NOTE TO FILE

☒ **WORK PRODUCT**

December 17, 2024

Investigator: Senior Criminal Investigator Cory Brodzinski, DA86

RE: Suspect: **Employee 5**
Case Number: D0162024TM000329

Lead Charge: CRS 1-13-708(2) Knowingly Causing Voting System Passwords to be Published (F5)

This is a chronological report of the investigative steps that were taken. It may not include all steps or actions taken to investigate the publication of voting machine BIOS passwords on the Colorado Department of State website. The scope of this investigation is limited to whether the BIOS passwords were knowingly published on the website and if there was any official misconduct on the part of any CDOS employee. Response to the discovery of the passwords, actions taken by the CDOS outside of the publication of the passwords, whether the BIOS passwords were used to access voting machines, who may have seen or downloaded the passwords, and/or the security of the election are not being investigated.

Friday, November 1, 2024

Inv. Brodzinski was contacted by Chief Investigator Garner and requested to investigate passwords to voting machines being published on the Colorado Secretary of State's website. The scope of the investigation will be whether the passwords were knowingly published and if there was a violation CRS 1-13-708(2). This statute states: "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." The investigation will also be focused on whether there was a violation of CRS 18-8-405(1), which states: "A public servant commits a second degree official misconduct if he knowingly, arbitrarily and capriciously: (a) Refrains from performing a duty imposed upon him by law or (b) Violates any statute or lawfully adopted rule or regulation relating to his office."

Monday, November 4, 2024

Around 9:00 AM, Inv. Brodzinski called Deputy Secretary of State Employee 11 to inquire about this event. Employee 11 was friendly and cooperative and offered to provide any necessary information. He was, however, in the process of preparing to testify in a lawsuit later this same

day and declined to take the time to speak to me now. We scheduled a follow-up call for 9:00 AM on November 5, 2024.

That lawsuit was brought by the Libertarian Party of Colorado (24CV33363) and heard in Denver District Court courtroom 275 before the Honorable Judge Kandace Gerdes. The trial was live streamed on the court's website beginning around 1:30 PM, and Inv. Brodzinski watched, hoping to learn the facts of the case.

From the trial testimony, Inv. Brodzinski learned the passwords in question were on hidden worksheets in an Excel spreadsheet workbook and that they were passwords to the voting machine system BIOS. From training and experience, Inv Brodzinski knows that BIOS is an acronym for Basic Input/Output System, and it is essentially the framework on a computer that is the bridge between the hardware and software of that computer.

Inv Brodzinski is very familiar with Excel spreadsheets and knows it is simple to hide worksheets in a workbook, a collection of worksheets saved with the same file name. To hide or unhide a worksheet, one only has to right-click the worksheet tab and select hide. To unhide a worksheet, right-click on the visible worksheet and select unhide.

Tuesday, November 5, 2024

Inv Brodzinski called Employee 11 at 9:00 am for a follow-up interview. The call lasted approximately 30 minutes. The following was learned about how the spreadsheet with passwords came to be posted online.

The posted spreadsheet is a Microsoft Excel xls file named "Voting System Inventory." During this conversation, Employee 11 said that by rule or statute, the Secretary of State's Office (Colorado Department of State/CDOS) must post a list of all voting equipment in Colorado on its website. The spreadsheet was posted to comply with that rule. The equipment listed on the inventory includes such things as ballot scanners and ballot marking devices, which visually impaired people use for casting their ballots. Inv Brodzinski understood that the equipment in the inventory is generally used for counting or tabulating paper ballots, and it did not include the machines people interact with for in-person voting.

Employee 11 said there are two vendors for these machines in Colorado- Dominion Voting System and Clear Ballot. The state is required to post a list of their equipment for each county on the CDOS website.

On June 21, 2024, the Voting System Inventory was published as an Excel spreadsheet on the CDOS website. This was the first time it's believed to have been posted as a spreadsheet. All previous times it was updated, it was provided as an Adobe Acrobat Portable Document File (PDF). Employee 11 stated it was posted as an xls at the request of Voting System Team manager Employee 7. Employee 11 believes Employee 7 intended to publish it as an XLS instead of a PDF, as it is a more helpful file type for searching, sorting, and ordering data.

Employee 11 believes Employee 7 was trying to be helpful to the end users by providing a more useful file type to work with.

According to Employee 11, Employee 7 did not publish the file on the website himself. He believes that Employee 7 submitted a work request ticket to the office's web team, who would, in turn, have uploaded the file to their website.

Employee 7 does not maintain the Voting System Inventory file; Employee 5 currently does. Employee 5 took over this file from Former Employee 1 (aka, Former Employee 1), who voluntarily separated from the CDOS in May 2023. Employee 11 said Former Employee 1 [redacted]. Employee 11 did not know [redacted] but believed [redacted]. Employee 11 will ask their human resources department for other identifying or contact information. He thought Former Employee 1's [redacted] name might be "Former Employee 1" or something similar.

Employee 11 believes neither Employee 7 nor Employee 5 knew the Voting System Inventory file contained hidden worksheets, most of which were created by Former Employee 1. They had no reason to suspect the file contained hidden worksheets with passwords, so Employee 7 saw no risk in posting it as an XLS instead of the usual PDF format.

On the afternoon of October 24, 2024, Clear Ballot personnel contacted Employee 7 to inform him that the spreadsheet online had BIOS passwords for voting machines. Employee 7 was in a meeting and did not answer the phone, so Clear Ballot called Employee 12 next to inform him. Employee 12, in turn, called Employee 10, the elections director. Clear Ballot also called Dominion Voting Systems to tell them, who also called Employee 10.

Employee 10 then called Employee 11, who informed Employee 1, the CDOS's IT Director. Employee immediately removed the file from the website. Employee 10 also told the United States Department of Homeland Security Cybersecurity and Infrastructure Security Agency. Employee 11 called John Poulos, CEO of Dominion Voting Systems. Employee 11 said everyone involved was working to identify if the published passwords had been used to access any voting machines or if the machines had been compromised because of the passwords.

Employee 11 said there is no evidence that passwords were used or that machines were compromised. He also said some passwords were very old—the file had not been updated since before Former Employee 1 separated from the CDOS in May 2023. There were no passwords for the voting machine put-in service after May 2023, and the list published included approximately 650 passwords on three separate hidden worksheets. Employee 11's investigation determined that approximately 255 machines used in various counties had passwords in the published list. Forty-six counties have machines where the BIOS password was in the published file.

Employee 11 said CDOS personnel spent the following days, through just before midnight on October 30, accessing all the impacted machines and changing the BIOS passwords of the devices on the published list.

Employee 11 does not believe Former Employee 1 had unlawful intentions when she added the hidden worksheets to the Voting System Inventory list. Instead, Employee 11 believes it was poor cybersecurity and information security practice to keep the passwords attached to the same list as the actual devices. Employee 11 described it as "sloppy" but likely not criminal.

At 4:38 PM, Inv. Brodzinski received an email from Employee 11 with contact information from Employee 7 and Employee 5 and the last known contact info for Former Employee 1.

Wednesday, November 6, 2024

Inv Brodzinski received an email from Employee 11 requesting a phone call, saying he had additional information to provide. Inv Brodzinski called Employee 11 around 8:15 AM.

