BAIRD QUINN LLC

ATTORNEYS AND COUNSELORS AT LAW

THE BUSHONG MANSION
2036 E. 17th Avenue
Denver, Colorado 80206
Tel: 303.813.4500 • Fax: 303.813.4501

Beth Doherty Quinn
Direct: 303.322.5334
bdq@bairdquinn.com

December 8, 2024

ATTORNEY-CLIENT PRIVILEGED INFORMATION
ATTORNEY WORK PRODUCT
CONFIDENTIAL

VIA EMAIL (Chris.Beall@coloradosos.gov)
Chris Beall
Deputy Secretary of State
Colorado Department of State
1700 Broadway, Suite 550
Denver, Colorado 80290

Re: External Investigation Regarding BIOS Password Disclosure

Dear Mr. Beall:

I submit to you this Investigatory Report addressing the June 21, 2024, public disclosure of certain voting systems component BIOS passwords on the Colorado Secretary of State's website.

I. Nature Of The Investigation

On November 12, 2024, I was retained by the Colorado Department of State ("CDOS") to (i) investigate what events occurred that led to the June 21, 2024, public disclosure of certain, active voting systems component BIOS passwords when an Excel file containing hidden worksheets (informally called tabs) which included those passwords was uploaded in native format to the Secretary of State's website; (ii) determine whether any events or conduct that led to the public disclosure violated any CDOS policies or procedures; and (iii) recommend changes to existing policy to prevent any such future public disclosures.

I was provided with a number of policies, documents, files, data, and notes by CDOS. Some of those materials were provided to me *sua sponte* by CDOS. Some were requested by me. All of the materials provided to me are listed on *Exhibit A*. I reviewed in detail the policies, documents, files, data and notes listed on *Exhibit A*. I further requested that CDOS E-mails and Microsoft Teams messages be searched based on search terms I provided. Communications responsive to those search terms were provided to me by CDOS. The search terms are listed on *Exhibit B*. The responsive E-mails and Microsoft Teams messages are numerous and will not be individually listed. However, after review of those communications, I determined that they are not materially helpful to this analysis.

I conducted ten factual interviews, including nine active CDOS employees and one former CDOS employee. All interviews were conducted by Zoom teleconference unless otherwise noted. All interviews were observed by a Legal Policy Advisor from CDOS. I interviewed Employee 1, Chief Information Officer, CDOS, on November 18 and 20, 2024, for a total of three hours. I interviewed Employee 2, Deputy Director, Elections, CDOS, on November 20 and 22 for a total of one hour and twelve minutes. I interviewed Employee 3, Voting Systems Specialist, CDOS, on November 21, 2024, for a total of one hour. I interviewed Employee 4, Voting Systems Specialist, CDOS, on November 21, 2024, for a total of one hour and six minutes. On November 22, 2024, I interviewed Employee 5, Voting Systems Specialist, CDOS, in person for a total of two hours and twenty-four minutes. Employee 5's private legal counsel was present for the interview. On November 22, 2024, I interviewed Former Employee 1, former CDOS Voting Systems Specialist, by telephone for thirty minutes. On November 22, 2024, I interviewed Employee 6, Webmaster, CDOS, for thirty-six minutes. On December 2, 2024, I interviewed Employee 7, Voting Systems Manager, CDOS, for one hour and forty-eight minutes. Employee 7's private counsel was present for the interview. On December 2, 2024, I interviewed Employee 8, Ballot Access Manager, CDOS, for twelve minutes. On December 4, 2024, I interviewed Employee 9, Elections Director, CDOS, for forty-eight minutes.

Finally, I requested that CDOS retain a company specializing in digital forensics for the limited purpose of providing expertise regarding certain metadata and other information associated with the Microsoft Excel program and specific Excel files, including the Excel file uploaded to the Colorado Secretary of State website. At my recommendation, CDOS retained the computer forensic company Archer Hall. On December 4, 2024, I spoke with Expert 1 and Expert 2 of Archer Hall by Zoom teleconference for one hour. Expert advice provided by Expert 1 or Expert 2 is outlined in this report.

I reviewed and evaluated the statements and demeanor of the factual witnesses who were interviewed, the written materials listed on *Exhibit A*, the responsive E-mail and Microsoft Teams communications provided by CDOS, and further considered and relied upon the opinions of the forensic computer experts with whom I spoke to develop this report, its factual findings, conclusions regarding policy violations, and recommendations.

II. Potentially Applicable Policies

The State of Colorado, as well as CDOS, have a number of cyber security and information technology policies. Only policies directly applicable to this matter, or otherwise touching upon matters discussed herein, have been set out in this section.

CDOS Acceptable Use Computing Policy, Dated 8/29/2022 ("CDOS AUP")[1]

I. Introduction

"Information's confidentiality, integrity, and availability are critical to the []CDOS operation and purpose…. it is imperative that employees … ("users") use the computer systems responsibly. Even inadvertent misuse of CDOS computer systems can cause enormous operational, legal, and monetary problems for the Department." *See Exhibit C § I(a)*.

III. Policy
b. User Responsibilities
i. General

"Computer resources and data are to be used for departmental business only…..Unauthorized attempts to use these resources will be grounds for disciplinary action, to include but not limited to suspension, termination, and legal action." *See Ex. C § III(b)(i)(1)*.

