accuracy tests as an "election-related activity" subject to watcher access has no logical basis and has the effect of preventing or allowing the prohibition of watcher access to logic and accuracy tests which are, in any case, almost entirely useless to verify the proper and secure functioning of a computer-based voting system, since the entirety of the configuration and functionality of a computer-based voting system can be altered by a single-bit code change. At a minimum, witnesses to logic and accuracy tests should include all watchers, but also any other uncredentialed individuals as space limitations and safety codes allow. Furthermore, all election-related activity should be subject to uninterrupted video surveillance such that any member of the public can observe any aspect of the election-related activity at any time, since all citizens have equal right to know and observe the election activities for themselves.

With respect to Rule 11.4, the Secretary of State's insistence and prescription for backups of Election Database Projects and complete negligence to describe and specify backup of election records which would encompass all required files and data explicitly described under the 2002 Voting System Standards, reflects a breach of her duty to ensure the Federal and State statutes regarding election records are complied with, and her interference with the discharge of duty by county election officials. Her neglect of the statutory requirements includes but is not limited to failure to backup non-proprietary operating system files and logs from the election management system server, but also complete and utter neglect of the requirement to preserve log and audit trail records from other, non-EMS components of the voting system. Furthermore, because she has approved the certification of voting systems in the State of Colorado which, by design and configuration mandatory under her promulgated technical data for the voting systems, automatically and systematically deletes election records in the form of log files, the Secretary has ensured that all counties using those voting systems will violate both Federal and State statute.

With respect to Rule 11.4.3, requiring counties to submit hash values for election setup records files to the Secretary of State, the Secretary, knowing full well that she retains control over voting system BIOS passwords, and that voting system vendors retain supervisor account passwords, and that the voting system components are procured from overseas, without any supply-chain security whatsoever, and with inadequate hardware, software, and firmware security verification by Voting System Testing Labs, the personnel of which, in any case, have admitted in court records to possessing no particular cybersecurity expertise or background, implies and asserts that the voting systems are secure when, in fact, having had no supply-chain security whatsoever, and there being no standards in the applicable 2002 Voting System Standards, no in the standards for accreditation of Voting System Testing Labs, they can never be secured. The Secretary certifies and allows the use of unsecure and unsecurable voting systems, violating the Colorado Constitution, Article VII, Section 11, and violating the rights of Colorado citizens.

With respect to Rule 20.2.3(E), the Secretary inappropriately asserts an authority to restrict or prescribe restrictions on access granted by County election officials to Election Project Backups and the media containing them, and other copies of election records, but the preservation of these records involves a duty of election officials not subject to discernment or modification by the Secretary of State. Furthermore, the Secretary has demonstrated a profound ignorance of or disregard for the necessary and intended scope of these records, with respect to the explicit requirements for audit trail records described in the 2002 Voting System Standards and subsequent Voluntary Voting System Guidelines. Being that the Secretary is the individual who has destroyed and been responsible for the destruction of the greatest volume of election records in Colorado history, the People have no reason to entrust her office with access determinations related to each County Clerk's responsibilities as an election official.

With respect to Rule 20.3.2(B), and (D), the fact that majority of the computers and components in Colorado's certified voting systems were manufactured overseas, of overseas components, without any supply chain security whatsoever, and the absence of sufficient technical competency and proficiency in the Secretary of State's and county staffs, makes obvious the futility and inappropriateness of requiring county officials to pretend that they can train anyone to "detect tampering with voting equipment, memory cards, or election data."

With respect to Rule 20.5, the Secretary of State's proposed rules implicitly indicate that following the rules will result in the "security" of the voting systems; nothing could be further from the truth. The voting systems incorporate components manufactured in foreign countries, by foreign workers, of foreign components, with no supply chain security and no requirement nor capability on the part of either the Secretary of State or the Voting System Testing Labs to conduct any testing or component verification approaching adequacy to detect or mitigate compromises.

With respect to Rule 20.5.2(B), the Secretary of State inaccurately implies that a copy of a hard drive or any part of a hard drive, not incorporated into and necessary for the function and use of a voting system, comprises a "component" of the voting system. This is obviously inaccurate and unwarranted, and only technical illiteracy or a desire to extend her authority over functions and resources to which it does not pertain could motivate this assertion.

With respect to Rule 20.5.2(C), the Secretary's restriction on use for the Administrative User Account reflects the Secretary's awareness of the fact that the Administrative User Account is effectively a shared use account, and therefore that the Administrative User Account represents a violation of the 2002 Voting System Standards numerous clear requirements that no action on a voting system be unattributable to an individual user, e.g. in para 2.2.5, which requires that only identified users affect the system while election software is running, or para 3.2.3.1, which requires that voting systems shall accurately record all election management data entered by the user, and that "all systems shall: a. Record every entry made by the user."