Employee 11 provided additional information related to the workflow within their IT system. He said that after we spoke yesterday, IT Director Employee 1 learned that Employee 5 had requested a work ticket in their Jira system on June 21 to upload the Voting System Inventory spreadsheet. On October 24 at about 1:45 PM, Employee 7 sent a Teams message to an IT department employee and requested that the file be taken down. This was not the standard procedure for IT work requests- Employee 7 did not submit the request via Jira. The receiving IT employee copied the Teams message into a work ticket they created, completed the ticket by taking the file down, and closed it about 15 minutes later.

Inv. Brodzinski requested that Employee 11 provide him with copies of both work tickets and the related Teams messages. Employee 11 said he would provide those. They were received via email around 11:47 AM, and Inv Brodzinski saved them for the case on Evidence.com. Later that day, Inv Brodzinski received a call from the IT Director Employee 1. Employee 1 explained how the work tasks occurred and offered his opinion on why the inventory file was uploaded as a spreadsheet in June instead of as a PDF as it usually was.

Employee 1 stated that CDOS employees were under guidance to make public documents as accessible as possible. He did not elaborate on how a document was made accessible or what characteristics would indicate it was accessible. Employee 1 opined that Colorado state government employees are under significant pressure to make publicly viewable documents accessible and that it is easier to make a spreadsheet file accessible than to make a PDF document accessible. Employee 1 thinks that pressure, plus internal pressure with the then-upcoming primary and general elections, caused Employee 5 to request posting the document as a spreadsheet and not as a PDF as had been done previously.

Further, Inv Brodzinski knows from experience that when an Excel spreadsheet is converted to an Adobe PDF, only the first worksheet tab is converted; the other tabs, hidden or unhidden, do

not get converted and do not appear in the resulting PDF. Given this, Inv Brodzinski thinks it is possible that those hidden sheets were present in the file long before Employee 5 was responsible for it and were never posted publicly in the past because the inventory had always been posted as a PDF in the past.

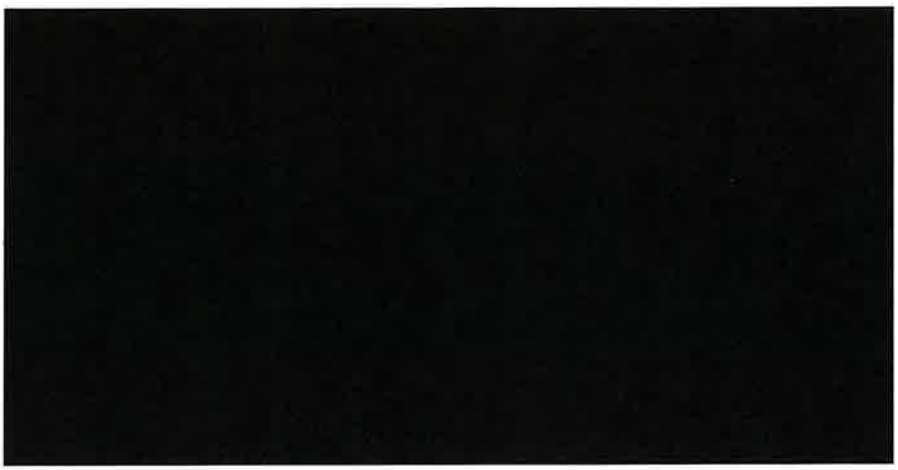
Employee 1 offered to provide records and files that would be of use to this investigation, to include an original copy of the "Voting System Inventory.xls" file. Inv. Brodzinski provided him with a community request link in Evidence.com to share those files. Employee 1 provided those records, and they will be reviewed.

Employee 1 discussed the acceptable use of password guidance that employees must follow. This includes using secure passwords comprising unrelated words or phrases, as well as numbers and symbols. He further stated that using LastPass or other password management systems is preferred. He said the method in which these BIOS passwords were stored- in hidden sheets within the same documents as the machines they go to- was not an acceptable form of password management. He seemed to generally agree this was due to laziness by the employee who stored them there.

Inv Brodzinski investigated Former Employee 1's [redacted] based on the date of birth provided by Employee 11 and the possible use of the first name Former Employee 1. Using the CLEAR database, Inv Brodzinski found Former Employee 1, whose date of birth was [redacted], and who is now likely residing in [redacted]. CLEAR showed an address of [redacted]. Inv Brodzinski next checked [redacted] driver's license records and found Former Employee 1 with a listed address of [redacted]. Sex is listed as female, with the same date of birth as Former Employee 1, and the license was issued on [redacted].

Inv Brodzinski next searched for publicly viewable Facebook profiles for Former Employee 1 and located a profile named "Former Employee 1" at URL: [redacted] The public information states they live in [redacted]. The last public posting was on [redacted]. Preservation of this profile was requested via Facebook LERS.

Based on these facts, Inv Brodzinski believes Former Employee 1 is now Former Employee 1, residing at [redacted]. A Google Street View check shows this is likely a valid street address. The side-by-side comparison photos of Former Employee 1's [redacted] driver's license photo and the profile photo from Former Employee 1's Facebook profile show they are very likely the same person.



Thursday, November 7, 2024

Denver DA case number 24TM0329 was assigned to this case. A case was opened in Evidence.com to store records received.

At 8:22 AM today, Inv Brodzinski received an email from Employee 11 in which he stated, "We have advised them of your interest in speaking with them, and they indicated that they wished to confer with legal counsel. We have indicated to both Employee 5 and Employee 7 that the AG's office cannot represent them in a criminal investigation but that the office would pay for outside independent legal representation should they wish to have such. I do not yet know whether either Employee 5 or Employee 7 have been successful in engaging counsel.

In any event, I understand that both Employee 5 and Employee 7 are expecting a call from you."

Around 9:30 AM, Inv Brodzinski and DA Investigator Daniel Hines attempted to interview Employee 7 at his home in [redacted]. His driveway and sidewalk had been cleared of most snow, except what seemed to be falling at the time. Cars in the driveway had snow on them, and the license plate of a [redacted] in the driveway was registered to Employee 7. Inv Brodzinski rang the doorbell twice, and investigators waited approximately 5 minutes at the front door for an answer. No one answered the door, but a dog could be heard barking loudly inside. Inv Brodzinski left his business card in the door.

A records preservation request was emailed to Employee 11 at 12:11 PM. At 12:20 PM, he replied via email and confirmed receipt of the request. A copy of that request letter is stored with this case file. No records were requested, only a letter requesting preservation.

Inv. Brodzinski searched within NCIC for criminal histories for [redacted] and [redacted]. No criminal history was found for [redacted] or [redacted] was found to have a criminal history in [redacted] and [redacted], with the most recent event being over 20 years ago. The criminal history records were saved in the case file.

Friday, November 8, 2024

Inv Brodzinski reviewed the files provided by Employee 1. Six documents were provided.
"Acceptable Use Computing Policy 9-15-07"

This document discusses the CDOS computer use policies, security and password expectations, and computer use restrictions. It emphasizes the need for secure passwords and the expectation that employees do not share passwords. Employees are expected to sign a statement acknowledging these acceptable uses and restrictions.