"CDOS users are required to adhere to Federal, State, and local laws. Users are required to adhere to the State of Colorado's Cyber Security Policies as well as the Department's Employee Handbook, Cyber Security Policies and Acceptable Use Policy." *See Ex. C § III(b)(i)(2)*.

iii User ID and Password

"Each user will be given a unique user ID for access to the network and other resources. Each Logon-id will have a password that is set by the user upon initial logon…. The password is required to be 15 characters long at a minimum and must consist of a combination of at least three out of four of the following: uppercase letters, lower case letters, numbers, and symbols... *See Ex. C § III(b)(iii)(1)(a)*.[2]

"Users should utilize the department provided password safe and are not permitted to use any other personal password safe for department information or passwords." *See § Ex. C III(b)(iii)(1)(c) (this provision added on 8/29/22 when the current version of the policy was issued).*

---

[1] A prior version of the Acceptable Use Computing Policy, dated September 15, 2017, is substantially similar in all material respects unless noted.

[2] The minimum character number for passwords has gone up to 16 characters and that information has been disseminated to all CDOS staff, including in an April 2, 2024, newsletter. The minimum character length will be updated in the upcoming version of the AUP.

"To ensure additional security, users should:

i. Log off computer system or lock the screen [if away].
ii. Protect their password from disclosure to others.
iii. Choose passwords that are not obvious. A good password includes a combination of upper case letters, lower case letters, numbers, and symbols. Passwords should never consist solely of dictionary words, even from foreign language dictionaries. Dictionary words, even with symbol substituted characters, repeated words, or numbers on the end, can often be easily compromised ….
iv. Not write their passwords down …." *See Ex. C § III(b)(iii)(1)(e).*

iv. System File Shares/Drives

"The Secretary of State and [each] Division's Director will set security policies for access to Division's drives and sites…..Only users given permission to view directories within the drive .. will have permission to access the files." *See Ex. C § III(b)(iv)(1).*

"To ensure file safety, users should store mission critical data on their assigned network drives …." *See Ex. C § III(b)(iv)(3).*

The Acceptable Use Computing Policy contains a signature page for each employee to sign, acknowledging that the employee has read and understood the policy and agrees to abide by the policy. *See Ex. C p. 8.*[3]

A Cybersecurity Education Training Program that CDOS has recently required all staff to review also sets forth the following information regarding setting and managing strong and secure passwords. Specifically, the Training Program states that passwords should be at least 18 characters in length, should be uncommon and unrelated to the user, and should be complex such as using three unrelated words of at least six characters each or a phrase of at least 18 characters in length. The Training Program encouraged use of multi-factor authentication in conjunction with passwords.

[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.

CDOS Employee Handbook, September 2022[4]

Conflicts of Interest and Confidentiality Policy

"The Colorado Secretary of State's office expects all employees to conduct themselves and department business in a manner that reflects the highest standards of ethical conduct, and in accordance with all federal, state, and local laws and regulations." *See Exhibit D p. 12*.

Confidential Information Policy

"The protection of confidential information is vital to the interests and success of the Secretary of State's office. Confidential Information is any and all information disclosed to or known by you because of employment with the agency that is not generally known to people outside the agency. An employee who improperly uses or discloses confidential information will be subject to corrective and/or disciplinary action up to and including termination of employment and possibly legal action, even if the employee does not actually benefit from the disclosed information." *See E. D p. 12*.

Computers, Internet, Email, and Other Resources Policy

"Employees must use appropriate password protections for such devices [described as electronic devices such as laptops, tablets, smartphones, and other data storage media] and physically secure them as recommended by IT Department administrators." *See Ex. D pp. 25-26*.

Colorado Information Security Protocol (CISP) 018: Acceptable Use Of State Data and IT Resources

7. Data Protection and Handling

7.2 "Users may learn, or have access to, sensitive information concerning state and/or agency business …. It is the responsibility of Users to maintain the confidentiality of all state information. Users must take precautions to protect against the unauthorized or careless disclosure of this information at all times and must never share account credentials." *See CISP-018: Acceptable Use of State Data & IT Resources (AUP) – December 2022 § 7.2* found at https://oit.colorado.gov/standards-policies-guides/technical-standards-policies.

7.3 "Devices storing sensitive information, even for a limited duration, must be encrypted in compliance with all applicable Colorado Information Security Policies (CISPs) and OIT Technical Standards as posted on OIT's public website at oit.colorado.gov." *See CISP-018 § 7.3.*

[4] A prior version of the Employee Handbook, dated October 2021, is substantially similar with regard to the material policies listed herein.

15. Unacceptable and Prohibited Use of State IT Resources

15.7 "Users may not use state IT resources, including public-facing state IT resources, to engage in any conduct in violation of any local, state or federal law or regulation ... or any of the Colorado Information Security Policies." *See CISP-018 §15.7.*

18. Annual Acceptance

"This policy must be accepted by Users at the start of employment and no less than annually thereafter. *See CISP-018 §18.*[5]

Colorado Information Security Protocol (CISP) 010: Data Protection, Recovery and Sanitization

8.3 Business Owner

8.3.1 "As Data Steward, the Agency/Business Owner is responsible for ensuring the State's data is accessible, usable, safe and trusted. This responsibility includes overseeing every aspect of the data life cycle: creating, preparing, using, storing, archiving and deleting data, in accordance with data compliance requirements and Business Owner's established data governance principles for promoting data quality and integrity."

9.3 Configure Data Access Control Lists

9.3.1 "ITSP [Information Technology Service Provider (such as the CDOS IT Division)] shall configure data access control lists, also known as access permissions, to local and remote file systems, databases and applications, based on a user's role within the Agency or need to know.

