www.nomorenincompoops.com

No More Nincompoops, IEC
David.Blake@nomorenincompoops.com

(202) 255-9668

MEMORANDUM

TO: The People of Colorado

FROM: No More Nincompoops

DATE: May 11, 2026

RE: The BIOS Password Scandal and Jena Griswold's Candidacy for Colorado Attorney General — A Review of the Public Record

I) Introduction

This memo is designed to answer critical questions when considering whether Jena Griswold is fit to be Colorado's next Attorney General. Surprisingly, we actually know very little about this candidate despite nearly eight (8) years in public office and the numerous deleterious headlines she has garnered as the elected Secretary of State. Griswold is either polarizing mostly for one thing – she doesn't much care for Donald Trump. Lest we forget, Jena Griswold was first elected in 2018, as part of the mid-term "Blue Wave" backlash election during Trump's first administration.[1] In her first four years, she repeatedly took credit for others' good work, including claiming title to arguably the premier election infrastructure in the country, and enjoyed zero budget issues,[2] Departmental reputation for quality staff, respect from county clerks and high public confidence. Griswold has harnessed growing anti-

[1] Griswold beat Republican incumbent Wayne Williams in 2018 despite being relatively unknown in 2017, lacking the endorsement of the Denver Post (an endorsement she has never received; The Denver Post endorsed her opponent, Pam Anderson, in 2022) or any major newspaper, and having exceedingly little experience in government or as an attorney, let alone managing elections. The Colorado Springs Gazette called her a partisan hack. See Editorial, Colorado Secretary of State Jena Griswold Goes Off the Rails, Colo. Springs Gazette (May 20, 2019), https://www.coloradopolitics.com/2019/05/20/the-colorado-springs-gazette-colorado-secretary-of-state-jena-griswold-goes-off-the-rails-542fab2e-7b41-11e9-b303-6bd6439054aa; Jennifer Brown, Why Are So Many People Riled Up by Jena Griswold?, Colo. Sun (Oct. 19, 2020), https://coloradosun.com/2020/10/19/elections-chief-jena-griswold-fighting-trump/

[2] Upon taking over the Department of State, the agency's total funds for FY 2018-19 were entirely cash funded at $25,375,937. In FY2025-26, the total funds budget had ballooned to $48,963,071, an increase of 93%!

Trump sentiment both within Colorado and built a brand across the nation through seemingly endless hits on CNN, PBS, MSNBC and through other speaking/media opportunities.[3] Especially after the 2020 election of Joe Biden, the melee at the Capitol on January 6 and fears and allegations – justified or not – about election integrity, Griswold took every opportunity presented to her to publicly harangue Trump, including capitalizing on the media frenzy around the attempt to remove him from the Colorado ballot in 2024.[4] She doubled down on strained relationships with County clerks,[5] including referring Mesa County Clerk Tina Peters for criminal investigation[6] to prosecutors and – with the full support of the Attorney General – civilly suing two other Republican clerks.[7] Despite her nascent beginning, Griswold – who never fails to remind anyone listening that she was the youngest Secretary of State in Colorado history – has unquestionably achieved one thing: she has become a career politico, consistently seeking power complete with aspirations for higher office and sharp elbows.

(Facebook, June 2021)

And, despite the laundry list of policy pronouncements that have aged poorly, the clear lack of principles (beyond herself), there is still one controversy that really did stick to "Teflon Jena": the leak of election equipment passwords during a Presidential election.

---

[3] *David A. Graham, The Fallout of Trump's Colorado Victory, The Atlantic (Mar. 4, 2024),* https://www.theatlantic.com/politics/archive/2024/03/jena-griswold-donald-trump-colorado-primary/677657/

[4] *Sam Levine, Trump Was Wrongly Removed from Colorado Ballot, US Supreme Court Rules, The Guardian (Mar. 4, 2024),* https://www.theguardian.com/us-news/2024/mar/04/trump-scotus-colorado-ruling

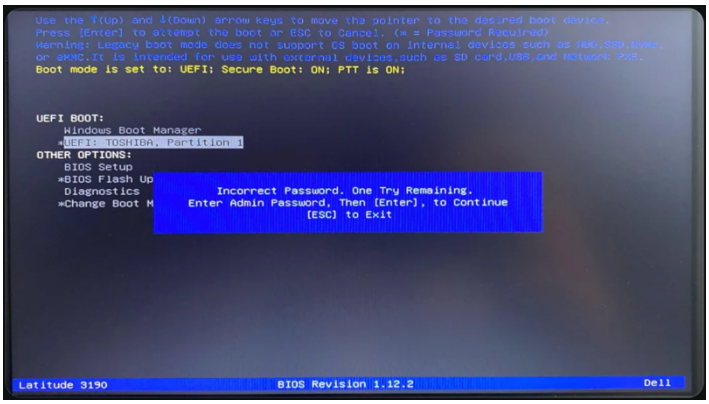
[5] *Bente Birkeland, County Election Officials Say Secretary of State Jena Griswold Is Politicizing Her Office, Risking Trust, Colo. Pub. Radio News (Oct. 9, 2020),* https://www.cpr.org/2020/10/09/jena-griswold-colorado-election-officials/

[6] Press Release, Colo. Sec'y of State, Statement from Secretary Jena Griswold on Indictment of Mesa County Clerk Tina Peters (Mar. 9, 2022), https://www.sos.state.co.us/pubs/newsRoom/pressReleases/2022/PR20220309Indictments.html

[7] Daniel Ducassi, Douglas County Clerk Merlin Klotz Under Investigation by Colorado Secretary of State's Office, Colo. Sun (Feb. 3, 2022), https://coloradosun.com/2022/02/03/merlin-klotz-jena-griswold-investigation/; Jesse Paul, Jena Griswold Wants Answers from Elbert County Clerk on Potential Breach, Colo. Sun (Jan. 24, 2022), https://coloradosun.com/2022/01/24/jena-griswold-dallas-schroeder-election-security/

II) Background

In the summer of 2024, while Secretary Griswold was focused on ensuring more Democratic Secretaries of State were elected in states other than Colorado, non-partisan staff at the Colorado Secretary of State's Office (CDOS) published a "Voting Systems Inventory" spreadsheet on its website as part of routine election equipment documentation. Unbeknownst to officials at the time, the native Excel file contained hidden worksheets with BIOS[8] passwords for voting system equipment associated with forty-six (46) counties.[9] That document remained available and accessible to anyone until just days before the 2024 Presidential election. Subsequent internal reports suggest at least 158 unique IP addresses accessed that information.[10] This breach and inappropriate release of passwords went unrecognized by anyone at CDOS for months because they were not visible in the default view. The formal internal review procedure that should have caught this mistake was deemed a "mere formality" by senior CDOS officials.[11] The file remained publicly accessible from its posting in June for another 125 days, when CDOS officials were alerted by a election equipment government contractor who had known of the hidden tabs since at least July.[12]



[8] BIOS stands for Basic Input/Output System – this is a computer's basic startup system which controls how the machine boots and interacts with hardware before the operating system loads. It can prevent unauthorized users from changing critical settings—such as boot order, hardware access, and important security features including Wi-Fi or Bluetooth settings. See generally BIOS, Wikipedia, https://en.wikipedia.org/wiki/BIOS (last visited Apr. 30, 2026).

[9] Transcript of Hearing on Motion for Preliminary Injunction at 90, Libertarian Party of Colo. v. Griswold, No. 24CV33363 (Colo. Dist. Ct. Nov. 4, 2024), https://archive.org/details/libertarian-party-v-griswold-24cv33363-hearing-transcript-2024-11-04.

[10] Note to File from Cory Brodzinski, Sr. Crim. Investigator, Denver Dist. Att'y's Off., Re: Suspect Employee 5; Case No. D0162024TM000329; Lead Charge: CRS 1-13-708(2) Knowingly Causing Voting System Passwords to be Published 7 (Dec. 17, 2024), https://www.denverda.org/wp-content/uploads/news-release/2024/Password-Investigation-Report.pdf [hereinafter Denver DA Report].

[11] Letter from Beth Doherty Quinn, Baird Quinn LLC, to Chris Beall, Deputy Sec'y of State, Colo. Dep't of State, Re: External Investigation Regarding BIOS Password Disclosure 14 (Dec. 8, 2024), https://archive.org/details/cdos-baird-quinn-report-exhibits-a-b-2024 [hereinafter Baird Quinn Report].

[12] Denver DA Report, supra note 10, at 22.

And, upon learning about the unauthorized release of 655 passwords for election components during voting, we have exactly no idea what the Secretary of State did. If asked today, Griswold's supporters and Democrats generally point to two investigations as definitive proof this debacle is over. Yet, oddly, **Jena Griswold is never mentioned in either report**. Not once. Despite two investigations – one criminal, conducted by the Denver District Attorney's Office, and a second, "independent" review, conducted by a lawyer chosen by and paid by CDOS (after first choosing a different firm that withdrew because of political conflicts) – the Secretary of State's actions in the immediate wake of October 24 until at least October 29 are never discussed! So, while election equipment contractors Dominion Voting Systems and Clear Ballot Group alerted each other to the breach – concerned enough to involve the Dominion voting CEO himself – and they contemporaneously alerted senior staff including the then Deputy Secretary of State, the Elections Director, and the IT Director, there is *no* record of when Jena Griswold was briefed, her reaction, her immediate response or her directives to staff to cure, notice or mitigate the then unknown damage. What we do know is CDOS staff called the Federal government, removed the document from the website and stayed silent for at least five more days.[13] We have absolutely no insight into what the Secretary of State was doing during those five days.

On October 29, apparently having been tipped off about the investigation happening behind closed doors at CDOS, the Colorado Republican Party[14] – complete with an affidavit of a yet another non-government person who accessed the passwords – alerted the public. This is the first time anyone beyond the Secretary Griswold's inner circle learned of the controversy. The Colorado county clerks were understandably irate; they were after all in the middle of administering the 2024 election,[15] receiving and counting mail-in ballots and preparing for the November 5th in-person voting day spike. In fact, on October 29, the Secretary issued a press release touting that "1,271,157 ballots have been returned statewide."[16] Then, Secretary of State Griswold, after what presumably must have been 5 days of intense crisis management appeared on 9News with anchor Kyle Clark only to give what, even supporters

[13] There is no indication that anyone but Griswold made this determination. For example, CISA advice – to disclose or not – has never been shared with the public or investigators (they claim the response was beyond their scope) and other than having communications with Clear Ballot and Dominion, there seems to be nobody else consulted.

[14] Letter from Colo. Republican Party to Colo. Sec'y of State Jena Griswold (Oct. 29, 2024) (with accompanying affidavit re BIOS password disclosure), https://archive.org/details/republican-party-bios-email-ltr-aff.

[15] For the 2024 Colorado General Election, early *in-person* and mail voting in Colorado began 15 days before Election Day — which means October 21, 2024 for the November 5, 2024 general election.

[16] Press Release, Colo. Sec'y of State, General Election Ballots Returned: October 29, 2024 (Oct. 29, 2024), https://www.sos.state.co.us/pubs/newsRoom/pressReleases/2024/2024GeneralElectionBallotReturnReporting7dayso ut.pdf (reporting 1,271,157 total ballots returned as of 11:59 PM on October 28, 2024).

acknowledge, was an underwhelming interview performance.[17] It did not get better for the Secretary or her team as they limped through a now rushed but obligatory curing process (only made possible by support from Governor Polis, Colorado's Office of Information Technology and the Colorado Bureau of Investigation[18]) on the eve of the eventual reelection of Donald Trump for a second term.[19]

III) Leadership Failures and Administrative Anomalies

After almost two years, and two investigations, there remains almost no information regarding Secretary Jena Griswold's direct handling of the 2024 BIOS password leak incident. A complete review[20] is warranted outside the pressures of the then-looming 2024 presidential election, the intense public scrutiny that followed the disclosure of the breach, and with a new lens: whether Jena Griswold possesses and exercises good judgment and the legal acumen to be Colorado's next Attorney General. The conclusion is obvious to anyone not willfully ignoring the evidence. Jena Griswold is a poor manager,[21] comfortable

---

[17] Interview by Kyle Clark, Secretary of State Jena Griswold Discusses Voting System Password Leak, 9News (Oct. 29, 2024), https://www.youtube.com/watch?v=NLi-0WI-f7M. Griswold declined a separate interview request from CBS Colorado. See Shaun Boyd, Colorado Republicans Critical of Secretary of State After Voting System Passwords Posted Online, CBS Colo. (Oct. 30, 2024), https://www.cbsnews.com/colorado/news/colorado-republicans-critical-of-secretary-of-state-after-voting-system-passwords-posted-online/.