"All Staff Meeting Notes_3.24.21 – final.docx"

This document is the "All Staff Meeting Agenda" from March 24, 2021. Item #10 on the agenda is attributed to [redacted] and is titled "LastPass password manager." Inv Brodzinski believes this is when the expectation to use a password management system was conveyed to CDOS staff.

"AUP Acceptable Use Policy-Docusign.docx"

This document appears to be the copy of the Acceptable Use document discussed above that employees are expected to sign.

"Emails to Office.docx"

This document appears to be a summary of cybersecurity tips and directives sent to employees of CDOS. It is not the original emails themselves, but notes on dates of emails and what they contained with respect to password storage. It specifically mentions the use of LastPass.

"Employee 1Notes.docx"

This document appears to be Employee 1's notes tracking their response to the discovery of the passwords being posted online. This document is lengthy and will not be reiterated here, please see case file for the original document. The notes discuss the response to take down the spreadsheet and getting the BIOS passwords changed. It does not contain information about when or how the document was posted originally. It does state that on October 25, 2024 at 7:00 AM Employee 1 found that 158 unique IP addresses has accessed the Voting Systems Inventory since June 21, 2024.

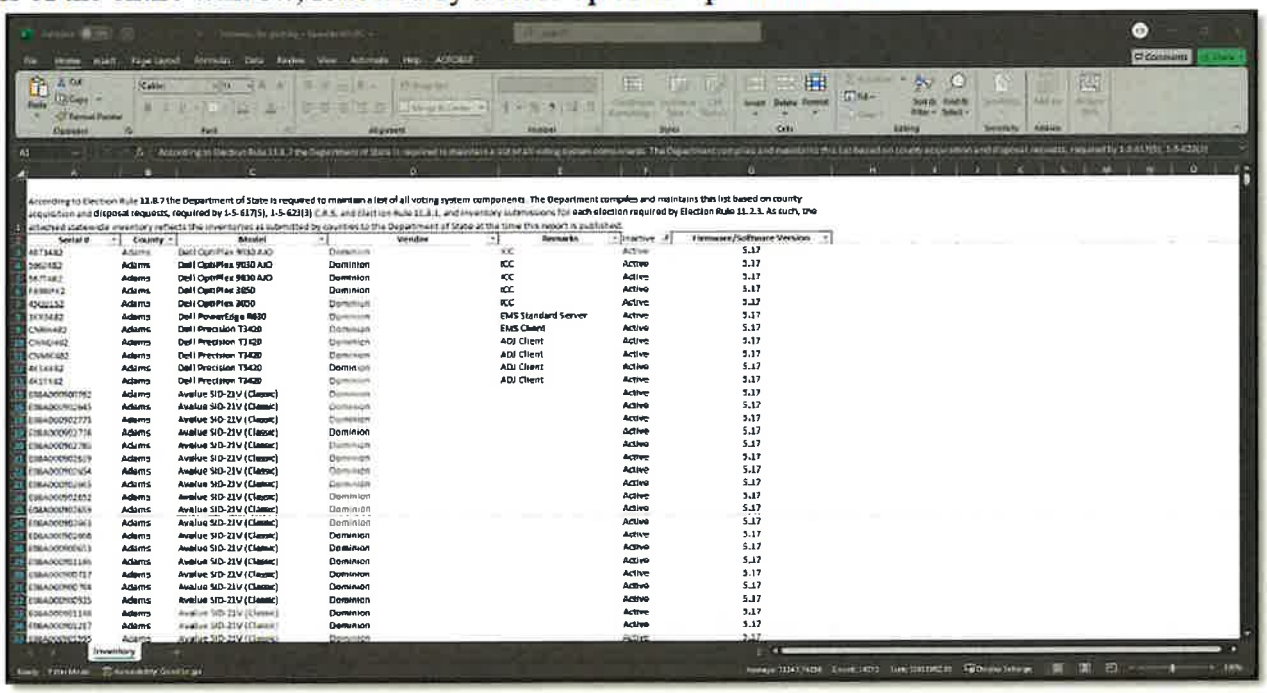
By decompressing the .docx file, the underlying document properties were able to be viewed. Inv Brodzinski reviewed those properties and determined it was created by Employee 1 on October 25, 2024 at 12:55:00 Zulu time. It was last modified on November 5, 2024 at 17:40:00 Zulu time. Inv Brodzinski knows Zulu is an alternate term for UTC and that on October 25, 2024,

UTC was 6 hours ahead of local time in Denver, Colorado. Due to daylight savings time ending, UTC was 7 hours ahead of local time in Denver, Colorado on November 5, 2024.

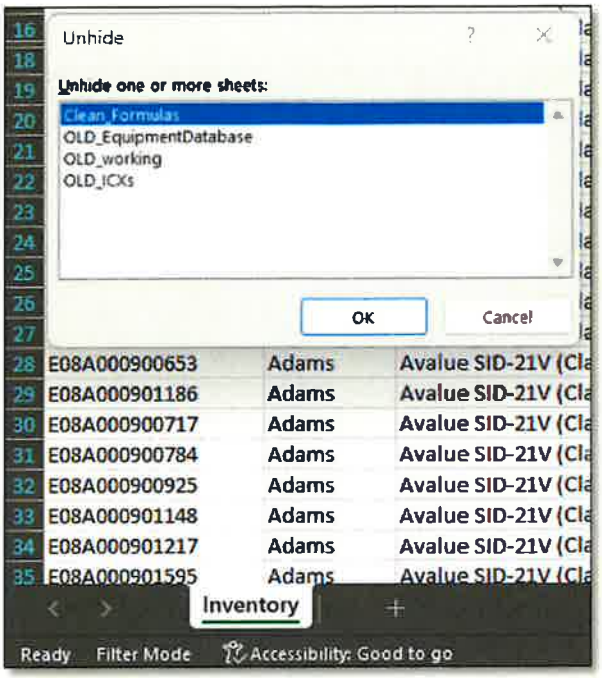
"Inventory for posting.xls"

This appears to be the original xls spreadsheet that was posted with the hidden sheets of passwords on June 21, 2024. In a similar manner as above, Inv Brodzinski reviewed the documents properties. It was created by Former Employee 1 on May 23, 2022 at 14:51:39 Zulu (May 23, 2022 8:51:39 PM local time in Denver, Colorado). The document was last modified by Employee 5 on June 20, 2024 at 16:14:20 Zulu (June 20, 2024 10:14:20 AM local time in Denver, Colorado).

As first opened, the document displays one spreadsheet- see screen capture below. The first one is of the entire window, followed by a close-up of the spreadsheet tabs.