9.7 Encrypt Data on End-User Devices

9.7.1 "ITSP [Information Technology Service Provider (such as the CDOS IT Division)] shall encrypt data on IT assets containing data deemed sensitive to Business Owner or in adhering to applicable laws and regulations."

Colorado Information Security Protocol (CISP) 001: IT Access Control Management and User Security

9.15 Publicly Accessible Content

9.15.2 Business Owner shall train authorized individuals to ensure that publicly accessible information does not contain non-public information.

9.15.3 Business Owner shall review the proposed content of information prior to posting onto the publicly accessible Information System to ensure that non-public information is not included.

[5] There is no evidence in the personnel files for the VS Team members provided to the investigator that these employees have ever signed the State's Acceptable Use Policy.

9.15.4 Business Owner shall review the content on the publicly accessible Information System for non-public information and remove such information, if discovered.

Of Note: C.R.S. § 1-13-708(2)

"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." *See C.R.S. § 1-13-708(2)*

III. Factual Findings

VS Team Responsibilities

CDOS' Elections Division includes a group of employees known as the Voting Systems team ("VS Team"). The VS Team is typically comprised of one Voting Systems Manager and three Voting Systems Specialists. One of the many responsibilities of the VS Team is to certify voting systems components submitted by a county to the Secretary of State for certification. For voting systems components containing software, as part of the certification process, the VS Team uses a Trusted Build to install voting system software and firmware (firmware is software that assists in the start-up of a device) on the component.[6] As part of that Trusted Build process, the VS Team ensures that firmware known as the Basic Input/Output System ("BIOS") has certain settings selected to enhance security of the voting systems component. For example, Bluetooth or Wi-Fi access would be disabled. After the appropriate BIOS settings are selected, the VS Team assigns and inputs a complex password to the BIOS which only the VS Team retains.

The VS Team maintains, as is required by law, an inventory of all voting systems components that are used or available for use by each of Colorado's sixty-four counties (hereinafter referred to as the "Voting Systems Inventory" or "VSI").[7] The BIOS passwords are recorded, along with other voting systems component information, in the VSI maintained by the VS Team.

---

[6] *See coloradosos.gov/pubs/elections/VotingSystems/files/trustedBuildProcedures.pdf* (describing the Trusted Build procedure and stating that a Trusted Build is a software build "performed with adequate security measures implemented to give confidence that the executable code is a verifiable and faithful representation of the source code.")

[7] 8 CCR 1505-1, Rule 11.8.7 states that the Secretary of State will maintain a list of all certified … voting systems, devices and related components, purchased, leased or used by Colorado political subdivisions. The list will include, at minimum, the name of the jurisdiction, the name and version of the voting system, the date of acquisition, and the serial numbers of voting devices.

The Excel File Housing The VSI

Historically, the VS Team kept the VSI in a single Microsoft Access database. Personnel file information shows that in June 2020 a new Voting Systems Specialist, Former Employee 1, was hired onto the VS Team. Former Employee 1 was employed on the VS Team through May 19, 2023, when she resigned her position.[8] While employed by CDOS, Former Employee 1 was the employee on the VS Team that had primary responsibility for maintaining the VSI. Former Employee 1's Job Description reflects that responsibility. By August 2021, Former Employee 1 recommended to Employee 7 that the VSI be migrated to, and maintained in, an Excel file rather than in the Microsoft Access database. Employee 7 ultimately accepted that recommendation. As a result, Former Employee 1 exported the VSI information housed in the Microsoft Access database to a new Excel file to create a new working VSI file. Former Employee 1 created not only the original Excel file housing the VSI, but also subsequent copies of that file as well.

The Excel file in use today by the VS Team to track VSI has the following file name: !NEW! Equipment Database. It is housed on the Elections Division Shared Drive in a restricted access subfolder titled Voting Systems/Equipment Inventory. Former Employee 1 recalls giving the file this name when she first created it. Metadata located (and viewed by undersigned investigator) in the File/Info tab of this document reflects Former Employee 1 as the author of the document and May 23, 2022, 8:51 AM as the "Created" date. According to the forensic computer experts, Expert 1 and Expert 2, the "Created" date is metadata from the Excel file that reflects the date the document was first created and saved. In other words, here, the metadata demonstrates that Former Employee 1 first created the Excel file housing the VSI on May 23, 2022.[9]

Further, according to the forensic computer experts, when an original file is copied (e.g., opened and a new version is saved via the "Save As" button rather than opening a new, blank Excel workbook), the copied file will retain the original Created date – here, May 23, 2022 – of the file from which the copy was made. Thus, as is the case here, the !NEW! Equipment Database Excel file currently in use today by the VS Team can have a Created date of May 23, 2022, but also metadata that reflects it was copied and subsequently saved to its current location on January 20, 2023.

---

[8] Personnel documents show Former Employee 1's last active day of employment was Friday, May 19, 2023, but she remained on the employee roster through August 7, 2023, due to utilization of PTO.

[9] Other metadata from the !NEW! Equipment Database Excel file reflects a "Content created" date of January 20, 2023 3:38 PM in the Properties/Details tab locating by right clicking on the document icon. According to the forensic computer experts, the "Content created" date is not a date on which forensic examiners rely. It could reflect when the document was first saved to a specific file path or some other saving event. Varonis (CDOS' data audit and protection software) audit logs do reflect that the Excel file named !NEW! Equipment Database was created and saved in its current file path on January 20, 2023, 3:38 PM.