With respect to Rule 20.5.2(C)(10), the Secretary of State's proposed rule that the Voting System Provider may not have administrative or user access to the county's election management system is unsatisfiable and unverifiable, since the Secretary has approved certification of voting systems which are built for remote access undetectable to local, including county, officials, including the incorporation of numerous wireless networking devices, central processing unit chipsets from Intel which incorporate what Intel calls "Active Management Technology," built for remote out-of-band access and configuration, and components such as the integrated Dell Remote Access Controller(iDRAC), again, built for the sole purpose of facilitating remote out-of-band management of the computer system and network, without either detection or approval of local officials and operators. Furthermore, the manuals for some voting systems certified by the Secretary of State for purchase and use in Colorado specifically identify supervisory access by voting system vendors which allows their employment of functionality and features on the voting systems neither accessible nor modifiable by election officials.

With respect to Rule 20.5.3(A)(1), the Secretary's rule that County Clerks must ensure wireless capability or devices in voting systems are disabled is impossible for Clerks to satisfy. In the first place, the Clerks do not have BIOS access, necessary to even verify that the devices are not being employed by nor are accessible to the operating system. In the second place, the hardware incorporated in the voting systems is designed to be able to employ embedded and connected wireless and other networking devices without reference to or awareness by the operating system. In the third place, as previously described, the total absence of supply chain security in the manufacturing of the voting system components and in the testing regime required for Secretary of State certification, means that not only do County Clerks have no ability to meet this requirement, neither does the Secretary of State.

With respect to Rules 20.5.3(C)(2)-(4), the Secretary of State requires that removable storage devices may not be connected to a voting system without first reformatting the device but the Secretary allows and instructs the counties to use the voting system vendor-provided reformatting application and permits the counties to connect a removable storage device, unreformatted, which has been connected to SCORE, which is already known to have been exposed to multiple vulnerabilities, and which has had no comprehensive independent audit to determine its integrity or security, or if the storage device contains files "remotely programmed by the voting system provider." This rule and the exceptions again illustrate either the Secretary of State's gross ignorance of the cyber threat to critical systems, or her blatant disregard for the best and recommended security practices to mitigate that threat. SCORE is not secure. Downloaded files from a vendor are not secure. Untested, uncertified vendor-proprietary software is unacceptable, from a security and election integrity standpoint, to ensure the security and integrity of the voting system. The Secretary makes no provision for and apparently has either no concern for or awareness of the possibility of portable code, hidden and encrypted partitions that may be present on removable storage devices, or the inability of either CDOS or county election officials to detect or mitigate the risks implied by those threats.

With respect to Rule 20.5.3(D), the Secretary of State has misinterpreted this, her own rule, to imply that she has authority to install software on a component of the voting system; she does not, except in accordance with Title 1, which requires all the same certification steps for the introduction of new software, regardless of whether it is vendor-recommended or Secretary of State-approved, as are required for a new system (testing for compliance w/Federal 2002 VSS standards, written approval by Secretary of State after review, etc). Furthermore, the "Department of State" cannot approve either a new voting system or a modification; only the Secretary or her Deputy may.

With respect to Rule 20.5.3(F) the Secretary of State again displays either ignorance or willful disregard for the threats posed to computer systems, by assuming that any USB device is safe to connect to a voting system; the massive, targeted, sustained campaign of supply chain attack and compromises employed by foreign nation states and the well-documented precedent of introduction of threats and malware into critical systems via counterfeit and modified hardware both indicate clearly that State and County personnel have no ability to discern hardware containing a covert wireless device from hardware without. Furthermore, having certified voting systems for sale and use in Colorado which incorporate as many as several dozen wireless devices per county, the Secretary's apparent knowledge that wireless devices are so risky that they must be prohibited is striking and inexplicable.

With respect to Rule 20.5.4(D) and (E), either the safeguard of two different individuals, with two different party affiliations, is required, or it is not; it makes no sense to require two different individuals with two different party affiliations for non-contract transportation, but to allow only a single individual with unknown party affiliation to transport the same voting equipment under contract.

With respect to Rule 20.5.6(C), the Secretary of State states that counties must preserve all election records on the voting system before reformatting, but the Secretary of State does not meet this same requirement when installing a "Trusted Build" modification to voting systems, wherein she reformats the hard drives of voting system components without ever having preserved the election records explicitly identified in the 2002 Voting System Standards as necessary to meet audit trail requirements.

With respect to Rule 20.6.2, the Secretary of State proposes to restrict the public from observing the conduct of a "Trusted Build" of voting systems, thereby depriving citizens of transparency into a vital election-related process which directly affects the exercise and preservation of their rights. There is no statutory authority for the Secretary of State to restrict public access, and her claim to do so under the umbrella of "security" is hollow and baseless. The General Assembly in Colorado has no authority except that delegated from the People. The Secretary has no authority except that provided by legislation passed by the General Assembly in accordance with their obligation under Colorado's Constitution to pass legislation to secure the purity of elections and safeguard the elective franchise. Depriving the People of transparency into their own election processes does neither, and asserts an absolute authority to the Secretary when, in fact, her authority is highly circumscribed and singular in its purpose.