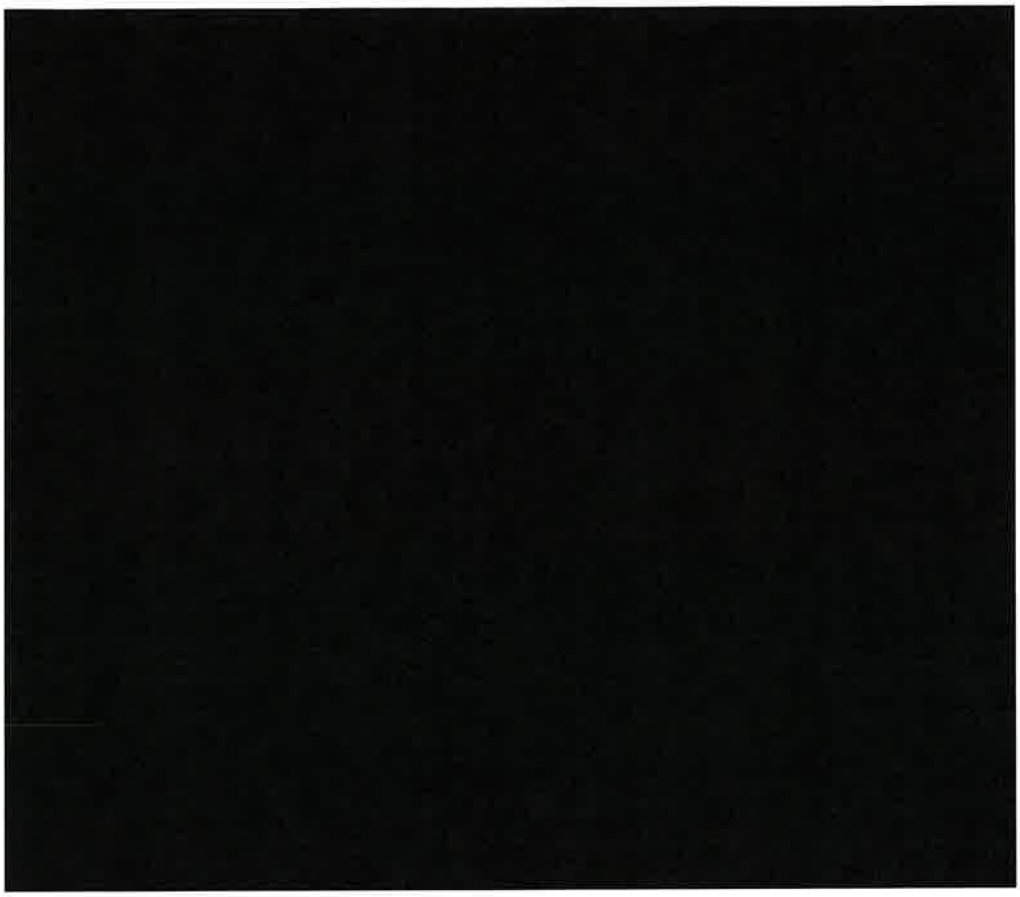
If the user right-clicks on the Inventory tab, a pop up window allows the user to "unhide" other sheets, as displayed below.



If all of those sheets are selected, they become visible to the right of the Inventory tab, as shown below.

The three sheets that then become visible are labeled 'Clean_Formulas,' 'OLD_EquipmentDatabase,' 'OLD_working,' and 'OLD_ICXs.' Of these, all of them except OLD_ICXs contain a column with BIOS passwords. This is all as expected from conversations with CDOS personnel.

Around 10:00 AM, Inv Brodzinski reviewed the publicly viewable portion of Former Employee 1's Facebook profile and noted that on [redacted] she posted a link to a video on YouTube.com titled "[redacted]." The image in the link was of then-President Donald Trump and his wife dancing in a large hall, ostensibly them dancing at an Inaugural Ball after his first Inauguration. Below is a screen capture of this posting.



Inv Brodzinski followed the link in the posting to YouTube.com, where the video is hosted. It is posted at URL: [redacted] on a channel named "[redacted]"

Inv Brodzinski watched the entire video, which was 52 seconds long. The video is of the then-President and First Lady dancing in formal attire on a stage with onlookers, seemingly in a large concert hall. It is set to jazz music. The video is displayed as being viewed 81 times and was posted 7 years ago. There are no comments and the description states: [redacted]" and says the music is "Dance of the Dream Man (Instrumental)" by Angelo Badalamenti. It is from the soundtrack to the TV show Twin Peaks.

Inv Brodzinski checked the "About" page for the YouTube channel and found there was only one subscriber and only the one video shared. The About page is located at URL: [redacted]

Around 11 AM, Inv Brodzinski began reviewing the Jira work tickets that Employee 11 emailed on November 6, 2024. Four tickets were received as PDF's, apparently screen captures from the Jira system. In his email to me about these Jira tickets, Employee 11 wrote, in part:

"Attached here are the Jira tickets that I mentioned to you this morning.

Also copied on this email is our CIO Employee 1, who can walk you through the sequence as follows:

1. *WEB-3938 Update Voting Systems Inventory – Web Requests.pdf*

June 21, 2024, request by Employee 5 to post .xlsx file to the Voting Systems Inventory URL

2. *WEB-4396 Remove voting systems inventory file.pdf*

Oct. 24, 2024, ticket created by Employee 6 based on IM message from Employee 7

3. *WEB-4401 Post clean Voting System Inventory.pdf*

Oct. 25, 2024, request by Employee 5 to post a clean version of the .xlsx file to the Voting Systems Inventory URL

4. *WEB-4439 Publish new version of voting system inventory file.pdf*

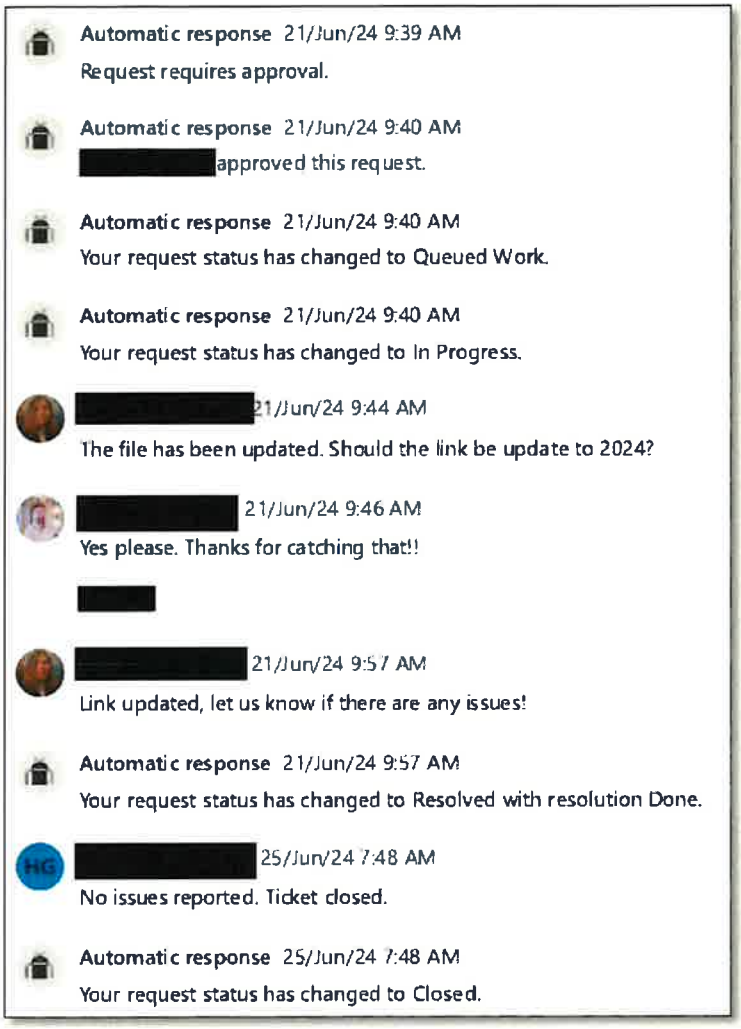
Nov. 1, 2024, request by CISO [redacted] to post a new version of the .xlsx file to the Voting Systems Inventory URL"

The Jira work request tickets will be reviewed below.