This !NEW! Equipment Database Excel file contains a worksheet (tab) visible to the user that is labeled Inventory which contains eleven columns with the following information:

Serial Number of the voting systems components
County of Ownership
Model Number of the voting systems component (e.g., Dell Lattitude 3490)
Equipment Vendor (e.g., Dominion or Clear Ballot)
PEA Usage
Remarks column
Device Type (e.g., laptop)
Inactive/Active Status
Disposal Status
Firmware of Software Version (e.g., 5.13 or 5.17)
BIOS Password

This has been the same format for this visible Inventory worksheet (tab) since the file was set up by Former Employee 1. It is the final column, labeled BIOS Password, in which the VS Team inputs new BIOS passwords that it creates when it performs Trusted Builds and certifies new voting systems components. It should be noted that if a voting systems component being certified is merely a software upgrade (e.g., not a brand, new component), the new BIOS in the upgraded software will not be given a new BIOS password but will retain the old BIOS password. This eleventh column in the visible worksheet (tab) marked Inventory in the !NEW! Equipment Database Excel file is the only place the VS Team records BIOS passwords (password protected copies of this document in the Voting Systems subfolder also contain the BIOS passwords).

Cybersecurity Measures Related To the !NEW! Equipment Database Excel File

At all times the !NEW! Equipment Database Excel file containing the statewide VSI was subject to a number of security precautions. The two that the VS Team focused on are: (i) only the VS Team members had access to the Voting Systems subfolder in which this Excel file (or copies thereof) are stored; and (ii) the Excel file itself, and any copies thereof, are password protected. Employee 7 himself requested that access to the Voting Systems subfolder be limited only to his team which request was granted and followed. The password is not written down and is known only to the VS Team members (or IT personnel on an as needed basis). Other cybersecurity features protecting this Excel file include the more general cybersecurity protections applied across CDOS, including, but not limited to, the use of encrypted laptops/computers for all staff and the use of log-on passwords that changed every ninety (90) days and two-factor authentication to gain access to CDOS computer equipment and servers. The password to access !NEW! Equipment Database, which was provided to the undersigned investigator, has not been changed for a long time. That password now has been changed as of the date this report is being issued.

A discussion regarding CDOS' password safe is warranted here. CDOS currently uses the LastPass password manager/password safe program. The LastPass software was introduced at a March 24, 2021, All Staff meeting. There are no written materials from that presentation. As noted above, CDOS's Acceptable Use Computing Policy ("AUP") states that Users should utilize the department provided password safe for department information or passwords. However, this policy is located in a section of the AUP titled "User ID and Password" and is situated directly between provisions directed only at passwords associated with an employee's User ID. However, an April 19, 2024, IT newsletter to all CDOS staff states that "You are encouraged to use LastPass to store your office passwords. LastPass is a password manager that can store all your passwords securely, so you don't have to worry about remembering them…. With LastPass you only need to remember one password, your Master Password, which is the key to the rest of your login credentials. All your passwords are stored in your own personal encrypted password vault." Employee 1 stated that he and other IT leadership have regularly communicated to CDOS employees a need to use the password safe for all CDOS log-in credentials. However, neither the written policy nor the communication demonstrate a requirement to store BIOS passwords (which are created and held by the VS Team but apply to county voting systems equipment and are different from CDOS log-in credentials) in the password safe. Elections Division employees interviewed did not understand there to be any type of requirement that BIOS passwords be stored solely in a password safe (as opposed to personal log-in credentials). Employee 1, Chief Information Officer, 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.

Hidden Worksheets (Tabs) In the Excel File Named !NEW! Equipment Database

At some point after Former Employee 1 migrated the VSI data from the Microsoft Access database into the Excel file named !New! Equipment Database, Former Employee 1 created four hidden worksheets (tabs) within that Excel file that are titled (i) Clean Formulas; (ii) OLD_ Equipment Database; (iii) OLD_ working; and (iv) OLD_ICXs within the database. Those hidden worksheets (tabs) contained BIOS passwords (recall that those BIOS passwords are also found in the eleventh column on the visible Inventory worksheet). Former Employee 1 used these hidden worksheets (tabs) solely for her own purposes. Former Employee 1 stated that they should be considered similar to "scratch paper" that were "functional to me" which she used to help her clean up the active VSI on the visible worksheet (tab) marked "Inventory." Former Employee 1 also used the hidden worksheets (tabs) to be able to provide responses to inventory queries. Former Employee 1 does not, after the passage of time, recall with any more specificity the nature or purpose of those worksheets. Former Employee 1 never told anyone that there were hidden worksheets (tabs) in the !NEW! Equipment Database Excel file that was used to track the statewide VSI. While this file was used and reviewed by the whole VS Team at various times, the hidden worksheets did not, according to Former Employee 1, serve any team-wide purpose and thus she would not be surprised that they would be unaware of their existence.