[18] Press Release, Off. of the Governor, State of Colo., Gov. Polis and Secretary of State Griswold Announce Additional State Resources are Being Deployed to Ensure Election Security (Oct. 31, 2024), https://governorsoffice.colorado.gov/governor/news/gov-polis-and-secretary-state-griswold-announce-additional-state-resources-are-being-deployed.

[19] That was followed by a confirmed criminal investigation of her office, and utterly reasonable concerns about her credibility. While numerous calls and complaints had been voiced, and pressure had been building for several days to criminally investigate the unauthorized release of the passwords, Griswold's office was formally aware no later than November 4, 2024.

[20] A comprehensive review is not possible because the Secretary has been unwilling to make relevant information available for public review and consideration. Indeed, her office recently quoted a fee of $34,978.34 to give No More Nincompoops. access under a Colorado Open Records Act request of her calendar. All told, the Secretary has sought or collected at least $75,000 in fees in 2026 to comply with citizen's public records requests.

[21] See Jimmy Sengenberger, Griswold Pays Six Figures on Discrimination Claim, Denv. Gazette (Apr. 12, 2024), https://www.denvergazette.com/2024/04/12/griswold-pays-six-figures-on-discrimination-claim-jimmy-sengenberger/ (reporting that Abbas Montoya, a Hispanic career staffer with a decade-long tenure, filed a July 2022 grievance after being passed over for deputy director of business and licensing, and detailing the broader pattern of staff turnover under Secretary Griswold); Jimmy Sengenberger, Hard to Justify Muzzling of Ex-Public Employees, Colo. Springs Gazette (Apr. 19, 2024), https://gazette.com/2024/04/19/hard-to-justify-muzzling-of-ex-public-employees-jimmy-sengenberger/ (reporting that the Secretary of State's office paid Montoya a $120,000 settlement in August 2023 and that Montoya left the office in October 2023).

contorting the truth,[22] and a competence-adjacent lawyer motivated by self-interest.[23] She calls herself a fighter but sidesteps any arena where she might take a hit,[24] insisting on accountability for others while evading it herself. The BIOS password fiasco lays it bare.

---

[22] See Marshall Zelinger, Griswold Falsely Claims She Argued Before the Supreme Court, 9News (Mar. 2, 2026), https://www.9news.com/article/news/local/local-politics/griswold-falsely-claims-supreme-court/73-57a75ab3-5733-4b6f-8753-67565dab1ff0 (reporting that Secretary Griswold repeatedly claimed in campaign materials, fundraising emails, and a March 2, 2026 appearance before the Longmont Area Democrats that she "argued at the Supreme Court that Donald Trump should not be eligible for President," and confirming that the case in question, Trump v. Anderson, was actually argued by Colorado Solicitor General Shannon Stevenson on briefs filed by Attorney General Phil Weiser's office; 9News legal analyst Scott Robinson characterized Griswold's claim as "inaccurate and, quite frankly, a misrepresentation"); see also Sandra Fish, Colorado's AG Race Pivots on Legal Experience and a Candidate's Misleading Claims, Axios Denver (Mar. 10, 2026), https://www.axios.com/local/denver/2026/03/10/colorado-attorney-general-ag-2026-democrats-jena-griswold (Griswold campaign acknowledging she "did not personally argue the case").

[23] Secretary Griswold has repeatedly sought higher office before her current bid for Attorney General. See Ernest Luning, Democrat Jena Griswold Exploring US Senate Bid Against Cory Gardner, Colo. Pol. (July 16, 2019), https://www.coloradopolitics.com/2019/07/16/democrat-jena-griswold-exploring-us-senate-bid-against-cory-gardner-fce5aa1e-a776-11e9-9704-1386a278907c/ (reporting that, less than seven months after taking office as Secretary of State, Griswold formed a federal exploratory committee to consider a 2020 U.S. Senate run against Senator Cory Gardner after meeting with Senate Minority Leader Chuck Schumer); Jesse Paul, Jena Griswold Says She Won't Launch a Primary Bid to Unseat Republican Cory Gardner, Colo. Sun (Aug. 9, 2019), https://coloradosun.com/2019/08/09/jena-griswold-wont-run-for-senate/ (reporting that Griswold's exploratory committee raised over $200,000 in two weeks before she declined to run amid criticism over leaving her office so soon). More recently, see Marianne Goodland, Campaign Finance Complaint Filed Against Colorado Secretary of State Jena Griswold, Denv. Gazette (Jan. 22, 2025), https://www.denvergazette.com/2025/01/22/campaign-finance-complaint-filed-against-colorado-secretary-of-state-jena-griswold-23d0beeb-3a65-585b-997b-5762dc5b8c4a/ (detailing that the domain jenaforgovernor.com was purchased on August 8, 2024, with a "Jena for Governor" placeholder page declaring "Launching Soon" and collecting supporter emails, and that the site was scrubbed only after 9News' December 20, 2024 report exposed it); Marianne Goodland, Campaign Finance Complaint Against Colorado Secretary of State Jena Griswold to Be Dismissed, Colo. Springs Gazette (Apr. 14, 2025), https://gazette.com/2025/04/14/campaign-finance-complaint-against-colorado-secretary-of-state-jena-griswold-to-be-dismissed/ (noting that the investigation — conducted by the Office of the Attorney General to avoid conflict of interest — was dismissed for insufficient evidence after the Secretary's brother and campaign manager, Chris Griswold, accepted responsibility for purchasing the domain, and that Griswold ultimately announced her candidacy for Attorney General rather than Governor).

[24] See Thelma Grimes, 'The People's Lawyer Should Show Up,' Democratic AG Candidates Say as Griswold Misses Forum, Colo. Pol. (Jan. 22, 2026), https://www.coloradopolitics.com/2026/01/22/the-peoples-lawyer-should-show-up-democratic-ag-candidates-say-as-griswold-misses-forum/ (reporting that Secretary Griswold did not attend a Denver Press Club attorney general candidate forum despite being invited and contacted multiple times by the organizer; opponents Hetal Doshi, Michael Dougherty, and David Seligman — all of whom attended — said her absence was "disappointing" and "telling," with Dougherty observing that "if you're going to be the people's lawyer, then you show up and answer the people's questions"); John Frank, Jena Griswold, Not Trump, Is Targeted in Colorado's Democratic Attorney General Race, Axios Denver (Jan. 23, 2026), https://www.axios.com/local/denver/2026/01/23/jena-griswold-colorado-democratic-attorney-general-race-2026; Allison Sherry, Attorney General Race Heats Up for Democrats, Just in Time for Weekend Assembly, Colo. Pub. Radio (Mar. 27, 2026), https://www.cpr.org/2026/03/27/colorado-democrats-attorney-general-candidates-2026/ (reporting that, while Doshi, Dougherty, and Seligman "kept bumping into each other in various locations in the San Luis Valley, the eastern plains, the western slope and the Denver metro in search of primary voters," Griswold instead "relied mostly on national television hits and social media" — a pattern Griswold dismissed as her opponents "ganging up" on her).

1) **Materially Misleading Statements** – Proving the maxim "it is better to remain silent at the risk of being thought a fool than to talk and remove all doubt,[25]" on October 29, 2024, Secretary of State Jena Griswold agreed to be interviewed on Kyle Clark's show *Next* on Colorado's NBC. In part, they had the following exchange:

> Kyle Clark: "Your office is acknowledging that you inadvertently leaked voting system passwords by putting them on your website. The Colorado Republican Party says that this was more than 600 BIOS passwords for voting systems in all but one Colorado county. Is that accurate?
>
> Secretary Griswold: That is not accurate."

According to Secretary Griswold's own timeline, "CDOS completed the identification of the specific voting system components affected by the [BIOS passwords] posting on the morning of October 29th."[26] So, during her interview with Kyle Clark, Secretary Griswold knew or should have known all the information that would ever come out and yet still 1) failed to be forthcoming and 2) did what she could to mislead the public and minimize political fallout. In fact, we know that there were ~650 passwords[27] contained in multiple separate "hidden tabs" that mapped to approximately 255

---

[25] *Maurice Switzer, Mrs. Goose, Her Book (1907).*

[26] Colo. Dep't of State, Fact Sheet: 2024 General Election (Dec. 8, 2024), https://www.sos.state.co.us/pubs/newsRoom/pressReleases/2024/20241208CDOSFactSheetOnPasswordDisclosure.pdf (it is unclear how the document is released on December 8, 2024, dated December 9, 2024, but contains information dated December 20, 2024).

[27] Press Release, Denver Dist. Att'y's Off., Denver DA Announces Decision in Voting Machine Password Case (Dec. 20, 2024), https://www.denverda.org/news-release/denver-da-announces-decision-in-voting-machine-password-case/ (attaching Denver DA Report, supra note 10)

https://www.denverda.org/wp-content/uploads/news-release/2024/Password-Investigation-Report.pdf

machines used in various counties.[28] Passwords (some that were outdated) registered to forty-six (46) counties, including 12 counties where the machines were not in use, leaving thirty-four (34) counties whose valid BIOS passwords correlated with voting equipment in active use.[29]

Secretary Griswold continued to deflect and obfuscate during the interview rather than be transparent or forthcoming. When asked by Clark how many passwords, she ignored the question stating instead:

> "the spreadsheet located on the department website improperly had a hidden tab with partial passwords . . . This is not the full password to access voting equipment . . . we had started an investigation – actually have people in the field – that have been working on this issue . . . ."

Again, not true, and a poor attempt to minimize. We know the Excel document had *four* hidden tabs, not one.[30] There was no CDOS policy against having hidden tabs and the Excel spreadsheet absolutely had the active and complete BIOS passwords.[31] What the spreadsheet lacked was a *second* password for the operating system (and system login ID) that would grant a user full access to the *software* suite. Griswold also suggested as part of her investigation she put people "in the field." But under oath, Deputy Secretary of State Beall told the Denver District Court that the teams "in the field" on October 29th "conducting regular visits to counties".[32] Here again, Secretary Griswold attempted to mislead the public and create the impression she responded dutifully, when in fact it appears she did exceedingly little.

Also critical is to note that "dual control" passwords was not really central to Clark's question for the reasonable concerns of the clerks and public. Even CDOS "Former Employee #1" described that with just the BIOS password and physical access to the equipment:

---

[28] The list of affected counties was known on October 29, and it was even provided to the Denver District Attorney as part of their investigation, but the list has never been made public by the Secretary. See Denver DA Report, supra note 10, at 14.

[29] Transcript of Hearing on Motion for Preliminary Injunction at 90, Libertarian Party of Colo. v. Griswold, No. 24CV33363 (Colo. Dist. Ct. Nov. 4, 2024), https://archive.org/details/libertarian-party-v-griswold-24cv33363-hearing-transcript-2024-11-04.

[30] Id. at 29.

[31] BIOS passwords matter because they unlock the BIOS environment and, combined with physical access to a machine, would expose hardware-level functionality.

[32] Transcript of Hearing on Motion for Preliminary Injunction at 78, Libertarian Party of Colo. v. Griswold, No. 24CV33363 (Colo. Dist. Ct. Nov. 4, 2024), https://archive.org/details/libertarian-party-v-griswold-24cv33363-hearing-transcript-2024-11-04.