"WEB-3938 Update Voting Systems Inventory – Web results.pdf"

This file appears to be the original work ticket submitted by Employee 5 to upload the "Voting System Inventory.xls" file to the CDOS website. The ticket was created ('raised') on June 21, 2024 at 9:39 AM by Employee 5. He requested: "Please replace the PDF associated with Voting system inventory – 2023 (PDF) with the attached .xlsx document. Thanks!"

The screenshot below is from this work ticket and shows the timeline of work done at Employee 5's request. Employee 8 approved the upload, and it seems Employee 9 fulfilled the request. The work request was closed on June 25, 2024 at 7:48 AM.



"WEB-4396 Remove voting systems inventory file.pdf"

This file appears to be a Jira work ticket created by Employee 6 on October 24, 2024 at 2:00 PM. The description reads as if she created it on behalf of Employee 7, who sent his actual request via Teams message. That message is in the below screenshot.

Description

Urgent request via IM from [redacted] 1:46 PM

Hey, ladies. I know this isn't the right way to do this, but can you please remove the inventory on https://www.sos.state.co.us/pubs/elections/VotingSystems/VSHomePage1.html. It apparently contains hidden info and needs to be pulled down ASAP!

At 2:03 PM, Employee 6 commented on the work request: "Link removed from page and file deleted 1:49 PM." It is unclear how Employee 6 could have removed the file before creating the work ticket. Inv Brodzinski speculates that because the work request came via Teams and not directly via Jira, Employee 6 did the work and then went back and created the ticket to document the work after it was done. The work request was completed and closed on October 24, 22024 at 2:32 PM.

"WEB-4401 Post clean Voting System Inventory.pdf"

This file appears to be a Jira work request created by Employee 5 on October 25, 2024, at 9:33 AM. The description of the requested work is in the screenshot below, but he appears to be requesting a copy of the Voting System Inventory file be uploaded to the CDOS website.

Description

Can you please add a link entitled Voting system inventory - 2024 (.xlsx) under the certified systems tab and associate it with the attached spreadsheet?

Thanks!

PER [redacted]. This must have approval from [redacted] OR [redacted] before posting.

At 10:06 AM, Employee 1 commented in the ticket that "the new version is approved for posting," but at 10:09 AM, he commented, "Another version will be ready in 5 minutes. Sorry." Employee 5 provided the next version at 10:10 AM.

Employee 6 closed and completed the ticket on "Thursday at 7:26 AM." It is unclear what date Thursday refers to, but it is likely Thursday, October 31, 2024.

"WEB-4439 Publish newer version of voting system inventory file.pdf"

This file appears to be a Jira work ticket created by [redacted] on "Friday at 10:05 AM." It is uncertain what date Friday refers to, but it is likely Friday, November 1, 2024. [redacted] has requested that a newer version of the voting system inventory be re-published. See the screenshot below.

Description

This is a request for [redacted] web team to re-publish the voting system invientory spreadsheet at https://www.coloradosos.gov/pubs/elections/VotingSystems/VSHomePage1.html

I'll drop the latest version of the document in here in a few minutes.

At 11:50 AM, Employee 6 wrote in the ticket that she had uploaded the file at 11:03 AM.

Tuesday November 12, 2024

Inv Brodzinski reviewed Employee 11's response to a question sent on Monday, November 8, 2024. Inv Brodzinski had requested a list of all the counties impacted by these passwords being published. Employee 11 provided a file labeled "County equipment list, with assignment (cpb review).pdf." Inv Brodzinski put this file in Evidence.com on November 12, 2024. In his response, Employee 11 wrote:

"No worries. This request is pretty straight-forward.

The attached file gives you the names of the 46 counties (out of the 63 named in the hidden tabs of the 6/21/2024 posted version of the VotingSystemInventory.xlsx file) where the county still had a machine whose password was included on those hidden tabs.

For 12 counties, there was only one machine in each that had a disclosed password, and we confirmed that in each of those 12 counties, the one machine was not in use.

The remaining 34 counties had varying numbers of machines with disclosed passwords – with a total of 255 machines across those 34 counties.

The attached document names and lists the counties, the number of machines, and then when the passwords were changed."

Inv Brodzinski emailed DA Beth McCann a modified version of this list on Friday, November 8, 2024, at 1:23 PM. The file was modified only to show the directly impacted counties (34 of them) and how many machines are in each county (255). Counties with inactive machines were not included.

Around 9:45 AM, Inv Brodzinski began to review Employee 11's response to another email sent to him on November 8, 2024. Below is his response, where he included the questions I asked:

"*Personnel questions:*

- *Was former employee Former Employee 1 responsible for maintaining the inventory spreadsheet? Generally, yes, but this is a question you should explore with the supervisor of the voting systems team, Employee 7. The team generally functioned as a cohesive unit with all of the team working on all of the team's tasks. We understand that Former Employee 1 had primary involvement with the Voting Systems*

Inventory file, and this responsibility does appear in the formal personnel system position description for the position that Former Employee 1 held. (Copy attached – Former Employee 1 held position #189 in the Department.) But, it seems likely that others also were involved in working on the document from time to time even while Former Employee 1 was responsible for it. Of note, the responsibility for maintaining the inventory moved from Employee 5's position description to Former Employee 1's position description in October 2022.

Employee 1's team is currently working to find the internal location where that file was stored on our network, and to ascertain whether we can reconstruct the version history of that file. This work will also show whether other team members had access to the file (i.e., did they have system permissions for the location where the file was stored) and whether they actually modified the document and when.

- *Did Employee 5 take over that responsibility from Former Employee 1?*
  This is also a question that should be explored with Employee 7. Employee 5 was initially responsible for the Voting System Inventory file before Former Employee 1 took over that responsibility in October 2022. When that shift occurred, Employee 5's duties because more focused on other activities of the voting systems team. When Former Employee 1 left in May 2023, Employee 5 resumed involvement with the Voting System Inventory file while we searched for a replacement to fill Former Employee 1's position. That new person was note hired until 2024 and has not had as much involvement with the file as yet.

- *Did Former Employee 1 separate from the Department of State in May 2023?*
  Yes. Former Employee 1's last day of work (and hence, last day with access to our internal systems) was May 19, 2023. His last day on our payroll was August 7, 2023.

- *Did Employee 5 take over the maintenance of that document immediately, or was there another person in that approximately one year between when Former Employee 1 left and when Employee 5 requested the spreadsheet be posted?*
  This is also a question that will need to be explored with Employee 7, but our understanding is that when Former Employee 1 stopped working for us in May 2023, Employee 5 resumed managing that file.