Former Employee 1 never had responsibility for posting the VSI on the Secretary of State's website and there is no evidence that she ever posted it.[10] In addition, the VSI was only previously posted as a .pdf file. Specifically, Employee 6, the Webmaster who was asked to review the Secretary of State's website's content management system[11] to identify all posted VSI documents, could only find two other VSI documents that had ever been published on the website: a .pdf file posted on December 7, 2020, and a .pdf file posted on November 6, 2023. The web request ticket requesting that the list be posted on November 6, 2023, shows that Employee 5 made that request. CDOS does not have web request tickets dating back to 2020 and therefore cannot identify who requested that the VSI be posted in December 2020. No one interviewed recalls the VSI ever being published in a format other than a .pdf file. Thus, it appears that the practice at the time Former Employee 1 was responsible for maintaining the VSI in !NEW! Equipment Database was to publish the VSI only as a .pdf. According to the forensic computer experts, when an Excel file is converted to a .pdf file, hidden worksheets (tabs) will not show up in the .pdf document and therefore will not be discoverable from the .pdf. Thus, Former Employee 1 had no expectation that the hidden worksheets (tabs) would become public.

The Subsequent/Other Custodians of !NEW! Equipment Database Excel File Were Unaware Of The Hidden Worksheets (Tabs) Within This File

On May 20, 2023, Former Employee 1 resigned her CDOS employment. Employee 5 was assigned the responsibility of maintaining the !NEW! Equipment Database Excel file after Former Employee 1 left, though all members of the VS Team accessed the file periodically. One transition meeting with Former Employee 1 occurred. No one recalls any specific discussions from the transition meeting. However, no remaining member of the VS Team (or any other person) was ever told about the hidden worksheets (tabs) in the !NEW! Equipment Database Excel file at the transition meeting or at any other time prior to October 24, 2024. Former Employee 1 specifically stated that she does not believe she informed anyone on the VS Team about the hidden worksheets (tabs). The remaining members of the VS Team also never discovered the hidden worksheets (tabs) prior to October 24, 2024, when they were brought to their attention. Thus, Employee 7, Employee 5 and Employee 4 were entirely unaware of the hidden worksheets (tabs) in the !NEW! Equipment Database Excel file being used to track the statewide VSI until it was brought to their attention on October 24, 2024.[12] Former Employee 1's position was not filled until April 2024 at which time

[10] While CDOS treats the VSI as a public document, there is no legal requirement to post the inventory list on the Secretary of State website. The list is published for purposes of transparency and was only published periodically.

[11] A content management system is a software application that allows users to publish, edit and otherwise management digital content on a website.

[12] Employee 7 does note that he does not believe Former Employee 1 intentionally hid the tabs. Thus, he acknowledges the possibility that she could have mentioned them, but he has no memory of that ever happening. Given Former Employee 1's statement that she does not believe she told the VS Team about the tabs, it is unlikely this ever happened.

Employee 3, the newest member of the VS Team, was hired. Employee 3 did not become aware of the hidden worksheets (tabs) prior to October 24, 2024. Further, no one on the VS Teams used hidden worksheets (tabs) as a practice in any other document and no one on the VS Team appeared to know that that worksheets (tabs) could be hidden. The undersigned investigator notes that she is a fairly regular user of Excel worksheets, and while she knows that columns and rows can be hidden, she was unaware, prior to this investigation, that worksheets themselves could be hidden.

After October 24, 2024, when CDOS was informed that an Excel file on the Secretary of State's website had hidden tabs containing BIOS passwords (discussed below), the VS team went back and also looked at the !New! Equipment Database Excel file and discovered that it, too, had the hidden tabs (discussed in more detail below).

The Excel File That Was Posted On June 21, 2024, Exposing Certain BIOS Passwords

As of June 20, 2024, the Secretary of State website contained a link to a VSI that was a .pdf file. As noted above, that file had been posted in November 2023. The VS Team intended to update the VSI on the Secretary of State website prior to the June 25, 2024, Colorado Primary Election. Prior to publication, Employee 5 wanted to make the list more user friendly to the public (sortable and more easily searchable) and, therefore, wanted to publish the list in its native file format as an Excel file rather than as a .pdf as it had historically been published. Employee 5 raised this matter with Employee 7. Employee 7 agreed that the VSI could be published as an Excel file to increase functionality to the public. At this point, although Employee 3 had been hired and was responsible for maintenance of the VSI Excel file, Employee 3 was so new that Employee 5 took the lead in preparing and publishing the VSI.

To prepare the VSI file to be posted to the Secretary of State website, Employee 5 made a copy of the !NEW! Equipment Database Excel file, named it "For Posting" and saved it to a 2024 State Primary folder in the Voting Systems/Equipment Inventory subfolder on the Elections Shared Drive. This is supported by the Varonis audit logs which reflect that Employee 5 accessed the !NEW! Equipment Database Excel file multiple times between June 18, 2024, and June 21, 2024, and that he created an Excel file titled "For Posting" on June 18, 2024. According to the forensic computer experts, when the !NEW! Equipment Database Excel file was copied, the hidden worksheets (tabs) contained in that file (which contained certain active BIOS passwords) were also automatically copied as well – still in the hidden format. In this new "For Posting" Excel file, Employee 5 deleted two other visible worksheets (tabs) titled "Disposed Of" and "Statistics." On the sole, remaining visible Inventory worksheet (tab), Employee 5 deleted the BIOS password column and three other columns (PEA Usage, Device Type and Disposal Status). Employee 5 removed the password encryption for the file and then protected the Inventory worksheet (tab) so that it could not be altered.[13] According to the Varonis logs, on June 21, 2024, 9:39 AM, the "For

[13] As confirmed by the forensic experts, an Excel file can be encrypted with a password, or a password removed, and a worksheet can be protected or changed back to unprotected status, in

Posting" Excel file was opened and renamed to "Inventory For Posting." Metadata in the Inventory For Posting Excel file also suggests that it was copied from the !NEW! Equipment Database Excel file. Specifically, the Created date found under the File/Info tab in "Inventory For Posting" is May 23, 2022, 8:51 AM, with Former Employee 1 as the author – the same Created date and time stamp, and author, as is seen in the !NEW! Equipment Database Excel file metadata. This is because, as noted above, when an Excel file is copied and Saved As a new file, as Employee 5 stated that he did here to create the For Posting file (renamed to Inventory For Posting before posting), the new file will retain the Created date – here, May 23, 2022 8:51 AM – of the copied file. Thus, the Excel file created by Employee 5 for posting can be traced back to the original file created by Former Employee 1 in which she created the hidden worksheets (tabs).