> "[Former Employee 1] described the publication of these BIOS passwords as a serious cybersecurity issue and explained [to the DA investigator] that one would not necessarily need a system login to a device to use the BIOS passwords [explaining] that when a Windows-based machine is booting, there is an opportunity to enter the BIOS before Windows has completely loaded. Thus, a change could be made to the machine with the BIOS password, even without a local user login . . . functions such as the ability to boot from a USB drive or turn on/off networking functionality could all be managed within the BIOS."[33]

At a minimum, Griswold's minimizing statement was a mistake. At worst, she was lying.

Kyle Clark must have realized something was off, and next asked for clarification about a "partial password," stating:

> Kyle Clark: "When you say partial passwords, do you mean that it had one of the two passwords required to get into the system or it did not even have one full password?"
>
> Jena Griswold: "It had one of two. And not for all voting components, for some voting components in the state."
>
> Kyle Clark: "How many counties?"
>
> Jena Griswold: "Uhh, at this point Kyle, umm, we have staff in the field, uh, looking at the situation, uh, but we will disclose after they're out of the field. Umm, to be very clear, we do not see this as a full security threat to the state. This is not a security threat…"

Griswold's obfuscation and misstatements about the BIOS password release continue for several more minutes, and then days, weeks, months and remains ongoing today. Only after being pressed by Clark did she acknowledge there were two distinct sets of passwords.[34] Of course, she fails to mention (or perhaps to comprehend) that if one set of passwords are publicly available on the internet then they are universally available

[33] Denver DA Report, supra note 10, at 24.

[34] This was not a slip of the tongue. The "partial passwords" mirage was used in a press release from the Secretary's office released earlier in the day on October 29. See infra note 35. In fact, her talking point was always that a spreadsheet located on the Department's website improperly included a hidden tab including partial passwords to certain components of Colorado voting systems. The claim just did not hold up to any scrutiny.

anywhere there is a cell or Wi-Fi signal. That is, the compromised set of passwords are by default collocated with the second set, thereby defeating this security measure entirely. The layers of security facade – at least this layer – was always a red-herring. To be sure, it is a legitimate security procedure to keep two passwords (or sets) physically separated or, as the CDOS *told* the public: that these passwords "are kept in separate places and held by different parties."[35] But they were not kept separate, they were published to the world. It is nonsense to assert that credential separation is still a viable security layer after the BIOS passwords were posted to the internet for months. That security layer is pierced if the first party posts their "key" on the internet effectively empowering the second party to have the "master combo key" accessible anywhere the internet also exists.[36]

DHS/CISA[37] and leading cybersecurity experts warn of BIOS password leaks chiefly because they create the opportunity for unauthorized access to firmware and boot-level systems, which in turn enable something called an "evil maid" attack.[38] An evil maid attack involves someone with physical access who installs persistent malware or alters system behavior before the operating system loads, undermining secure boot and other defenses.[39] A leaked BIOS password reasonably

[35] Press Release, Colo. Sec'y of State, Secretary Griswold Statement on Voting System Passwords (Oct. 29, 2024), https://www.sos.state.co.us/pubs/newsRoom/pressReleases/2024/PR20241029Passwords.html.

[36] This is akin to a bank employee handing the vault key to anyone who walks in and asks.

[37] It has been stated that CDOS staff called CISA on October 24, 2024, but the Secretary has never disclosed what CISA advised or how CISA supported CDOS in its mitigation efforts (especially during the five (5) days that the Secretary didn't tell anyone else about the security violation). According to the CDOS Fact Sheet, "CDOS consulted with the U.S. Department of Homeland Security's Cybersecurity and Infrastructure Security Agency, as well as Dominion Voting Systems" but there is no indication they agreed with the Secretary's conclusion and public assertion that there was "no security threat." See Colo. Dep't of State, Fact Sheet on Password Disclosure (Dec. 8, 2024), https://www.sos.state.co.us/pubs/newsRoom/pressReleases/2024/20241208CDOSFactSheetOnPasswordDisclosure.pdf [hereinafter CDOS Fact Sheet].

[38] Cybersecurity & Infrastructure Sec. Agency, U.S. Dep't of Homeland Sec., Insider Threats 101: What You Need To Know (July 29, 2024), https://www.cisa.gov/sites/default/files/2024-07/insider-threat-101-fact-sheet_07-29-2024_508.pdf; Cybersecurity & Infrastructure Sec. Agency, U.S. Dep't of Homeland Sec., Election Infrastructure Insider Threat Mitigation Guide, https://www.cisa.gov/resources-tools/resources/election-infrastructure-insider-threat-mitigation-guide.

[39] This is exactly what Former Employee 1 warned the DA's investigator about during her interview. There is also concern that such a persistent malware could exist even after a "trusted build" occurred. See Denver DA Report, supra note 10, at 24.

raises this concern because it lowers the barrier to firmware-level tampering, making it easier for an insider or intruder to compromise a machine in ways that are difficult to detect, remove, or fully remediate. In turn, this makes the physical access logs critically important to fully assessing the actual risk. And, on October 29 it would not have been possible for Jena Griswold or her staff to make an informed assessment as they had not yet alerted the Clerks, let alone done the work necessary to review those voting machine logs. Auditing the access logs was not completed until November 1st, at the earliest,[40] after Governor Polis stepped in with the backing of the Office of Information Technology and the Colorado Bureau of Investigation. This is the absolute earliest moment anyone could have determined the BIOS password release was not a worst-case scenario event. Griswold's security threat assessment was negligently made without adequate knowledge or diligence.

Griswold's attempt to minimize the leak's scope was equally untenable. Her insistence that the exposed passwords covered "only some components" of the State's voting systems was, on its own terms, no defense: as Clark reminded her, the State's own rule — in force in both 2021 and 2024 — provides that the "public disclosure of the BIOS passwords for one or more components [of the State's] voting system alone constitutes a serious breach of voting system security protocols, as well as a violation of Election Rule 20.6.1".[41] In 2021, Griswold had tried to blunt criticism of an earlier leak by asserting that no "imminent direct security risk to Colorado's elections" existed because that leak did not occur during an election. That safe harbor was unavailable in October 2024: this breach spanned the 2024 primary and was disclosed only eight days before the presidential election. Worse, a 2022 statute Griswold herself championed,[42] had since made the knowing release of this data a felony. The relevant exposure window, moreover, was not the few weeks before Election Day but the entire period from June 24, 2024, when the spreadsheet was first published, through its removal in late October. During that window, Griswold's office administered a mandatory recount in the Republican primary for House District 58, decided by three (3) votes[43] and two

---

[40] Press Release, Colo. Sec'y of State, Governor Polis, Secretary of State Griswold Announce All Passwords Have Been Updated (Nov. 1, 2024), https://cdn.colorado.gov/governor/news/governor-polis-secretary-state-griswold-announce-all-passwords-have-been-updated-colorado.

[41] Press Release, Colo. Sec'y of State, Colorado Secretary of State Decertifies Mesa County Voting Equipment (Aug. 9, 2021), https://www.sos.state.co.us/pubs/newsRoom/pressReleases/2021/PR20210809MesaCounty.html.

[42] Press Release, Colo. Sec'y of State, Secretary Griswold Applauds Bipartisan Passage of the Colorado Election Security Act (May 10, 2022), https://www.sos.state.co.us/pubs/newsRoom/pressReleases/2022/PR20220510ElectionSecurity.html (announcing passage of SB22-153, which created a felony for "knowingly publishing voting system passwords online").

[43] Election Order 2024-02, Colo. Sec'y of State, Recount of State House Representative District 58 Republican Primary (July 15, 2024),

further mandatory recounts in the general election — in House District 16, also decided by three (3) votes, and House District 19, decided by 110.[44] The compromise of even a single tabulator in any of those districts could have changed the outcome, and at the time of her interview neither Griswold nor anyone else could rule that possibility out.[45] Characterizing a BIOS-password disclosure of any scale as anything less than serious was, on this record, a dereliction of duty.[46]

Secretary Griswold's half-truths continued throughout the interview that evening. A close examination of her words reveals she claimed:

- CDOS was "working with our federal partners" (stated four times in varying ways), but no documents or details have ever been revealed about what "work" was done during the 5-day delay before the public learned of the breach. CISA was apparently not involved in the operation to examine and update compromised election equipment on October 30 & 31, all public statements about that operation exclude anyone but State employees.

- CDOS alerted Dominion Voting (and Clear Ballot was already aware) of the breach but there have been no details about why or what role these government contractors played early on during the crisis response, or to cure the problem. It was confirmed that only background checked government employees operating in pairs, with local official oversight, were involved with

---

https://www.coloradosos.gov/pubs/newsRoom/pressReleases/2024/20240715ElectionOrder.pdf (Suckla 6,488 votes; Roeber 6,485 votes).

[44] Press Release, Colo. Sec'y of State, Secretary Griswold Confirms Mandatory Recounts in House District 16 and House District 19 (Dec. 5, 2024), https://www.sos.state.co.us/pubs/newsRoom/pressReleases/2024/PR20241205Recounts.html.

[45] Also recall that the three (3) votes tipping the win to Republican Rebecca Keltie over incumbent Democrat Stephanie Vigil robbed Democrats of the supermajority in the Colorado House. See Bente Birkeland, State House District 16 Race in Colorado Springs Officially Decided by Three Votes After Recount, Colo. Pub. Radio (Dec. 5, 2024), https://www.cpr.org/2024/12/05/republican-rebecca-keltie-wins-close-state-house-district-16-race/.

[46] It could be credibly argued that Griswold's statement violated C.R.S. § 18-8-404(1)(a), Official Misconduct, which provides that a public servant commits official misconduct if she knowingly refrains from performing a duty imposed by law — here, analogous to Tina Peters' prosecution, Griswold knowingly violated her statutory duties to safeguard election systems and the truthful administration of elections by allowing the unauthorized release of secure voting system information and deceiving other public servants and officials about the extent of risk and the appropriate response. We will likely never know: the Democratic District Attorney limited the scope of her investigation to charging CDOS Employee 5 with a violation of C.R.S. § 1-13-708(2) (Knowingly Causing Voting System Passwords to Be Published); no investigation of Jena Griswold or any other government official has ever been acknowledged.

the password updates.[47] Thus, we can logically conclude contractor support was not necessary to resolve the breach. So why was the Dominion CEO John Poulos one of the first calls made after the revelation on October 24? This has never been explained.[48] Jena omitted this detail from her answers to Kyle Clark.

- Griswold repeatedly couched her post-leak investigation as including "people in the field" and as only being necessary "out of an abundance of caution" (she asserted this four different times). Putting aside that these platitudes create confusion (and as pointed above, is contradicted by sworn testimony of her deputy), the statement is unsupported by any documentary or oral evidence and creates an obvious logic gap. If she had her people "in the field" for the preceding 5-days as was suggested, then she would have needed to alert the Clerks (or at least some of them) to get access to the election equipment (assuming it was secured and monitored). But no Colorado Clerk has ever corroborated such a timeline. Hypothetically, even if she was working with one or two clerks "in the field," the risk-assessment's footprint involved more than 30 counties across Colorado. In this instance, Griswold is either guilty of hiding this information from the Clerks or she is guilty of having a woefully inadequate response to the urgency of the problem her office created. Or both.

- The Secretary's claim that the response was "out of an abundance of caution" is equally absurd. Again, this is either evidence of supremely poor judgment, or she lied to the public. If caution was her motivation, why would she "request" Governor Polis activate SEOC[49] the next day and provide the resources to do in 36 hours what she had deemed unnecessary for at least 5 days? Polis apparently learned of the debacle at the same time as everyone else, on October 29, and was concerned enough to be briefed the next morning by the Colorado Department of Public Safety (CDPS), and then by Secretary Griswold herself on the afternoon of the 30th. Polis apparently threw caution to the wind; he activated SEOC, decided it was "necessary passwords [be]

[47] Press Release, Polis & Griswold, supra note 18.