- *What were Former Employee 1's position and responsibilities in the office?*
  Former Employee 1's title was Voting Systems Specialist. (Position #189, with a State Personnel System classification of Elections Specialist II.) His duties encompassed the various tasks of the voting systems team, running from the oversight and management of voting system equipment in the counties, certification of the software and hardware of those components, performing "trusted build" updates of the equipment when new equipment or software updates are purchased by counties, participating in the Election Night Reporting work, both before the election by working with the software vendor on the ENR system and testing the ENR system with the counties, and then on election night itself, working to upload election results from the counties. The voting system team also is responsible for managing the state's Risk Limiting Audit after the election, which includes managing the software that is used in the audit, and then directing and managing the counties as they perform the RLA. The full scope of Former Employee 1's duties is reflected in the attached position description.

- *What are Employee 5's position and responsibilities?*
  Employee 5's title also is Voting Systems Specialist. (Position #200, with a State Personnel System classification of Elections Specialist IV.) While more senior in longevity and classification, his duties cover many of the same areas. The one distinction is that Employee 5 has been much more significantly involved in the development and management of the RLA program. A copy of his current position description also is attached.

Technical questions:

- *Before June 21, what other times was the inventory list uploaded to be publicly available?*

The Voting System Inventory is updated whenever a county changes the voting system equipment it is using. We are researching how many times there were new versions of the file posted to our website and when. We will have to get back to you on the specific dates.

- *Was it posted any time between when Former Employee 1 left and when Employee 5 requested it be posted on June 21?*
  Likely yes, but we don't have specific dates yet.

- *How often is that file updated, revised, or posted?*
  As noted, the file must be revised (and reposted) whenever a county makes a change in the voting system equipment that it is using. There is no specified cadence for the frequency of revisions. It is instead a function of whenever a county makes a change in its own complement of voting system equipment and then reports that change to the voting systems team."

The position descriptions that Employee 11 referenced in his response above were saved and added to the case in Evidence.com

At about 8:30 AM, Inv Brodzinski sent a records request to Employee 11 and Employee 1. It was followed- up with an expanded records request at 9:13 AM. Those requests were saved as part of this case file. Employee 11 replied that they were received.

Wednesday, November 13, 2024

In the morning, Inv Brodzinski called defense attorney Joe Morales, representing Employee 5. On speaking to Mr. Morales, I learned he had not yet had a conversation with his client about the case and didn't expect that to happen until the week of November 18, 2024. I told him the importance of speaking with Employee 5 and that this needed to be completed before the case could be resolved.

I spoke with Elsa Archambault, an attorney representing Employee 7, in the afternoon. We scheduled an interview at the DA's office on Friday, November 15, 2024, at 10:30 AM. She wanted the interview to last an hour and seemed surprised that I thought it would take longer than that. We agreed to do one hour for this first meeting and schedule follow-ups if necessary. I made her aware that it would be recorded on BWC.

Around 11 AM, Investigators Brodzinski and Lucas met Employee 11 in the lobby of 1700 Broadway. He gave us three Dell laptops, one power cord, and passwords for each. Two are for Employee 7, and one is for Employee 5. Inv Brodzinski provided them to Analyst Chris Gray for imaging.

Later that day, Chris Gray informed me that he needed the BitLocker passwords for the devices and that what I had provided wasn't what he needed. I asked Chris Gray to contact Employee 1 to obtain those passwords.

Friday, November 15 2024

At 10:30 AM, Inv Brodzinski met with Employee 7 and his attorney, Elsa Archambault, at the DA's Office. No one else was present for the meeting, which was recorded on BWC and added to this case in Evidence.com.

The conversation can be reviewed verbatim in the BWC video or its associated transcript on Evidence.com. This report will cover only significant parts of the conversation. They will not necessarily be discussed in the order they were discussed with Employee 7.

Employee 7 identified his position at the CDOS as the Voting Systems Manager. He explained that his team oversees technical aspects of the election, including certifying voting machines, performing a risk-limiting audit, and reporting on election night. Employee 7 supervises the Voting Systems Specialists Employee 5, Employee 3, and Employee 4. He previously supervised Former Employee 1, who identifies as Former Employee 1, for her last few months at CDOS.

According to Employee 7, Former Employee 1 created the Voting System Inventory as an XLSX spreadsheet. Before Former Employee 1 joined their team, the records had been kept as a Microsoft Access database file. Former Employee 1 thought that was overly complicated for the data they needed to track and recommended making the file a spreadsheet instead. Employee 7 agreed, and Former Employee 1 did that. Employee 7 was adamant that neither he nor any team member knew the spreadsheet had hidden sheets or that those sheets contained the BIOS passwords for the machines.

Employee 7 explained that the Voting System Inventory file was published, to his recollection, all other times in PDF file format and that the June 21, 2024, posting was the only time it was posted as an XLSX. Employee 7 also said the team tried to update the file on their website shortly before each election period. Thus, it was posted on June 21, 2024, before the June 25, 2024 primary election date.

Employee 7 said he recalled discussing with Employee 5 posting the file as a spreadsheet rather than a PDF. Employee 7 believes the motivation was to give the public a more usable file type that can be sorted and filtered to search for data. Those functions aren't as easy to use in a PDF as in a spreadsheet.

Inv Brodzinski asked Employee 7 where the voting systems team thought the BIOS passwords were kept if they didn't know about the hidden sheets in the Voting System Inventory spreadsheet file. Employee 7 explained that the BIOS passwords were kept as a separate column in the "Inventory" sheet of the Voting Systems Inventory spreadsheet (see notes from November 8, 2024, for an explanation). This is the same sheet that was published to make it publicly available. Employee 7 explained that their process was to delete the column with the BIOS passwords from the sheet, export the file to a PDF, and publish it to their website. Or, in this instance, delete the column with the BIOS passwords and then publish the file in XLSX file format.

Employee 7 did not think anyone on the voting system team had an extreme political ideology that would motivate them to attempt to get the passwords published to subvert the election process. He confirmed that for the BIOS passwords to be of value to someone, they would need the BIOS password, physical access to the machine the password is for, and then the local user login and password to access the machine.

The Voting System Inventory file was password protected, and only the four voting system team members knew the password. Further, only those four people and Employee 7's manager, Employee 2, have access to where the file is kept.

Inv Brodzinski believes that Employee 7 was being open and honest in answering questions and that he was neither withholding information nor lying about information.

At 11:15 AM, Inv Brodzinski received an email from Employee 13, Legal Policy Advisor at the CDOS. She stated: "Also, Employee 1 and I came across evidence yesterday and today that shows the excel spreadsheet that was on our website from June through October was never updated or manipulated after the creator of the spreadsheet left our office in May 2023. This includes that no additional passwords were placed on the hidden sheet by anyone in our office." She did not specify what this evidence was.

Monday, November 18, 2024

At Analyst Chris Gray's request, around 8:56 AM, Employee 1 provided the BitLocker passwords for the three laptop computers the CDOS provided in this investigation. He shared them via Evidence.com. Chris Gray informed him that the passwords would have to be in his final report about his examination of the computers. Chris Gray continued to work on making images of the laptops for examination.