It should be noted that in every Excel file, under the File/Info tab, there is an "Inspect Workbook" function. This function, which is a form of metadata, actually informs the user whether hidden worksheets exist in the document (along with hidden columns or rows). None of the VS Team members or any person interviewed in connection with this investigation were aware of the "Inspect Workbook" function– other than one of the forensic computer experts, Expert 2, who specialized in Excel files. Expert 2 communicated that in his fifteen (15) years of computer forensic/ Excel experience, most non-experts he interacts with are unaware of the Inspect Workbook function in an Excel file. He noted that the only way to find the Inspect Workbook function is to use the File / Info tab and specifically look for the Inspect Workbook warnings. The Inspect Workbook information is not viewable on the Save or Save features of an Excel file.

Here, the Inspect Workbook function on the file actually posted to the Secretary of State website actually states:

> **Inspect Workbook**
> Before publishing this file, be aware that it contains:
> - Document properties, printer path, author's name and absolute path
> - Hidden rows
> - Hidden worksheets
> - Custom XML data
> - Links to other files
> - Active filters

The Website Posting Process

On June 21, 2024, at 9:39 AM (the same time the Varonis logs reflect that the "For Posting" file was renamed to "Inventory For Posting"), Employee 5 sent a web request (Web Request 3938),

---

one of two ways: (i) by selecting the Review Tab and selecting Protect Sheet or Protect Workbook and taking those steps, or (ii) by using the File / Info tab and selecting the Protect Workbook function and taking those steps.

also known as a JIRA ticket,[14] to the Web Requests & Content Management Team within the CDOS IT Department. That team is comprised of two Webmasters, Employee 6 and Employee 10. Employee 5's web request stated "Please replace the the [sic] PDF associated with Voting system inventory – 2023 (PDF) with the attached .xlsx document." Web Request 3938 reflects that the document attached to the web request is an Excel file labeled "Inventory For Posting."

As part of the website posting process, Employee 5's web posting request has to be approved by one of a number of authorized approvers before the Webmasters can post the document on the website. For example, Employee 9 and Employee 2 are authorized approvers. Employee 8 is also an authorized approver for Employee 5's request even though he works on a different team in the Elections Division (Ballot Access and Voter Registration). Employee 8 was the employee who approved Employee 5's web request. Approval requests for web requests (JIRA tickets) come through as an E-mail to all of the authorized approvers. The first authorized approver to respond approves the request. Here, according to the JIRA ticket, Employee 8 approved Employee 5's web request within one minute. Employee 8 simply clicked on the approval button without looking at the request or file to be uploaded. Within four minutes, Employee 10 uploaded the Inventory For Posting file to the website (and within ten or so minutes had relabeled the link to the file to reflect the current year, 2024). There is no policy, no directive and no written procedure for approving a web request. Employee 8 received no training when he became an authorized approver. Employee 8 understands that the approval step is a mere formality with no actual review required. Employee 9 and Employee 2 confirmed that there are no written or unwritten procedures or policies for approving web requests and that the approval is almost completely a ministerial act, short of simply noting whether the person requesting the post would have a reasonable reason to post an item. Some employees within the Elections Division assumed that the IT Division would review the documents for posting. On the IT side, there is an assumption that the authors of the content to be posted would review the materials to ensure it was suitable for posting before requesting posting. Of course, as it turned out, the Excel file posted to the website contained the hidden worksheets that were only accessible if the user knew to right click on the visible Inventory tab and click Unhide.

The Entire VS Team Was Unaware Of The Hidden Worksheets (Tabs) Within The Excel File That Was Posted To The Website

As the entire VS Team was unaware of the hidden worksheets (tabs) in the !NEW! Equipment Database Excel file, they were all equally unaware of the hidden worksheets (tabs) that had been automatically carried over to the file created by Employee 5 for posting and which contained certain BIOS passwords (only some of which were still active). On October 24, 2024, when the VS Team was alerted that certain active BIOS passwords could be found on the posted Excel spreadsheet on the Secretary of State website, the VS Team immediately requested that the webmasters take down the Excel file. The file was immediately taken down from the website by a

[14] JIRA is software used for IT project management.

Webmaster. The VS Team members searched the posted Excel file for the BIOS passwords. Initially, they could not locate the passwords. Only after Employee 5 began clicking on items in the Excel file, including the visible Inventory worksheet, (tab) did he and the VS Team discover the "Unhide" option that, when clicked, exposed the hidden worksheets (tabs).