[48] It is possible the Dominion CEO was called for legal, liability, or public-relations coordination rather than technical support — but shouldn't the public know that? And if any of those are legitimate reasons to make the call, why wouldn't the same logic apply to the Governor, the elected County Clerks, and others?

[49] The State Emergency Operations Center (SEOC) is Colorado's centralized, multi-agency coordination center, run through the Division of Homeland Security and Emergency Management at CDPS, and is activated during major incidents, disasters, or credible security threats.

changed as quickly as possible" and showered the Secretary with the resources (including helicopters) to address the problem. Within 24 hours every affected voting machine across the State had been assigned new BIOS passwords. This was a massive operation and the proper reaction commensurate to the threat Griswold created and then neglected for days.

- Griswold fibbed again, or perhaps just over-lawyered, her response to Clark's question about her intent to inform the Clerks before the Republican Party email forced her hand. Her answer: "We did not decide not to disclose something to county clerks." What is something? And when? If the leak was not a security threat, and the investigation was purely out of an abundance of caution, then the obvious conclusion is she would *not* tell the clerks. That approach, as offensive as it is, is exactly what was contemporaneously relayed to Adams County Clerk Josh Zygielbaum (and an unknown number of other clerks and officials) on an October 31 conference call by then Deputy Secretary of State Chris Beall stating: "We were *not* going to tell counties because we could not tell counties without it becoming the media storm it has become."[50] Media storm or not, the duty of the Secretary was to voluntarily and quickly alert the Clerks of the breach in the same way they felt obligated to alert CISA and Dominion Voting's CEO on October 24.

As Griswold seeks to be the highest law enforcement office in the State, and further attempts to proclaim her legal prowess, perhaps someone should remind her about Colorado Rule of Professional Conduct (RPC) 8.4(c). That rule states: "It is professional misconduct for a lawyer to engage in conduct involving dishonesty, fraud, deceit or misrepresentation. . ." The duty is not limited to just when a lawyer is before a tribunal (RPC 3.3), or representing a client (RPC 4.1), or other situations like being interviewed by law enforcement (which also never happened in this case). RPC 8.4 is an omnipresent obligation. There is a non-rhetorical comparison to Jenna Lynn Ellis; it is a direct parallel of professional accountability. Just as Ellis was sanctioned for misrepresenting the factual outcome of the 2020 election to undermine public confidence, a public official who minimizes a verified security breach misrepresents the state's actual security posture. In both instances, the 'harm' is the same: the lawyer uses their platform and credibility to deceive the public—and by extension, the 'tribunal' of the electorate—into accepting a false narrative about the integrity of

[50] Colorado GOP, Excerpts from SoS Call to County Clerks, YouTube (Oct. 31, 2024), at 1:06, https://www.youtube.com/watch?v=Q55Z9s1By9M&t=58s. It is relevant to note that Secretary Griswold was not even on this call; informing the County Clerks and answering their question was in explicably delegated to the Deputy Secretary.

then ongoing democratic process. Under RPC 8.4(c), a half-truth intended to obscure a material risk is as much a misrepresentation as an outright lie. Jena Griswold has widely criticized Trump's attorneys after the 2020 election and Ellis was publicly censured by the Colorado disciplinary system in March 2023 for those misrepresentations on national television and social media.[51]

2) **Compliance.** The "legal basis" for posting the Voting System Inventory (VSI)[52] appears to have been initially misstated, then weeks later recanted to certain investigating officials but not the public. In initial conversations with DA investigators Deputy SOS Chris Beall asserted CDOS was required "by rule or statute" to post the inventory.[53] Many news stories likewise told the public that the spreadsheet contained information "the state is required to make public, online."[54] The suggestion being it was a legal obligation; this justification appears in many news articles published contemporaneously with the leak. It created an air of inevitability and allowed for the bitter pill to be swallowed. The theme from day one of the controversy was: this was a good faith, low-risk ministerial goof that resulted from a lawful transparency obligation. Like many aspects of the Secretary's response, that is just false. The VSI was never, and is not now, obligated to be made public. To Beall's credit, he corrects the record with the criminal investigator at the end of his investigation.[55] But the Secretary has never sought to correct this misimpression with the public or press.

This is important because:

i) Apparently, Secretary Griswold and staff at CDOS lack command of their actual legal obligations. While voluntary transparency is welcome – especially

[51] Colo. Rules of Pro. Conduct r. 8.4(c). See, e.g., People v. Ellis, No. 23PDJ004 (Colo. Off. Presiding Disciplinary Judge Mar. 8, 2023) (publicly censuring Trump campaign attorney Jenna Ellis for violating Colo. RPC 8.4(c) by making misrepresentations about the 2020 presidential election), available in Disciplinary Case Summaries, Colorado Lawyer, https://cl.cobar.org/news/pdj/.

[52] The Voting System Inventory is the inventory of all voting systems equipment and components used or available for use by Colorado's election officials across the entire state. The elected county clerks are obligated by statute and regulation to report details about election equipment to CDOS. See C.R.S. § 1-7-513.5; 8 CCR 1505-1, Rule 11.

[53] Denver DA Report, supra note 10, at 2 (Nov. 5, 2024 follow-up interview of "Employee 11").

[54] Bente Birkeland & Kiara DeMare, Colorado's Election Equipment Password Breach Explained, Colo. Pub. Radio (Nov. 28, 2024), https://www.cpr.org/2024/11/28/colorado-election-equipment-password-breach-explainer/.

[55] Denver DA Report, supra note 10, at 26 (Dec. 18, 2024 follow-up; Employee 11 "stated he was mistaken when he previously said there was a specific rule" requiring publication of the Voting System Inventory).

from CDOS – to mislead the public during damage control operations by suggesting this information (without the passwords) must be publicized and wrapping oneself in a cloak of compliance is rotten. In fact, the mistaken release of the passwords was an "own goal" by the Secretary, one error compounding another and much less good-faith transparency run amok. It remains unexplained why it was believed to be good public policy for this information to be collated and republished. Or why the CDOS was so keen to get the file reposted (without passwords)? Or maybe it wasn't good policy, because this information no longer appears to be accessible on the website. We have no idea who used (or uses) this information other than government contractors who mine it for marketing opportunities and intel. Has anyone ever done the risk analysis - can be used for nefarious purposes – especially when consolidated and updated on a regular basis? Perhaps it is smart to keep this information dispersed among the counties and not aggregated for the public.[56]

ii) Regardless, we have no insights into how Jena Griswold handled this challenge and what questions she asked – if any – about the history, purpose or need to post this document in a user-friendly format, or .pdf, or not at all.

IV) Careless Adherence to Rules, Regulations, and Policy Workflows

Senior CDOS staff described the leak as being the result of "poor" and "sloppy" adherence to cybersecurity policies or "due to laziness" (see DA Investigative Report). But lax adherence to policy and regulations is a reliable indicator of weak leadership because it signals that standards exist on paper but not in practice, undermining accountability, consistency, and institutional discipline. When leaders tolerate shortcuts, uneven enforcement, or informal workarounds, they communicate that rules are

In this Thursday, Aug. 6, 2015 file photo, people kayak in the Animas River near Durango, Colo., in water colored yellow from a mine-waste spill. A crew supervised by the U.S. Environmental Protection Agency has been blamed for causing the spill while attempting to clean up the area near the abandoned Gold King Mine. (Jerry McBride/The Durango Herald via AP, FILE)

[56] Aggregation may itself be the risk. An aggregated list creates a "one-stop shop" for a bad actor to identify the weakest or oldest software and most prevalent hardware versions across the state — information that would be far harder to gather if a malicious actor had to query 64 individual clerks.

optional, which erodes professionalism, invites risk, and incentivizes complacency rather than excellence. Consider the 2015 Gold King Mine disaster here in Colorado, where slipshod oversight and procedural shortcuts by the U.S. Environmental Protection Agency and its contractors led to the accidental release of more than three million gallons of orange toxic sludge and waste into the Animas River. After action investigations found that basic safety protocols, risk assessments, and engineering reviews were ignored or inadequately followed, reflecting weak management and poor regulatory discipline. Over time, this culture of permissiveness compounds errors, weakens internal controls, and leaves organizations vulnerable to preventable failures, crises, and loss of public trust. That same culture was created by Jena Griswold at the Department of State and can be directly traced to the BIOS password leak.

1) **AUP.** There was no evidence that the CDOS' Acceptable Use Computing Policy (AUP) was ever adhered to by anyone at the agency. The IT Chief provided CYA documents to the Denver DA's office to suggest the policy was clear and well documented by the Department. But the investigator could not even determine what provision of the files really meant. Regardless, both reports note two critical facts: (1) there was no evidence of anyone signing the annually required AUP Acknowledgment form between 2018 and 2024,[57] and (2) the policy had not been significantly modified or updated since at least 2015.

   This is important because:

   i) Jena Griswold was elected in 2018 and sworn in 2019. The reports would therefore suggest nobody in the Department – presumably including Jena Griswold herself – had ever formally acknowledged their core obligations to protect and safeguard secure information under their control during her entire tenure! And she is running to be Colorado's "General Counsel."

   ii) The failure to enforce the AUP is not a personnel-management lapse; it goes to the foundation of any criminal or disciplinary action arising from the leak. An employer cannot prove that an employee acted "knowingly" if it cannot first prove that the employee was on notice of the rule they are said to have

[57] Baird Quinn Report, supra note 11, at 4 n.3 ("In the VS Team personnel files reviewed, there are employee signature pages reflecting receipt and review of the Acceptable Use Policy from 2018. There are no employee signature pages after that date even though a new Acceptable Use Policy issued in 2022."); see also id. at 3–4 (CDOS AUP discussion).

broken.[58] Annual AUP acknowledgment is the State's standard mechanism for establishing that notice, and the record shows it was not collected for six straight years. Neither report draws the connection, but it is the operative one: without documented acknowledgment, the State cannot make the threshold showing of notice that a "knowing" violation requires. The leadership failure is therefore not merely supervisory — it is the proximate reason the conduct underlying the leak is unlikely to be prosecuted.

iii) No chief information security officer in the private sector — in any industry that handles sensitive personal, financial, or election-infrastructure data of the kind CISA designates as critical — would treat annual or biennial review of acceptable-use practices as optional. That is the baseline Secretary Griswold publicly insisted on for county clerks and litigated against the federal government to defend; yet her own office let it lapse for six consecutive years, spanning the 2016 Russian interference campaign, the COVID-era expansion of remote access, and the rapid integration of generative AI into routine workflows.

2) **Password Policy.** According to the CDOS CIO during his interview with the DA's investigator, employees must use secure passwords and that "LastPass or other password management systems is preferred" and it was his determination that "the method in which these BIOS passwords were stored . . . was not an acceptable form of password management." But the Baird Quinn investigation determined that "Elections Division employees interviewed did not understand there to be any type of requirement that BIOS passwords be stored solely in a password safe" indicating that whatever the password policy was, at a minimum CDOS leadership had done a poor job of conveying and enforcing the policy. Further still, the Baird Quinn investigator reported that Griswold's CIO – in contradiction to his prior statements to the Denver DA – "agreed that storing the BIOS passwords in a file on the CDOS server (with its layers of protections) with properly complex password protection is an acceptable alternative to use of the password safe." So if the CIO doesn't know what the policy is, how can leadership expect their staff to know?