At 12:17 PM, Inv Brodzinski received an email from Employee 11. He provided the transcript of hearing testimony from the lawsuit brought against the CDOS by the Colorado Libertarian Party (24CV33363, November 4, 2024). It was not requested, but Employee 11 offered it in case it would be useful in this investigation. The transcript was saved to this case in Evidence.com.

In the afternoon, Inv Brodzinski spoke to defense counsel Joe Morales about interviewing Employee 5. We agreed to meet at the DA's Office on Tuesday, November 19, 20224, at 11:00 AM.

Tuesday, November 19, 2024

At 8:30 AM, I asked Employee 11 for contact information for Employee 4 and Employee 3. He replied and clarified that Employee 11's last name was Employee 11 last name, not Employee 11 last name. I later asked for Employee 9's contact information, which was provided.

Employee 5 and attorney Joe Morales arrived for an interview at 11:00 AM The interview was recorded on BWC and added to this case in Evidence.com. It concluded around 11:52 AM Inv Brodzinski believes that Employee 5 was being open and honest in answering questions and was neither withholding information nor lying about information.

The conversation can be reviewed verbatim in the BWC video or its associated transcript on Evidence.com. This report will cover only significant parts of the conversation. They will not necessarily be discussed in the order they were discussed with Employee 5.

Employee 5 said he'd worked at the CDOS since 2015 and has been a voting systems specialist since 2018. Before that, he worked on the legal team in the elections division. His educational background is in political science. His current manager is Employee 7. He identified Employee 4 and Employee 3 as other team members. He said [redacted] began in approximately May 2024 and is now most directly responsible for the Voting System Inventory file. However, she was so new there when this file was published on their website that he wasn't sure if she even knew how to publish it. Employee 5 described his and the team's duties similarly to how Employee 7 described them.

As to the Voting System Inventory file, Employee 5 said that Former Employee 1 first created it from an Access database file. The file type was changed due to the complexity of Microsoft Access, and a spreadsheet was a better file format to keep this data in. Employee 5 explained that the BIOS passwords were kept in a column within the "Inventory" sheet in the file. This sheet is posted publicly on the CDOS website. That column was deleted from the sheet before it was posted. Also deleted were two other visible sheets. Employee 5 thought those sheets might have been named "Disposed of" and "Statistics," but he wasn't completely confident about the names of these sheets. They were both deleted before the spreadsheet was posted online. This left only the hidden sheets. Employee 5 said he did not know they were there and didn't think anyone else on the voting systems team did, either.

Employee 5 said the decision to publish the file in June was made because of the upcoming primary election. He suggested publishing it as an Excel spreadsheet this time to give the end users a more user-friendly file format. Employee 5 said he believed it had always been published as PDF in the past.

Employee 5 did not think anyone on the voting system team had an extreme political ideology that would motivate them to attempt to get the passwords published to subvert the election process. He confirmed that for the BIOS passwords to be of value to someone, they would need the BIOS password, physical access to the machine the password is for, and then the local user login and password to access the machine.

The Voting System Inventory file was password protected, and only the four voting system team members knew the password. Further, only those four people and Employee 7's manager, Employee 2, have access to where the file is kept.

The remainder of the interview can be reviewed in the BWC video.

Wednesday, November 21, 2024

I received an email from Employee 13 stating that they're still working on the requests for records and hope to have them ready by Friday, November 23, 2024.

Thursday, November 21, 2024

Inv Brodzinski called Employee 3 on the phone number provided by CDOS and tentatively schedule an interview with her for Friday, November 23, 2024, at 1:30 PM at the DA's office. She confirmed her last name is [redacted], not [redacted]. Inv Brodzinski left voicemails requesting a callback from Employee 9 and Employee 4.

Employee 9 returned my call, and we scheduled an in-person interview at the DA's Office on December 4, 2024, at 12:30 PM.

Friday, November 22, 2024

Employee 11 arrived for her interview as scheduled. The interview was recorded on BWC and added to this case in Evidence.com. Inv Brodzinski believes that Employee 3 was being open and honest in answering questions and was neither withholding information nor lying about information.

The conversation can be reviewed verbatim in the BWC video or its associated transcript on Evidence.com. This report will cover only significant parts of the conversation. They will not necessarily be discussed in the order they were discussed with Employee 3.

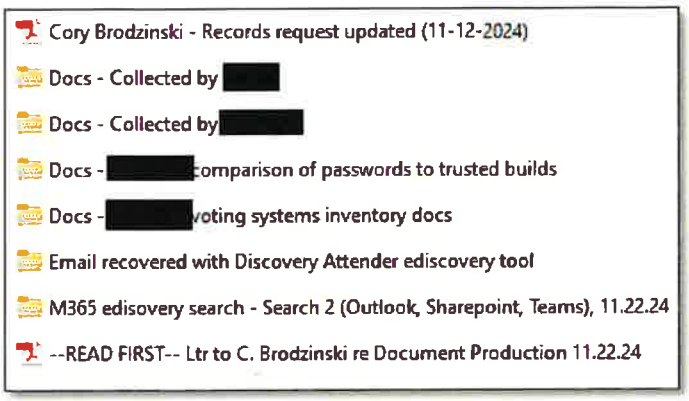
Employee 3 clarified that her correct name is Employee 3, and she is in the process of having it legally changed to Employee 3. She currently works as a Voting Systems Specialist on the CDOS Voting Systems Team. She was new to this position around the end of April 2024. She described her duties consistent with what other persons interviewed generally said about the job description. Employee 3 said she did not participate in preparing the Voting Systems Inventory file to be published in June 2024 because she was too new to the office to be involved with that.

Employee 3 did not know the spreadsheet had hidden tabs added to it, stating the spreadsheet was already established when she started working there.

Nothing Employee 3 said during the interview contradicted anything else learned thus far in this investigation.

Monday, November 25, 2024

Inv Brodzinski met with Employee 11 in the lobby of the DA's Office and was provided an encrypted thumb drive containing requested files. It was given to Analyst Gray for uploading to the DA's network and was added to the case in Evidence.com. A cursory review of the contents show the following file and folder structure:



Wednesday, December 4, 2024

Employee 9 arrived for an interview at 12:30 PM The interview was recorded on BWC and added to this case in Evidence.com. It concluded around 1:00 PM. Inv Brodzinski believes that Employee 9 was being open and honest in answering questions and was neither withholding information nor lying about information.

The conversation can be reviewed verbatim in the BWC video or its associated transcript on Evidence.com. This report will cover only significant parts of the conversation. They will not necessarily be discussed in the order they were discussed with Employee 9.

Employee 9 confirmed her role as one of the webmasters for the CDOS, along with Employee 6. She stated the work request from Employee 5 was not uncommon or unusual, and posting files to their website was a common task for her. She's been in this role for about 12 years and thinks she may have posted a Voting System Inventory file in the past as a PDF, but she could not recall it being posted as an Excel document previously. Employee 9 said she doesn't regularly review or check files before posting, as they've already been approved for posting by the requestor. She sometimes checks a file to see its name and label it correctly. Employee 9 said that the Jira ticket shows Employee 8 approved Employee 5's posting request, but she wasn't sure who he was within the organization compared to Employee 5. She said it is possible Employee 8 did approve the posting as fast as he did- within about one minute.