There are a number of reasons the undersigned investigator concludes that no one on the VS Team, beyond former employee Former Employee 1, was aware of the hidden worksheets (tabs) in either the !NEW Equipment Database Excel file that they regularly used to track VSI, or in the Excel file posted to the Sectary of State website. First, I found the VS Team witnesses to be credible in their statements that they were at all times unaware of the hidden worksheets. Their collective accounts of what transpired are consistent and believable. Former Employee 1 herself explained that she did not tell her VS Team coworkers about the hidden worksheets. Employee 7 and Employee 5 sincerely described their belief in the importance of their work – facilitating secure and fair elections – and the importance of doing their job well. The "devastating" impact described by Employee 7 and Employee 5 that this disclosure has had on the VS Team, and on the health and well-being of particular individuals on the VS Team, was palpable during interviews. In addition, no one on the VS Team (other than former employee Former Employee 1) used hidden worksheets as a practice or knew hidden worksheets were an option in Excel. No one was aware of the Inspect Workbook feature. As stated by Former Employee 1, the hidden worksheets (tabs) did not have a VS Team purpose and, therefore, the VS Team had no reason to look for them. Finally, the steps that the VS Team took to secure the BIOS password data during the course of their jobs, and the steps Employee 5 took to eliminate the BIOS passwords from the visible Inventory worksheet before posting the VSI, suggest a sincere desire to maintain the confidentiality of the BIOS passwords which is contrary to an intentional, knowing or malicious disclosure.

In addition, a review of the BIOS passwords that were publicly disclosed on the hidden worksheets in the Excel file posted on the website that was conducted during this investigation by a CDOS Legal Policy Advisor and reviewed in detail by the undersigned investigator, suggests that the hidden worksheets had not been updated since Former Employee 1 left. More specifically, Employee 4 pulled a list of every trusted build that occurred after Former Employee 1 left her CDOS employment. For many of the Trusted Builds on that list, neither the new equipment nor the associated new BIOS password was listed on the hidden worksheets. They were, however, listed on the visible Inventory worksheet in the !New! Equipment Database file. If the equipment and BIOS password from the new Trusted Build lists prepared by Employee 4 did appear on the hidden worksheets posted on the website, that equipment had already existed and been subject to a Trusted Build before Former Employee 1 left. As noted above, if a Trusted Build is conducted on an existing (not new) voting systems component (e.g., for a software upgrade), the BIOS password from the earlier Trusted Build is retained (and thus would still appear on the hidden worksheets even though the Trusted Build occurred after Former Employee 1 left). The lack of updating to the hidden worksheets when the visible worksheet had been updated also suggests that no one on the remaining VS Team knew the hidden worksheets existed.

Thus, the substantial weight of the evidence demonstrates that the BIOS passwords contained in the hidden worksheets posted on the Secretary of State website were posted mistakenly, unknowingly and unintentionally because the VS Team was unaware the hidden worksheets existed.

IV. Conclusions Regarding Potential CDOS Policy/Procedure Violations

1. A series of inadvertent and unforeseen events led to the public disclosure of the BIOS Passwords. However, the failure to review the posted document to ensure that non-public information would not be disclosed violates a Colorado Information Security Policy on publicly accessible content issued by the Governor's Office of Information and Technology. That policy is made applicable to CDOS through CDOS' own AUP. In reaching my conclusions about potential policy violations, consideration was given to all of the following issues.

a. The facts presented raised the question as to whether the VS Team's practice of storing BIOS passwords in the !NEW! Equipment Database Excel File (or Former Employee 1's practice of having BIOS passwords on hidden worksheets within that file) violate the following CDOS Acceptable Use Computing Policy ("CDOS AUP"): "Users should utilize the department provided password safe and are not permitted to use any other personal password safe for department information or passwords." *See § Ex. C III(b)(iii)(1)(c).* While the policy does state that Users should utilize the department provided password safe for department information or passwords, this policy is located in a section of the CDOS AUP titled "User ID and Password" and is situated directly between provisions directed only at passwords associated with an employee's User ID. Neither the policy regarding the password safe, nor any communications reviewed by the investigator regarding the same, mandate use of the password safe for passwords such as the BIOS passwords which are kept and safeguarded by the VS TEAM and are applicable to voter systems equipment owned by the counties. While the password safe would have been an available option to store the BIOS passwords, the storage of the BIOS passwords outside the password safe is not a policy violation. In fact, Employee 1, Chief Information Officer, CDOS, stated that storing the BIOS passwords in a file on the CDOS server (with its layers of protection) with properly complex password protection is an acceptable alternative to use of the password safe.

b. The facts presented also raised a question as to whether Former Employee 1's decision to create hidden Excel worksheets containing BIOS passwords on a secure, confidential, and password protected document without ultimately disclosing the existence of those worksheets to the other members of the VS Team violates the State's Acceptable Use of State Data & IT Resources Policy (CISP-018) which requires that Users take precautions to protect against the unauthorized or careless disclosure of sensitive information, or the CDOS AUP's general requirement to use computer systems responsibly. Former Employee 1's actions did ultimately lead to the posting and public disclosure of BIOS passwords. While Former Employee 1's failure to eliminate or disclose the hidden worksheets to the VS Team prior to her departure arguably could be deemed a failure to take precautions to protect against unauthorized or careless

disclosure, the file containing the hidden worksheets was subject to a significant number of appropriate security measures described herein and was treated securely and confidentially by Former Employee 1. Former Employee 1 had no reasonable expectation that the file would ever be publicly disclosed in its native format. As a result, the investigator finds that Former Employee 1's conduct did not violate these policies.