With respect to Rule 20.6.3(B), the Secretary proposes that county clerks must ensure a trusted build is conducted under video surveillance, and also that no one may surreptitiously record the trusted build by video or audio; this is inherently self-contradictory, since, if the video surveillance must be maintained as an election record, per (B)(3), it must accessible to the public as a public record. The Secretary of State's rules imply that the Secretary does not believe she can or must trust County Clerks, but she demands that the People trust her. The People have no obligation to trust the Secretary of State and any interpretation of her authority which entails restrictions on the People's right to transparency in their elections must be null and void.

With respect to Rule 20.7.1, it makes no sense whatsoever to "secure" unvoted paper ballots when the Secretary allows use of paper ballots with no discrete security measures, e.g. serialized numbering, which would prevent the introduction of innumerable paper ballots prior to delivery to county election officials. The ballot is sent to UOCAVA voters as a pdf file. The ballot is sent to ballot printers as a pdf file. Anyone can take their own paper ballot and produce from it a pdf file which they may then use to reproduce the ballot.

With respect to Rule 20.8.1, the Secretary of State, by allowing a voting system provider to deliver election database and project programming, exposes certified voting systems to the introduction of uncertified code and malware; this violates and undermines the entire purpose of certification testing and the trusted build, which is to trust the certified post-test configuration, not the vendor which originally provided it to the Voting System Testing Lab.

With respect to Rule 20.8.2, the acceptance testing procedures prescribed by the Secretary of State are grossly inadequate to identify security compromises in the equipment and are thus the façade of security without the substance – they can only provide, at best, false assurance.

With respect to Rule 20.9.1, the Secretary's prescription of outdated and insecure WPA2 wireless network security, and shared wireless passwords, and mixed number/case letters password requirements all reflect a lack of knowledge of both cyber threats and best practices for mitigation; they are inadequate to secure SCORE.

With respect to Rule 20.10, the Secretary continues to assert, implicitly, that an Election Project is an adequate backup of all voting system election records required for preservation under Federal and State statute; it is not. It does not encompass all log files and other artifacts identified in the 2002 Voting System Standards as required for the audit trail of election conduct on the computer-based voting systems, not only because it does not include all required EMS server log files, but because it does not include all log files from thousands of other computers

used in Colorado voting systems. The Secretary's rules prohibit and restrict County Clerks from preserving all required election records from their voting systems and thereby illegally interfere with those County Clerks,' election officials in their own right and by the Federal statutory definition, discharge of their duties. In doing so, the Secretary violates the civil rights of Colorado citizens, who are entitled to free and fair elections, the safeguards that ensure them, and the transparency to verify all of it for themselves.

With respect to Rule 20.10.2(B), the Secretary explicitly states election records the county must preserve does not include "logs generated outside of the election management system software;" her exclusion of those logs, in fact, her failure to explicitly require preservation of those logs, violates both Federal and State statute, because the 2002 Voting System Standards are explicit in requiring the operating system logs from voting systems (including but not limited to the election management system) and in their purpose to provide the audit trail information described in the Department of Justice's 2021 Federal Law Constraints on Post Election Audits.

With respect to Rule 20.10.3, again, the Secretary restricts the ability of County Clerks to create images of their voting systems and provides not only no other mechanism for preservation of the election records on their voting systems, but explicitly prohibits them from preserving required election records, in violation of Federal and State statute.

With respect to Rule 20.12.2(3), the Secretary's proposed mandate that a county must cooperate, including providing any documentation or answers requested by the Department during the course of the Department's investigation, is overly broad and ambiguous. The county must, obviously, provide any documentation or answers to which the Secretary is entitled in accordance with her statutory authority circumscribed by the stated legislative and Constitution purpose of that legislation, but not any other. The Secretary has already previously demonstrated herself a poor, ignorant judge of the limits of her own authority and entitlement, and she cannot be trusted in this respect. In particular, the Deputy Secretary of State has already verbally confirmed, according the Mesa County District Attorney, his knowledge that the Department's investigatory powers are administrative and not criminal. Nor are they plenipotentiary. Any request for documentation or answers by the Department is circumscribed by the Secretary's authorities according to the General Assembly, and the General Assembly's authorities are circumscribed by the Colorado Constitution, which is clear regarding the retention of sovereignty by the People of Colorado.

With respect to Rule 21.11.6, the Secretary of State has authorized the violation of CRS 1-7-309 by certifying a voting system which allows adjudication of or refers ballots for scrutiny or election judge adjudication of overvotes. The only permissible adjudication of an overvote is "no vote." Furthermore, by allowing the voting system itself to determine which ballots must be referred for adjudication by election judges, the Secretary has in fact allowed the voting system itself to decide whether ballots must be adjudicated. The recent Mesa Forensic Report #3 documented an instance where the same ballot records were adjudicated differently by the same voting system; one instance is enough to know that it is possible and that it cannot possibly ensure equal protection of Colorado voters' civil rights.