This is important because:

[58] Colo. Rev. Stat. § 1-13-708(2) (2024) ("Any person who knowingly publishes or causes to be published passwords or other confidential information relating to a voting system shall immediately have their authorized access revoked and is guilty of a class 5 felony."), as amended by Colorado Election Security Act, ch. 322, sec. 16, 2022 Colo. Sess. Laws 2241, 2256 (codifying SB22-153, eff. June 2, 2022).

i) In response to criticisms, Jena Griswold repeatedly blames staff for failing to follow Departmental password policy. Yet, not even the CIO knew what the policy was and told different investigators at different times different things. It is upsetting that leadership would seek to push staff in front of a bus when they failed over the course of years to issue a clear policy, educate staff on implementation and enforce the policy appropriately. The investigations' contrary conclusions simultaneously undermine their integrity yet prove up the policy dysfunction bred by Griswold.

ii) Also relevant is that password policy was not really, ever, the issue. This was more sleight of hand by Griswold. The critical data was not hacked nor were weak passwords exploited by some dark web computer wizard. They were posted unwittingly by staff with authorized and proper access to this information. CISA defines an "insider threat" as: "the threat that an insider will use their authorized access, wittingly or *unwittingly*, to do harm to the department's mission, resources, personnel, facilities, information, equipment, networks, or systems."[59] And, CISA teaches there are specific types of insider threats, including "negligent" and "accidental." Obviously, good policy guidance and adherence to those policies is designed to defeat these types of threats. But Jena Griswold – despite having harped on insider threats from Clerks for years – apparently didn't know she was the real threat. When asked by Kyle Clark if this was an insider threat, Griswold inexplicably said "no." If she did know – and regardless of whether her staff engaged in negligence or mistake – then her response was a blatant attempt to mislead.

3) **Process Failure.** As the Baird Quinn report reveals, by year six of Jena Griswold's administration, CDOS was truly bureaucratic – in all the worst ways. Most on point is the dismissive approach to posting documents on the web. Indeed, there were lots of processes, rules and regulations applicable to this situation. Nearly one-quarter of the Baird Quinn report simply restates and explains the relevant policies (see pages 3-7) so it can then apply them to the facts. It is a bit ridiculous to expect every government employee to know every rule and regulation across multiple agencies of government until you realize this is exactly what government does to its citizens and businesses everyday when they make a mistake.

This is important because:

[59] Cybersecurity & Infrastructure Sec. Agency, U.S. Dep't of Homeland Sec., Defining Insider Threats, https://www.cisa.gov/topics/physical-security/insider-threat-mitigation/defining-insider-threats.

i) The website posting processing (at least there was a process – this is of course logical) was ineffective, and abused. Directly resulting in the release of the BIOS passwords was Employee 8's approval of the June 21 request to post the Excel spreadsheet. This employee reported he was never trained to be an authorized approver and whenever a request came through, he just clicked OK. He admitted no knowledge of voting system inventory (VSI) and simply trusted whoever the requester was. If true, why have a process at all? It easily (and unfairly) reinforces the mocking image of government incompetence.

ii) Jena Griswold has claimed "nobody is above the law" or some variation of that cliché so many times it has lost its import. Yet, when Jena Griswold's office runs afoul of the law there seems to be no accountability by Jena for her failed leadership and no consequence to her staff.

iii) Diligence by underlings to adhere to annoying aspects of any job derives directly from their leadership. Those processes are only in place to ensure compliance or quality, so universal, they become automatic and routine. They do not lose their importance with time unless they are bad policy in the first place. So, regardless of whether these were necessary quality controls that went unenforced or wasteful bureaucratic nonsense, Jena Griswold is ultimately responsible.

4) **Lack of Training**[60] - Employee 8 states that he was granted approval authority in JIRA without ever receiving formal training, reflecting a lack of basic controls over who could authorize sensitive actions. Within the Voting Systems Team, no one other than Former Employee 1 appears to have been adequately trained in Microsoft Excel, despite the fact that the software itself provides simple tools for identifying hidden data—an elementary safeguard that went unused. Former Employee 1 also gave inconsistent accounts of whether any meaningful transition or exit training occurred when she joined or left the office, even though such handoffs are among the most basic human-resources responsibilities. While some gaps might be understandable when employees do not overlap, ensuring minimal continuity is a core management obligation. Compounding these failures, Former Employee 1 has been unwavering in

[60] Ironically, the Clear Ballot employee did not recognize the security risk created by the BIOS passwords' erroneous public posting until he was in security training on October 24, 2024. See Denver DA Report, supra note 10, at 23 ("It was not until he was in an election security training course in October that [Clear Ballot Employee 2] realized the presence of those BIOS passwords could be a problem. . . . Inv Brodzinski believes that all occurred on October 24, 2024.").

asserting that she never disclosed the existence of hidden tabs, despite her uncertainty about training, and neither investigation meaningfully tested this internal inconsistency in her testimony. Taken together, these examples show a systemic failure by leadership to prioritize training, enforce competence, or create incentives for institutional learning across multiple operational areas.

This is important because:

i) This pattern of inadequate and inconsistent training is especially significant because leadership has repeatedly pointed to "additional training" as the primary remedy for the failure, even though the record shows that training was already treated as optional, informal, or poorly enforced. When employees are granted authority without instruction, lack basic technical competence, and experience no structured transition process, promising more training after the fact amounts to little more than a rhetorical fix rather than a substantive reform. Effective training is not a one-time response to a crisis but a sustained management function that requires standards, documentation, accountability, and reinforcement. Without evidence that leadership has fundamentally changed how it prioritizes, delivers, and verifies training, assurances of improvement lack credibility and do little to reduce the risk of future failures.

V) Grisgate

There are dozens upon dozens of news and academic articles and books that discuss political cover-ups in the United States and globally. But there are commonalities to them all: early minimization of the incident; shifting explanations as new facts emerge; selective transparency in which some documents are released while others are withheld; a relentless focus on process over substance; scapegoating of junior staff; delayed disclosures of key facts; controlled investigations scoped to avoid sensitive areas; suspicious gaps in the record; and message discipline in which officials repeat near-identical talking points. The BIOS password scandal satisfies every one of these hallmarks.[61]

[61] See generally Cover-up, Wikipedia, https://en.wikipedia.org/wiki/Cover-up; List of Federal Political Scandals in the United States, Wikipedia, https://en.wikipedia.org/wiki/List_of_federal_political_scandals_in_the_United_States.

1) **Early minimization.** Secretary Griswold's first public statement on October 29 was that the Colorado Republican Party's description of the breach was "not accurate."[62] She then told Kyle Clark's audience "we do not see this as a full security threat to the state"[63] — a security assessment made without having reviewed the audit logs, without having notified the county clerks, and before anyone at CDOS could possibly have determined whether harm had occurred. As documented above, the audit log review was not completed until November 1.[64] The Secretary's declaration of "no security threat" on October 29 was factually unsupported at the moment she made it.

2) **Shifting explanations.** Deputy Secretary Chris Beall initially told DA investigators that CDOS was required "by rule or statute" to post the Voting System Inventory publicly.[65] That claim was repeated in numerous contemporaneous news articles[66] and created an air of inevitability: the posting was a lawful transparency obligation, not a policy choice. Weeks later, Beall corrected the record with investigators, conceding no such legal requirement existed.[67] The Baird Quinn report confirmed this: there is no statute or rule requiring the VSI — let alone a native Excel file with hidden tabs — to be posted publicly.[68] Secretary Griswold has never corrected this misimpression with the public or press. The "legal obligation" narrative, which softened the public's reaction to the breach, remains uncorrected to this day.

3) **Selective transparency.** Both investigations were narrowly scoped. The Denver DA's investigation expressly excluded any examination of CDOS's response to the disclosure, including how the leak response was managed.[69] The Baird Quinn Report,

---

[62] Colorado Secretary of State Posted Voting System Passwords Online, 9News (Oct. 29, 2024), https://www.9news.com/article/news/politics/elections/colorado-secretary-of-state-posted-voting-system-passwords/73-c9264216-7a0a-4d5b-9f64-60a28eb57e4d [hereinafter Griswold-Clark Interview] (Griswold, asked by Kyle Clark whether the Colorado GOP's claim that the Department posted "more than 600 BIOS passwords for voting systems in all but one Colorado County" was accurate, responding: "That is not accurate.").

[63] Id. (Griswold: "To be clear, we do not see this as a full security threat.").

[64] Press Release, Polis & Griswold, supra note 18.

[65] Denver DA Report, supra note 10, at 2.

[66] See, e.g., Birkeland & DeMare, supra note 54 (recounting Griswold's public statements that the publication was a transparency obligation).

[67] Denver DA Report, supra note 10, at 26 (Beall "stated he was mistaken when he previously said there was a specific rule" requiring publication).

[68] Baird Quinn Report, supra note 11, at 7 n.7 (citing 8 CCR 1505-1, Rule 11.8.7, which requires the Secretary of State to "maintain a list of all certified … voting systems, devices and related components," not to publish that list).

[69] Denver DA Report, supra note 10, at 1 ("Response to the discovery of the passwords, actions taken by the CDOS outside of the publication of the passwords … are not being investigated.").

commissioned by CDOS itself, was confined to whether the BIOS-password publication itself violated CDOS policy; while attorney Quinn requested e-mail and Microsoft Teams searches and concluded the responsive material was "not materially helpful to this analysis," what was withheld from her, or whether the responsive material would be material to a broader analysis.[70] Neither investigation addressed a single action taken by Secretary Griswold personally. Her name does not appear even once in either investigative report.[71] The Microsoft Teams messages and e-mail traffic most relevant to the June 2024 posting decision were lost entirely under CDOS's 45-day auto-deletion policy, with no recovery possible one day after deletion.[72] The June 21, 2024 posting decision predated the October 24, 2024 discovery of the breach by approximately 125 days; under the Department's own retention policy, any non-archived e-mail or Teams messages bearing on the decision had been auto-deleted before anyone knew there was anything to investigate. Even on its face, the policy does not address text messaging, Signal, or any other disappearing-message platform — a gap that became material when a former senior staffer publicly disclosed that Secretary Griswold and her senior team have routinely used disappearing-message applications to communicate "key directives," rendering those communications unrecoverable by design rather than by policy lapse.[73] That gap was identified but never addressed as a records-management failure. Ultimately, the public and the Clerks and the reviewers received only what CDOS chose to share.

4) **Process over substance.** Secretary Griswold invoked "working with our federal partners" four separate times in the Kyle Clark interview and "out of an abundance of caution" four additional times, redirecting the audience's attention to procedural

[70] Baird Quinn Report, supra note 11, at 1–2 (defining the scope of the engagement and noting that responsive e-mail and Microsoft Teams material was reviewed but "not materially helpful to this analysis").

[71] See generally Denver DA Report, supra note 10; Baird Quinn Report, supra note 11. Independent text searches of both reports return zero references to Secretary Griswold by name.

[72] Colo. Dep't of State, Record Retention Policy, https://www.sos.state.co.us/pubs/info_center/recordRetentionPolicy.html ("All email items in an individual user's mailbox older than 45 days, other than those stored in a designated subfolder …, will be automatically moved to the 'Deleted Items' folder on a daily basis"; "One day after this automatic deletion, these items are not recoverable by any means.").