c. The facts presented also raised a question as to whether the Secretary of State or CDOS itself violated the general policy under CISP 010 that requires all Data Stewards to ensure that the State's data is safe in accordance with governing data compliance requirements or violated any specific compliance requirement. The investigator finds that this unique set of circumstances would have been difficult to anticipate. Further, on an organizational level, the Secretary of State/CDOS consistently took significant and appropriate measures to protect state information, including the BIOS passwords. This is reflected in the promulgation of the CDOS AUP and other policies, the VS Team's overall efforts to protect the data, the other general CDOS IT precautions identified above and many, many other steps CDOS takes on a daily basis to protect the integrity of its information that are beyond the scope of this report. However, CISP 001-9.15 requires Data Stewards[15] such as the Secretary of State and CDOS to train authorized individuals to ensure that publicly accessible information does not contain non-public information and to review the proposed content of information prior to posting onto the publicly accessible Information System to ensure that non-public information is not included. While Employee 5 did remove the visible BIOS passwords from the Excel file prior to submitting it for posting as he knew he was responsible to do, he did not have the skill set to ensure that non-public information was not included in that document in hidden files or metadata and no person reviewed the document for the hidden non-public information prior to posting. Thus, while in all other respects reviewed by this Investigator the Secretary of State and CDOS ensured that the BIOS passwords were safe, in that regard I find that CISP 9.15.2 and 9.15.3 were violated.

2. There are violations of existing CDOS policies which occurred that did not lead to or result in the public disclosure of the BIOS passwords.

a. Specifically, while it was appropriate to place password protection on the !NEW! Equipment Database Excel file containing the BIOS passwords, the password did not meet the CDOS guidelines for password strength and should have been changed at a set interval. The password now has been changed and upgraded in strength. The failure to meet password strength guidelines or to change the password at a set interval did not lead to or result in the public disclosure of the BIOS passwords.

---

[15] A Data Steward is defined as "The Agency/Business Owner." *See* CISP 001-7(n). An Agency is defined as "public agencies as defined in C.R.S. 24-37-5-102(26). *See* CISP 001-7(b). C.R.S. § 24-37.5-102(26) defines a "public agency" as "every state office, whether executive or judicial, and all of its respective offices, departments, divisions, commissions, boards, bureaus, and institutions.

b. Further, it appears that CDOS may not be requiring review and signature by its employees on the Acceptable Use Policies promulgated by CDOS or the State. This failure did not lead to or result in the public disclosure of the BIOS passwords.

V. Recommended Changes To Existing Policy To Prevent Any Such Future Public Disclosures.

There are a number of potential policy or procedural changes (see, in particular, paragraphs 1 through 5) that, if put in place, should reduce the risk of any future, inadvertent disclosure of confidential information. There are other policy or procedural changes that should be considered in order to improve communications and understanding of CDOS policies (see, in particular, paragraphs 6 and 7). These changes should be evaluated for adoption by CDOS.

1. CDOS should consider creating a substantive review process for the Elections Division (and, possibly, other Divisions) associated with its existing approval requirement for web requests involving posting to the Secretary of State website. CDOS should consider including in that review process a checklist of items to be reviewed, including but not limited to: (i) discerning whether the document contains confidential or sensitive data or any kind; (ii) discerning whether the document contains hidden data of any kind; (iii) discerning whether the document contains links of any kind; (iv) eliminating metadata from the document (for example, in addition to the BIOS passwords, employee names are contained within metadata of the posted document); and (v) considering whether documents should be posted in .pdf format or native file format and the associated risks. CDOS should consider what contributions, if any, could be made to this process from the CDOS IT side of the house before posting. This process could include use of the Inspect Workbook or Inspect Document features in Excel and Word documents.

2. CDOS should consider instituting a policy prohibiting the use of the "hide" functions for highly sensitive or confidential information within documents (or requiring such files to be labeled as containing hidden tabs) to avoid inadvertent disclosure. CDOS should consider providing direction, now, to all staff to eliminate, or at least flag, any known hidden data from documents.

3. CDOS should consider a requirement that all passwords of any kind, whether they be individual user log-in credentials or password information such as the BIOS passwords, be kept only in a password safe unless an exception to that policy is granted in writing by the CDOS IT Division or other approving authority.

4. CDOS should consider requiring employees to be better trained on the data protection features of the computer software programs that are used on a daily basis, such as the Inspect Workbook and Inspect Document feature of Excel and Word documents.

5. CDOS should consider a review of the transition and exit process for departing employees whose responsibilities involve handling sensitive or confidential information to include a specific discussion of where such information is located and exactly how such information has been handled by the departing employee.

6. CDOS should consider updating the CDOS AUP so that the policy on the use of the password safe and the policy on creating and managing passwords are single stand-alone policies rather than policies contained at various places within the User ID and Password section of the AUP. Those stand-alone policies can be referenced within the User ID and Password section for clarity, if necessary. In any potential revision of the AUP, CDOS should consider more specifically defining the scope of the information to which the password safe policy applies and clarify whether the password safe policy is mandatory (aside from exceptions). In any revision, CDOS should also consider making clear, in the password creation and maintenance policy, that all passwords (not just network log-ins) need to be updated at some set interval. The investigator recognizes that this type of password creation and maintenance information has been provided in training material.

7. CDOS should consider requiring its employees to review its AUP policy every year and sign that they have reviewed the document, not just when the document is updated or when an employee first becomes employed with CDOS.

Please feel free to contact me if you have any questions or concerns regarding the information above.

Respectfully submitted,

BAIRD QUINN LLC

Beth Doherty Quinn

Beth Doherty Quinn, Esq.