[73] See "Single Most Insecure Person I've Ever Encountered": Former Griswold Aide Breaks Silence Ahead of AG Race, Rocky Mountain Voice (Apr. 2, 2026), https://rockymountainvoice.com/2026/04/02/single-most-insecure-person-ive-ever-encountered-former-griswold-aide-breaks-silence-ahead-of-ag-race/ (statement of Reese Edwards, former Director of Government and Public Affairs, Office of the Colorado Sec'y of State: "Transparency was also lacking. Key directives were communicated through disappearing-message applications, limiting accountability and public recordkeeping.").

activity rather than the substance of what had occurred and who was responsible.[74] This pattern continued throughout the subsequent days of public response: CDOS press releases described the cure process in operational terms while carefully avoiding any discussion of why the five-day delay had occurred, who had decided not to notify the Clerks, or what role the Secretary played.[75]

5) **Scapegoating.** The two investigations distributed accountability across three lower-level figures — none of whom set policy and none of whom was named publicly — while leaving the Secretary herself outside the frame. The criminal investigation's sole subject was an Elections Specialist IV identified only as "Employee 5" (Position #200), exposed to felony liability under the very statute Secretary Griswold championed in 2022, Colo. Rev. Stat. § 1-13-708(2).[76] The second target was "Employee 8," the authorized approver who cleared the spreadsheet for publication in under a minute. Employee 8 told investigators he had received no training for the approver role and "simply clicked on the approval button without looking at the request or file to be uploaded."[77] The third target was Former Employee 1, the original author of the hidden tabs. She had created those tabs years before the breach as informal "scratch paper," had no role in the June 2024 publication decision, and had left the Department before the file was posted. CDOS's public posture nonetheless treated her as the source of the policy violation. Both investigations reached the opposite conclusion: each found her credible, and the Baird Quinn report expressly concluded that she did not violate State policy because she had "no reasonable expectation that the file would ever be publicly disclosed in its native format."[78] A former employee no longer at the Department — with no platform from

---

[74] Griswold-Clark Interview, supra note 17 (Griswold repeating the phrases "working with our federal partners" and "out of an abundance of caution" throughout the interview).

[75] See, e.g., Press Release, Polis & Griswold, supra note 18; CDOS Fact Sheet, supra note 26 (each describing remediation steps in operational terms while omitting any account of the five-day delay or the Secretary's personal role).

[76] Denver DA Report, supra note 10, at 1 (identifying Employee 5 as the suspect under C.R.S. § 1-13-708(2)); id. at 15 (Employee 5 holds Position #200, with a State Personnel System classification of Elections Specialist IV); see Press Release, Colo. Sec'y of State, supra note 42 (Griswold championing SB22-153, the Colorado Election Security Act, which created the felony provision codified at C.R.S. § 1-13-708(2)).

[77] Baird Quinn Report, supra note 11, at 14 (Employee 8 "approved Employee 5's web request within one minute" and "simply clicked on the approval button without looking at the request or file to be uploaded"; "Employee 8 received no training when he became an authorized approver").

[78] Denver DA Report, supra note 10, at 23 (Former Employee 1 "described [the hidden tabs] as like 'scratch paper or a notepad'"); Baird Quinn Report, supra note 11, at 10 (Former Employee 1 stated they were "scratch paper" "functional to me"); see also id. (concluding Former Employee 1 did not violate state policy because she "had no reasonable expectation that the file would ever be publicly disclosed in its native format").

which to defend herself — was a convenient figure to whom blame could be assigned, and the Secretary did nothing publicly to correct the record. The pattern across all three figures is the same: accountability flowed to the people least able to set or contest the policies under which they were working, and away from the leadership that designed those policies, staffed those roles, and approved (or failed to require) the training and review controls that would have prevented the breach.

6) **Delayed disclosures.** The file containing 600-700 BIOS passwords was publicly accessible for approximately 125 days — from its June 21, 2024 posting through its discovery by Clear Ballot on October 24.[79] The public learned of the breach five days later, on October 29, and only because the Colorado Republican Party's email forced the issue.[80] During those five days, at least 158 unique IP addresses had already accessed the file.[81] Audit log review was not completed until November 1 — eight days after discovery. No County Clerk was formally notified before the Republican Party email was sent.[82]

---

[79] The exact number of BIOS passwords disclosed remains ill-defined: CDOS has never stated the precise figure, and contemporaneous press accounts diverge widely. Compare John Frank, Colorado Election Breach Controversy Escalates and Draws Trump's Attention, Axios Denver (Oct. 31, 2024), https://www.axios.com/2024/10/31/colorado-election-passwords-jena-griswold-donald-trump (describing the breach without ever stating a count of disclosed passwords), with Quentin Young, Election System Passwords Mistakenly Exposed on Colorado Secretary of State's Website, Colo. Newsline (Oct. 30, 2024), https://coloradonewsline.com/2024/10/30/election-system-passwords-colorado/ (referencing approximately 700). Whatever the precise figure, the unauthorized release of any number of BIOS passwords greater than zero is problematic; once that number reaches several hundred, the public is entitled to be deeply concerned. See also Baird Quinn Report, supra note 11, at 8, 12 (the underlying Excel spreadsheet was created on January 20, 2023; the public posting at issue occurred on June 21, 2024); CDOS Fact Sheet, supra note 26 (confirming the disclosure affected 34 of Colorado's 64 counties).

[80] An exceedingly odd coincidence was also raised by the affidavit and testimony of Shawn Smith. Mr. Smith indicated he discovered the hidden passwords on October 24. See Transcript of Hearing on Motion for Preliminary Injunction at 25-26, Libertarian Party of Colo. v. Griswold, No. 24CV33363 (Colo. Dist. Ct. Nov. 4, 2024), https://archive.org/details/libertarian-party-v-griswold-24cv33363-hearing-transcript-2024-11-04. That means that after 125 days of nobody noticing the hidden passwords posted on the Secretary's website, two people with no connection – Mr. Smith and separately, the employee at Clear Ballot – both discovered the hidden tabs on the same day and one of them alerted the Secretary of State and the other Republican Party. Neither investigation even considered this oddity.

[81] Denver DA Report, supra note 10, at 7 ("on October 25, 2024 at 7:00 AM Employee 1 found that 158 unique IP addresses ha[d] accessed the Voting Systems Inventory since June 21, 2024").

[82] Press Release, Colo. Sec'y of State, Department of State Updates Coloradans on Election Security Following Password Disclosure (Nov. 4, 2024), https://www.coloradosos.gov/pubs/newsRoom/pressReleases/2024/PR20241104Passwords.html ("County Clerks were informed that day; many had already learned of the disclosure from a press release issued by the Colorado Republican Party."); see also Griswold-Clark Interview, supra note 17 (Griswold confirming to Kyle Clark that the County Clerks had not been notified before the GOP email).

7) **Controlled investigations.** The Baird Quinn "independent" investigation was commissioned by Deputy Secretary Beall — the same official who made a materially inaccurate statement to DA investigators about a mandatory posting obligation.[83] CDOS held the purse strings for the engagement and maintained attorney-client privilege over it.[84] The scope of both investigations was explicitly limited to the posting event itself; crisis response, escalation to the Secretary, and leadership conduct were all placed out of scope.[85] The result is that the two official investigations of this incident produced a record of what a low-level employee posted to a website, but no record of what the Secretary of State did about it. This is the particular dishonesty of a controlled investigation — the public is left with neither the exoneration that a truly independent review would have delivered if no fault existed, nor the concrete findings of misconduct that an unconstrained inquiry might have produced. Secretary Griswold chose the path that allows this to hang over her permanently and yet, by design, leaves every critic without the documentary record needed to make the case stick.

8) **Record gaps.** Teams messages relevant to the June 2024 posting decision were lost due to CDOS retention policy — a gap identified by investigators but never explained as a compliance failure.[86] No contemporaneous written record exists of: who authorized the VSI to be posted publicly; why it was posted in native Excel format rather than as a PDF; what directives Secretary Griswold issued after October 24; or what she was told, by whom, and when.[87] Whether any parallel communications

---

[83] Baird Quinn Report, supra note 11, at 1 (engagement letter addressed to "C. Beall, Deputy Secretary of State"); see Denver DA Report, supra note 10, at 2, 26 (Beall's initial "by rule or statute" statement and his subsequent recantation); see also supra notes 64, 66.

[84] Baird Quinn Report, supra note 11, at 1 ("I was retained by the Colorado Department of State ('CDOS')"; report header marked "ATTORNEY-CLIENT PRIVILEGED INFORMATION / ATTORNEY WORK PRODUCT / CONFIDENTIAL"); see also John Frank, Jena Griswold Faulted in Outside Investigation into Colorado Election Breach, Axios Denver (Dec. 9, 2024), https://www.axios.com/local/denver/2024/12/09/investigation-fault-griswold-colorado-election-breach ("The secretary's office did not release the full report — making it difficult to gauge the extent of the investigation"; reporting investigation cost up to $30,000 borne by CDOS).

[85] See supra notes 69–70 (scope disclaimers in both reports).

[86] See Colo. Dep't of State, Record Retention Policy, supra note 72 (45-day auto-deletion); Baird Quinn Report, supra note 11, at 2 (Quinn requested e-mail and Microsoft Teams searches and concluded the responsive material was "not materially helpful to this analysis", but neither the Department nor the report characterizes the loss of older Teams messages as a compliance failure).

[87] See Baird Quinn Report, supra note 11, at 11–14 (documenting only the operational JIRA workflow — Employee 5's request, Employee 8's one-minute approval, Employee 9's fulfillment — with no written record identifying who authorized the posting at a policy level, why a native Excel file was substituted for the prior PDF practice, or any post–October 24 directives from the Secretary); see also supra note 71 (zero references to Secretary Griswold by name in either investigative report).

channels — personal email, text, messaging applications — were used was never investigated.[88]

9) **Message discipline.** Multiple CDOS officials repeated near-identical formulations in public statements and in communications with county clerks: "working with our federal partners," "out of an abundance of caution," "no security threat," "staff in the field."[89] This consistency is inconsistent with spontaneous reaction. It is consistent with coordinated messaging. The October 31 conference call on which Deputy Secretary Beall told Adams County Clerk Josh Zygielbaum "we were not going to tell counties because we could not tell counties without it becoming the media storm it has become" confirms that message management, not transparency, was the governing priority from the moment of discovery.[90]

   Moreover, executive branch scandals and cover-ups really only have three means of accountability: judicial, legislative, or public. There will be no judicial accountability of the BIOS password leak because the Democratic-elected District Attorney determined nobody "knowingly" released the information, or that those involved lacked the *mens rea* of actual harm.[91] And the legislative branch, also Democratically controlled, declined to conduct an Audit Committee hearing or investigation.[92] So, while this scandal satisfies all of the commonalities of a cover-up described above, the public — through the Secretary's lack of transparency — lacks the facts or information for full accountability to be achieved.

   Secretary of State Jena Griswold has made election security, election denialism, and election insider threats synonymous with her political existence. Because election security is the foundation of her political identity, the BIOS password leak threatened her more than any prior misstep. That is why suppressing public — and even official — acknowledgement of it became the governing priority from the moment of

[88] See supra note 10 & 70 (scope of both investigations limited to the posting event); cf. supra note 73 (Edwards disclosure that Secretary Griswold's senior team has routinely used disappearing-message applications to communicate "key directives" — a parallel channel neither investigation examined).

[89] See Griswold-Clark Interview, supra note 17; CDOS Fact Sheet, supra note 26; Press Release, Polis & Griswold, supra note 18.

[90] See Excerpts from SoS Call to County Clerks, supra note 50.

[91] Press Release, Denver Dist. Att'y's Off., supra note 27.

[92] See Birkeland & DeMare, supra note 54.

discovery. It is further why Griswold had to distance herself from responsibility,[93] minimize and mislead about the facts, blame her employees, and rely on senior staff to manage the crisis. It is a plain fact that Griswold is never named in either investigative report.[94] Both investigations were scoped so narrowly that they reviewed only the act of posting — never the crisis-management decisions that followed, the supervisory failures that preceded it, or the structural deficiencies that allowed it to happen in the first place. Yet with Griswold's decision to seek the Office of Attorney General, she has put the need for full accountability front and center.[95]

This is important because:

i) The sequence of events on and after October 24, 2024 remains remarkably opaque. Secretary Griswold was in Colorado that day — she held a press conference that morning addressing the ongoing Mesa County insider threat matter, demonstrating she was accessible to her staff.[96] Yet no record exists of when she was briefed about the BIOS password discovery that afternoon or evening, by whom, or what instructions she gave. The five days between October 24 (when Clear Ballot and CDOS senior staff learned of the breach) and October 29 (when the public learned of it) were not spent notifying county clerks, completing a thorough technical assessment, or engaging the Governor's office. Governor Polis learned of the scandal at the same time as the public, on October 29; he was briefed by CDPS the following morning and by Secretary Griswold herself on the afternoon of October 30.[97] He activated SEOC, declared password changes "necessary," and deployed helicopters and state resources to complete the cure in 36 hours — the same cure that Secretary Griswold had characterized as unnecessary for the preceding five

[93] Secretary Griswold did not even sign the emergency regulations promulgated on an emergency basis to facilitate the password changes and verify the security of all affected components. See Election Rule 20.5.2(c)(12), codified at 8 CCR 1505-1 and went into effect on October 31, 2024 (signed by Deputy Secretary of State Christopher Beall).

[94] See supra note 71.

[95] See Hannah Metzger, Jena Griswold's Greatest Gaffes: A Reign of Error at the Secretary of State's Office, Westword (Nov. 7, 2024), https://www.westword.com/news/colorado-secretary-of-state-jena-griswold-greatest-gaffes-22428803/.

[96] Press Release, Colo. Sec'y of State, Ballot Fraud Scheme Under Investigation in Mesa County (Oct. 24, 2024), https://www.sos.state.co.us/pubs/newsRoom/pressReleases/2024/PR20241024BallotFraud.html.

[97] See Press Release, Off. of the Governor, supra note 18 (Polis briefed Wednesday morning by CDPS, spoke with Sec'y Griswold Wednesday afternoon); Press Release, Polis & Griswold, supra note 18 (Nov. 1, 2024 announcement that all affected active equipment had undergone password updates).

days. Not one of Colorado's 64 county clerks has ever corroborated a claim that they were notified before October 29.[98]

ii) For a candidate seeking to be Colorado's chief law enforcement officer — overseeing the largest law firm in the state, supervising hundreds of attorneys, managing the statewide grand jury, and advising every agency of state government — voters are entitled to know how she managed one of the most sensitive security crises of her public career. In short, who knew what, and when? These basic questions remain unanswered.

VI)(Non)Independent Investigation

On November 4, 2024, the Secretary of State chose the law firm Garnett Powell Maximon Barlow & Farbes to conduct an "independent" investigation of the BIOS password leak.[99] David Powell, a well-respected and capable attorney, was to lead the investigation. The retention of Powell was meant to squelch criticism, but it had the opposite effect. His choice was criticized as being captured by the SoS, and he lacked documented experience conducting a technology-breach investigation.[100]

1) Subsequently, and without fanfare, on November 12, 2024, it was made known that Powell's firm was no longer doing the independent review, apparently because the firm had political conflicts.[101] The Secretary of State replaced Powell with a boutique firm, Baird Quinn. Of course, Baird Quinn is subject to many of the same criticisms, though to a lesser degree. And it cannot be called "independent" when the entity that is the target of the inquiry chooses the reviewer, holds the purse strings, and maintains attorney-client privilege over the engagement. That is like saying a defense attorney is "independent" of the person they represent.

---

[98] See Press Release, Colo. Sec'y of State, supra note 82 (acknowledging "County Clerks were informed that day; many had already learned of the disclosure from a press release issued by the Colorado Republican Party.").

[99] See Bente Birkeland & Molly Cruse, Secretary of State Details When Her Office Learned of Improperly Posted Passwords, Colo. Pub. Radio (Nov. 4, 2024), https://www.cpr.org/2024/11/04/secretary-of-state-jena-griswold-details-improperly-posted-passwords-timeline/.

[100] See Bente Birkeland, Secretary of State Switches Law Firms for Voting Machine Passwords Investigation, Colo. Pub. Radio (Nov. 12, 2024), https://www.cpr.org/2024/11/12/secretary-of-state-switches-law-firms-voting-machine-passwords-investigation/ (multiple partners at Garnett Powell Maximon Barlow & Farbes, including Stan Garnett and Hubert Farbes, had donated to Griswold's past campaigns).

[101] Id. Notably, Quinn Baird was actually engaged November 8, 2024.

This is important because:

i) If nothing else, the Powell-then-Baird Quinn sequence clearly demonstrates poor decision making. Rather than seek a truly independent review chosen by a disinterested party and paid with funds not under the Secretary's control, Griswold managed the political fallout. She did not seek real and timely answers about the consequences of the leak. The first choice failed. Rather than learn from that failure, she applied the same solution a second time.

ii) The Baird Quinn engagement raises structural conflicts that were never disclosed or resolved. The investigation was commissioned by Deputy Secretary Beall — the same official who made a materially inaccurate statement to DA investigators asserting a legal obligation to post the VSI. In effect, Beall commissioned an "independent" investigation that ultimately found his own statement to law enforcement was unsupported — without the obvious structural conflict ever being publicly acknowledged. Lead investigator Beth Doherty Quinn has a documented history of political contributions to Colorado Democrats.[102] Whether Baird Quinn filed a conflict disclosure, and what it said, has never been made public. The specific contract terms of the engagement remain undisclosed. And critically, no investigation — not the DA's office, not Baird Quinn — ever addressed the most fundamental question: what did Secretary Griswold do, and when did she do it? Her name does not appear in either report. In a review purportedly examining a failure of this magnitude, that omission is not an oversight. It is a design choice.

iii) Griswold's poor decision-making cost the state time and money. The transition from Powell to Baird Quinn created a gap of more than a week during a period of intense scrutiny. What information, if any, was gathered by Powell's firm and whether it was fully transferred remains unknown. Whether employees were interviewed by Powell, and whether those statements were shared, is unknown. Whether the switch was precipitated by confirmation of the criminal investigation is unknown. What or whose pressure caused

[102] See Colo. Sec'y of State, TRACER Campaign Finance Database — Contributor Search: Beth Doherty Quinn, Denver, CO, https://tracer.sos.colorado.gov/ (recurring donations 2010–2025 to overwhelmingly Democratic candidates and committees, including Phil Weiser for Colorado (current Colorado Attorney General), McCann for Denver DA, and Michael for Attorney General — the campaign committee of Boulder County District Attorney Michael Dougherty, a Democratic candidate for Attorney General against Secretary Griswold).

Griswold to abandon her first choice, despite minimal public reporting on the conflict, has never been explained.

VII) Inconsistencies or Poor Investigative Work

The Baird Quinn investigator confidently concluded that "One transition meeting with Former Employee 1 occurred" but then immediately stated that "no one recalls any specific discussions from the transition meeting."[103] Later in the same report, the investigator stated that Former Employee 1 "does not, after the passage of time, recall with any more specificity the nature or purpose of those [hidden] worksheets" but reiterates with equally baffling confidence that Former Employee 1 "*never* told anyone that there were hidden worksheets (tabs) in the '!NEW! Equipment Database Excel file'" (emphasis added).[104] The DA's investigator, who had the benefit of the Baird Quinn report prior to his interview, wrote that Former Employee 1 "thought no one currently at the Voting Systems Team would have had any way of knowing the hidden tabs were in the spreadsheet when it was published in June 2024" and "does not recall providing any transition training." The DA's office then concluded that "nothing Former Employee 1 said contradicted anything else already learned in this investigation and was not substantially different from what is reported in the Baird Quinn investigation." The contradiction in her own account — a meeting occurred, but nobody remembers it, including the person whose account is the foundation of the primary conclusion — was apparently not worth pursuing.[105]

1) A second category of investigative failure involves missing witnesses. Neither investigation interviewed external actors with alleged early knowledge of the BIOS passwords, including Shawn Smith (the affiant associated with the Republican Party email who claimed knowledge of the passwords as early as August 2024), Representative Stephanie Luck, candidate Jeff Patty,[106] or any of the 34 county clerks whose election equipment was compromised.[107] No forensic analysis was attempted to identify, let alone to contact, any of the 158 unique IP addresses that CDOS

[103] Baird Quinn Report, supra note 11, at 11.

[104] Baird Quinn Report, supra note 11, at 10.

[105] Denver DA Report, supra note 10, at 23–24.

[106] Republican Party Letter and Affidavit, supra note 14; Marshall Zelinger, Secretary of State grilled over leaked voting system passwords in Colorado, 9News (Jan. 23, 2025), https://www.9news.com/article/news/politics/colorado-s-leaked-voting-passwords-jena-griswold/73-edc748fd-a60f-4442-a526-aa467c4bc347 (relaying Hannah Metzger, Westword (Nov. 27, 2024), reporting that Smith identified Rep. Stephanie Luck (R-Penrose) and failed House District 38 candidate Jeff Patty as his tipsters at a Colorado Republican Party luncheon).

[107] CDOS Fact Sheet, supra note 26.

determined had accessed the file.[108] The DA did not interview Deputy Director of Elections Hilary Rudy (Employee 2) or Elections Director Judd Choate (Employee 10), despite both being key escalation nodes in the notification chain to senior leadership.[109] The DA did not explain these omissions.

2) A third anomaly involves the irregular treatment of Former Employee 1's political views in the investigative record. At a minimum, we know the Denver DA investigation apparently reviewed her social media activity related to Donald Trump and the 2020 election[110], even though both reports ultimately concluded that the password disclosure was accidental and unintentional. This presents an unexplained inconsistency in investigative purpose: if investigators concluded there was no malicious intent, why was political social media content gathered and reviewed? One explanation is that the review was designed to inoculate the Secretary politically — to establish that the responsible employee held anti-Trump views, providing a narrative shield against accusations of deliberate partisan sabotage. Another is that investigators started with a hypothesis the evidence did not support and then abandoned it without accounting for why the evidence was gathered in the first place. The record also shows inconsistent use of pronouns in describing Former Employee 1[111] alongside extensive redactions related to her political views.[112] Whatever the explanation, it was never disclosed.

   This is important because:

   i) The deeper failure is epistemic. The Baird Quinn report concludes that "nothing Former Employee 1 said contradicted anything else learned." But the record itself contains an unreconciled contradiction about transition training

---

[108] Denver DA Report, supra note 10, at 7; id. at 1.

[109] Baird Quinn Report, supra note 11, at 18, 19, 22–23 (documenting Employee 2's role in the October 24, 2024 escalation chain); Denver DA Report, supra note 10 (containing no record of any interview of Employee 2 or Employee 10).

[110] Denver DA Report, supra note 10, at 9–10 (Inv. Brodzinski reviewed Former Employee 1's Facebook profile and a YouTube video she had posted depicting then-President Trump and the First Lady; date of posting, video title, channel name, URL, and description redacted); we do not know exactly what information was shared with Baird Quinn because those exhibits have been withheld by the Secretary.

[111] Denver DA Report, supra note 10, at 15 (CDOS's written responses describe Former Employee 1 with both female and male pronouns within the same passage; "His last day on our payroll was August 7, 2023"; "His duties encompassed the various tasks…").

[112] Denver DA Report, supra note 10, at 5–6, 9–10 (redactions in original; identity-verification narrative blacks out an alternate first name, license issuance date, and address fields, alongside the politically-coded YouTube review).

— the very subject on which the investigations' causal chain depends. Stating that no contradiction exists is not resolving the uncertainty; it is papering over it. The choice between the two possible explanations matters. If Former Employee 1's account that she never disclosed the hidden tabs is accurate, then someone else must have known about them, and the organizational failure runs deeper than either report admits. If her account is not accurate, the central causal narrative of both reports collapses. The investigators chose not to press that choice. Two investigators failing to identify the basic inconsistency in the testimony of the witness whose account underpins their primary conclusion is, on its own, sufficient reason to doubt the conclusion. That doubt is compounded here by the fact that the underlying evidence has been withheld from public scrutiny and that serious questions about investigative bias remain unresolved.[113]

VIII) Minor Investigative Mishaps

While the following issues do not independently rise to the level of compromising the investigations' conclusions, they matter for two reasons: first, they confirm that this episode received less rigorous professional review than the gravity of the incident demands; and second, they impair any future effort to revisit the record, now that the electoral stakes are squarely in view. If elected, Griswold will not be overseeing inventory spreadsheets — she will be supervising multi-district murder prosecutions, complex white-collar investigations, environmental enforcement actions, and water compact litigation that must meet a beyond-a-reasonable-doubt standard in open court. These investigations set a far lower bar.

1) The most consequential procedural failing is the absence of any recorded or documented interview of Former Employee 1. The DA's investigator conducted a fifty-minute interview with her without recording it or taking contemporaneous notes. This is an extraordinary omission. Former Employee 1's testimony was foundational: she created the hidden tabs; she determined whether anyone else knew about them; and her account of BIOS password exploitability — that physical access plus a BIOS password is sufficient to alter boot-level machine behavior without a system login — was one of the most technically significant findings in either report. That conclusion

[113] Denver DA Report, supra note 10, at 23 ("Nothing Former Employee 1 said contradicted anything else already learned in this investigation"); Baird Quinn Report, supra note 11, at 10–11 (transition meeting "occurred" but "no one recalls any specific discussions").

rests entirely on unrecorded testimony from a single witness whose own statements were inconsistent across the two investigations.[114]

2) A second failing involves the divergence in witness coverage between the two investigations. Deputy Director of Elections Hilary Rudy (Employee 2) was interviewed by Baird Quinn but not by the DA. Elections Director Judd Choate (Employee 10) was a key escalation node for notification to senior leadership but was similarly not interviewed by the DA. Employee 12 (believed to be Caleb Thornton) and the CDOS Legal Policy Advisor Alonit Katzman also appear not to have been interviewed by the DA. No explanation for these omissions was provided. These are among the most senior CDOS personnel with direct operational responsibility for the VSI and the crisis response. Their absence from the criminal investigation's record creates an incomplete picture of the institutional decision-making chain that cannot now be remedied.[115]

3) Taken together, these procedural deficiencies are not merely academic. This record — incomplete, with unrecorded testimony, missing witnesses, and unexplained redactions — is the totality of the official accountability record that exists for the most significant election security breach in Colorado history. There will be no grand jury re-examination, no legislative audit, no second bite at the apple. What exists is what the public has. And what the public has is insufficient.

IX) Conclusion

The BIOS password scandal is not, at its core, a story about a spreadsheet. It is a story about judgment, leadership, and accountability — the precise qualities Colorado voters are being asked to evaluate as they consider whether Jena Griswold should be the State's next Attorney General.

1) Over the course of eight years as Secretary of State, Griswold built a national brand on one proposition: that she understood election security better than anyone else in Colorado, and that her relentless vigilance was the last line of defense against the insider threats and foreign adversaries she named in press release after press release.

---

[114] Denver DA Report, supra note 10, at 23 (Inv. Brodzinski's recording app failed before the conversation began; "there is no recording of this interview"; "Inv Brodzinski did not take handwritten notes during the conversation"; "The conversation lasted about 50 minutes"); id. at 24 (Former Employee 1's account of BIOS exploitability — "a change could be made to the machine with the BIOS password, even without a local user login").

[115] Baird Quinn Report, supra note 11, at 18, 19, 22–23 (Employee 2 interviewed); Denver DA Report, supra note 10 (containing no record of any interview of Employee 2 or Employee 10).

"[T]he folks who have access to voting equipment in counties do not have the BIOS passwords," she declared at a national conference in July 2022. "Those are the passwords to adjust the settings and passwords to the motherboard." She said this two years before she presided over the largest election security breach in Colorado's history — a breach involving precisely the BIOS passwords she described, affecting precisely the voting equipment she named.[116] The irony is not merely political. It is disqualifying.

2) What this review has documented is not a single failure but a compounding pattern across five distinct dimensions:

   i) **Leadership failures.** A six-year lapse in AUP acknowledgments under her tenure. A password policy so poorly communicated that the CIO gave contradictory accounts of its requirements to two separate investigators. An approval workflow so hollowed out that an authorizing employee "just clicked OK" because he had never been trained. A transition process so informal that the foundational facts of what one employee told another could not be determined by two separate official inquiries.[117]

   ii) **Deception.** A public interview in which the Secretary told viewers the Republican Party's account was "not accurate," while her own office's internal timeline confirms she knew or should have known it was substantially correct. A characterization of the breach as "not a security threat" made before the audit logs had been reviewed, before the Clerks had been notified, and before anyone could possibly have determined whether harm had occurred. Repeated minimizations of the scope and severity of the exposed passwords that are contradicted by the technical record.[118]

---

[116] StateScoop Radio, Secretaries of State Prepare for Insider Threats in Elections, NASS Summer Conference (Baton Rouge, La., July 14, 2022) (statement of Sec'y Jena Griswold), https://statescoop.com/radio/secretaries-of-state-prepare-for-insider-threats-in-elections/ ("the folks who have access to voting equipment in counties, do not have the BIOS passwords. Those are the passwords to adjust the settings and passwords to the motherboard.").

[117] Baird Quinn Report, supra note 11, at 4 n.3 (six-year lapse in AUP acknowledgments); Denver DA Report, supra note 10, at 4, 7 (CIO told DA investigator that storage of the BIOS passwords "was not an acceptable form of password management"); Baird Quinn Report, supra note 11, at 10, 16 (CIO told Baird Quinn that storing the BIOS passwords outside the password safe "is an acceptable alternative to use of the password safe"); Denver DA Report, supra note 10, at 25 (Employee 8 "simply clicked on the approval button without looking at the request itself"); Baird Quinn Report, supra note 11, at 10–11 (transition meeting "occurred" but "no one recalls any specific discussions"); Denver DA Report, supra note 10, at 24 (Former Employee 1 "does not recall providing any transition training").

[118] Griswold-Clark Interview, supra note 17 (Griswold characterizing the Colorado Republican Party's account as "not accurate" and stating "we do not see this as a full security threat"); Marshall Zelinger, Colorado Voting System

iii) **Accountability avoidance.** Five days of silence before the public learned of the breach. A decision, explicitly articulated by her own Deputy, not to notify county clerks because "we could not tell counties without it becoming the media storm it has become." Two investigations, both scoped to exclude the Secretary's own conduct, neither of which named her once. A cover process that required the Governor's intervention, the activation of SEOC, and the deployment of state helicopters to complete in 36 hours what the Secretary had deemed unnecessary for five days.[119]

iv) **Poor judgment.** The selection of an initial "independent" investigator with political conflicts, followed by the appointment of a replacement investigator commissioned by the same deputy who made a material misstatement to the DA. A public communication strategy, including the Kyle Clark interview, that even supporters acknowledged was underwhelming. A consistent instinct throughout the episode to manage the message rather than address the substance.[120]

v) **Unanswered questions.** Five basic questions raised by this review remain unresolved after more than eighteen months: (1) When was Secretary Griswold briefed on October 24, by whom, and what were her directives? (2) Who authorized publication of the VSI in native Excel format, and on whose policy judgment? (3) Why was the decision made not to notify county clerks for at least five days, and what role did Griswold play in that decision? (4) What did CISA ultimately conclude, and do any written findings exist? (5) Were public statements, press narratives, and court testimony in Libertarian

---

Passwords Did Not Start Getting Changed Until After Password Leak Became Public, 9News (Oct. 31, 2024), https://www.9news.com/article/news/local/local-politics/colorado-voting-system-passwords-changed-leak-public/73-b71a4e3f-7b08-4a4b-89b7-3b77af696d0c (CDOS did not notify county clerks until the breach became public; passwords were not being changed before the issue was made public).

[119] See supra (five-day disclosure delay; the "media storm" quote from Deputy Beall; activation of the SEOC and Governor's emergency response); Denver DA Report, supra note 10 (DA scope expressly excluded the Secretary's response); Baird Quinn Report, supra note 11 (engagement letter addressed to Deputy Secretary Beall; the report does not name Secretary Griswold).

[120] Bente Birkeland, Colorado Secretary of State Jena Griswold Details Improperly Posted Passwords Timeline, CPR News (Nov. 4, 2024), https://www.cpr.org/2024/11/04/secretary-of-state-jena-griswold-details-improperly-posted-passwords-timeline/ (Powell retention); Bente Birkeland, Secretary of State Switches Law Firms in Voting Machine Passwords Investigation, CPR News (Nov. 12, 2024), https://www.cpr.org/2024/11/12/secretary-of-state-switches-law-firms-voting-machine-passwords-investigation/ (Powell dismissal; Baird Quinn retention); Griswold-Clark Interview, supra note 17.

Party of Colorado v. Griswold accurate — and if not, has anyone corrected the record?[121]

None of this has been answered. Not by the DA's office. Not by Baird Quinn. Not by the Secretary. The standard of "nobody knowingly did this" sets the floor, not the ceiling, for accountability when a public officer holds the highest election security post in the state.

For context, retired Colorado District Court Judge Ann Frick publicly wrote — days before the March 2026 Democratic Assembly — that Griswold "is not a courtroom attorney" and "has never really tried a case," and expressly endorsed another candidate as far more qualified.[122] As of the June 2026 Democratic primary, Jena Griswold has never entered an appearance as counsel of record in any Colorado or federal court proceeding. She has never signed a pleading, never examined a witness, never made a closing argument. She would be the first Attorney General since 1963 never to have tried a case. At the Longmont Area Democrats forum on February 4, 2026, she admitted: "I am not a trial attorney. That is not what the Attorney General does."[123] She is wrong about the second sentence and candidly right about the first. The Attorney General does try cases, argue appeals, prosecute environmental violators, negotiate water compacts, and supervise complex multi-party investigations that must meet a beyond-a-reasonable-doubt standard in open court. Shannon Stevenson did it. John Suthers did it. Cynthia Coffman did it.

---

[121] The five enumerated questions are unresolved across the public record. The factual predicates for each are sourced supra: (1) October 24 briefing chain (see Baird Quinn Report, supra note 11, at 18–23); (2) authorization for native Excel publication (see Baird Quinn Report, supra note 11, at 11–14); (3) decision not to notify County Clerks (see Marshall Zelinger, Colorado Voting System Passwords Did Not Start Getting Changed Until After Password Leak Became Public, 9News (Oct. 31, 2024), https://www.9news.com/article/news/local/local-politics/colorado-voting-system-passwords-changed-leak-public/73-b71a4e3f-7b08-4a4b-89b7-3b77af696d0c); (4) CISA findings (no public written findings located); (5) statements in Libertarian Party of Colo. v. Griswold (D. Denver) (Griswold-Clark Interview, supra note 17).

[122] Hon. Ann B. Frick (ret.), Opinion: Jena Griswold's Fabrications Are Disqualifying in AG's Race, Westword (Mar. 26, 2026), https://www.westword.com/opinion/jena-griswold-fabrications-disqualifying-for-ag-opinion-40862653/. Judge Frick served as a District Court Judge for Colorado's Second Judicial District (Denver) from 2010 until her retirement, following a 32-year career as a commercial litigator and partner at Jacobs Chase Frick Kleinkopf & Kelley, LLC. See Ann Frick ('78), Colo. Law School (Feb. 27, 2023), https://www.colorado.edu/law/2023/02/27/ann-frick-78.

[123] Activism in the Face of Fascism — February 4, 2026 LAD Meeting, Longmont Area Democrats (Feb. 4, 2026), https://longmontdems.org/2026/01/31/next-lad-meeting-wednesday-february-4-630pm; see also Longmont Area Democrats, YouTube channel, https://www.youtube.com/@longmontareademocrats (hosting the full set of February 4, 2026 meeting clips).

> What it requires is the kind of judgment, rigor, and accountability that the BIOS password episode reveals Griswold fundamentally lacks.

Colorado deserves an Attorney General who can be trusted to demand answers when the government has failed — not one who has demonstrated, in her own office, an instinct to minimize, manage, and suppress accountability when it is inconvenient. The five days of October 2024 are not a footnote in Jena Griswold's political biography. They are the test. She failed it.