Employee 9 has no reason to think anyone was trying to post the passwords deliberately and thinks the file was made an Excel spreadsheet this time to make it more accessible. This is consistent with what other people have said as well.

Thursday, December 5, 2024

Investigators Brodzinski and Webster met with CDOS engineer Employee 14 in the lobby of their office building and were provided a hard drive with the rest of the requested documents. The encrypted thumb drive received from Employee 11 earlier was returned to him. Analyst Gray added this new hard drive to the Z network drive and copied to this case in Evidence.com. Investigators Brodzinski and Webster returned the hard drive to Employee 14 around 9:00 AM.

At 10:04 AM Inv Brodzinski called the main number found for Clear Ballot (857-250-4961) to contact Clear Ballott Employee 1. I spoke to another employee who said he'd send Clear Ballott Employee 1 a message to call me. Clear Ballott Employee 1 is believed to be the Clear Ballot employee who first notified CDOS about the BIOS passwords being accessible.

At 10:06 AM Clear Ballott Employee 1 returned my phone call. We spoke for several minutes over the phone, and the conversation was recorded via the Axon Capture app on my office-issued cell phone. The recording was added to this case in Evidence.com.

Clear Ballott Employee 1 confirmed that a business analyst at Clear Ballot named Clear Ballott Employee 2 (phone unknown, email [redacted]) first found the hidden spreadsheets while reviewing the data for business competition purposes. Per Clear Ballott Employee 1, Clear Ballott Employee 2 notified his manager, who notified Clear Ballott Employee 1, who attempted to notify Employee 7. Employee 7 was unreachable, so Clear Ballott Employee 1 notified Employee 12 at CDOS.

An email was sent to Clear Ballott Employee 2 at 10:24 AM requesting he call me to discuss how he found the passwords.

Monday, December 9, 2024

Inv Brodzinski interviewed Clear Ballott Employee 2, a business analyst for Clear Ballot, via video conference on Google Meet. [redacted], head of sales for Clear Ballot in Colorado, was also present at the interview. The interview was recorded on audio via the Axon Capture app on Inv Brodzinski's office-issued cell phone and added to this case in Evidence.com. Inv Brodzinski believes that Clear Ballott Employee 2 was being open and honest in answering questions and was neither withholding information nor lying about information.

The recorded audio and its associated transcript can be reviewed verbatim on Evidence.com. This report will cover only significant parts of the conversation. They will not necessarily be discussed in the order in which they were discussed with Clear Ballott Employee 2.

Clear Ballott Employee 2 confirmed he discovered the hidden tabs on the spreadsheet but stated it occurred sometime in July, not October 2024. As part of his duties as a business analyst, Clear Ballott Employee 2 does market research and spends a lot of time looking at spreadsheets of this type of data for market opportunities for Clear Ballot. He said it is normal for him to check spreadsheets for extra, hidden data that is sometimes present. Therefore, he right clicked on the

Inventory tab and unhid the spreadsheets. He saw the data included BIOS passwords but did not think anything of it then and continued with his market research.

It was not until he was in an election security training course in October that Clear Ballott Employee 2 realized the presence of those BIOS passwords could be a problem. He reported it to the head of QA at Clear Ballot, who then escalated the issue. Inv Brodzinski believes that all occurred on October 24, 2024.

Clear Ballott Employee 2 confirmed that he had not been contacted by anyone else about his discovery of the BIOS passwords.

Wednesday, December 11, 2024

Inv Brodzinski met with Former Employee 1 in the lobby of the [redacted] to discuss her work at the CDOS. Inv Brodzinski attempted to use the Axon Capture app on his office-issued phone to record the interview, but the app stopped recording after a few seconds and before the conversation began. Thus, there is no recording of this interview. As he thought the interview was being recorded, Inv Brodzinski did not take handwritten notes during the conversation. The conversation lasted about 50 minutes. Former Employee 1 was polite and cooperative and presented as being open and honest, although concerned if she was in any legal trouble. Inv Brodzinski told her she was considered a witness in this investigation.

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. Former Employee 1 said she began working for the CDOS in May 2022 and left on good terms in May 2023. She has a Bachelor of Science degree in Computer Science from [redacted]. She is well-versed in computer security and functionality.

Former Employee 1 said she did make the Voting System Inventory file, which she recalls naming "!NEW! Equipment Database" or something similar. She was the one who suggested to her supervisor, Employee 7, that the inventory be maintained in a spreadsheet as opposed to an Access database, as it is simply a list of equipment and does not need the complexity of being in a relational database that Access provided. Employee 7 agreed, and she exported the file from Access to Excel and maintained it there for the duration of her tenure. Former Employee 1 did create the hidden tabs- she thinks maybe as many as four or five of them- as a working place for the records. She described them as like "scratch paper or a notepad," where she could keep extra information she knew she needed for the inventory out of the way when she was working. Former Employee 1 has no memory of telling anyone else on the Voting Systems Team that those hidden tabs were present or in use. She was the Voting Systems Specialist most directly responsible for the routine maintenance of the inventory. Other team employees would access the file to look for information, but she managed the file. Former Employee 1, therefore, did not think it was necessary or even relevant to let other team members know those hidden tabs were there. She recalls the BIOS passwords also being in the workbook's main "Inventory" tab.

Former Employee 1 explained that CDOS needed the machine BIOS passwords to update the trusted build firmware on each machine, a process she was part of on a few occasions. She described the publication of these BIOS passwords as a serious cybersecurity issue and explained that one would not necessarily need a system login to a device to use the BIOS passwords. Former Employee 1 explained 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. Former Employee 1 said functions such as the ability to boot from a USB drive or turn on/off networking functionality could all be managed within the BIOS. This procedure would require someone to have physical access to the machine.

Former Employee 1 does not recall ever being part of publishing the inventory in the past but thought it was probably done as a PDF and not as a spreadsheet. She 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. She does not recall providing any transition training to her replacement when she left, wherein she would have had the chance to explain how the spreadsheet was organized.

Inv Brodzinski concluded the interview.

DA's office staff reviewed the Microsoft Teams messages provided by CDOS. They reviewed all provided messages for any messages that discussed the voting system inventory being published with passwords, instructions or discussion on posting it, and the agency's response to the discovery. Apparently due to retention periods, messages were only received as far back as late October 2024. Therefore, there were no messages about posting the file initially. Inv Brodzinski learned from Employee 1 that the time stamps on the messages are in UTC, not local time in Denver.

The following message was found in Employee 5's conversations. This message seems to be the first time Employee 7 was notified that the passwords were published, and it is consistent with what Inv Brodzinski has been told in interviews about who was notified, when, and how.

Employee 12 [redacted] ***> 10/24/2024 7:43 PM***
"Clear Ballott Employee 1 just called. He says the voting systems inventory on the website has hidden tabs thatcan be un-hidden, and one of them lists BIOS passwords. I know you're all busy but cansomeone ask webrequests to pull that down until you can provide a version that actuallydeletes the hidden tabs?"

Employee 7 <[redacted] ***> 10/24/2024 7:44 PM***
"Jesus"

Employee 7 <[redacted] ***> 10/24/2024 7:44 PM***
"I got it"

Employee 12 <[redacted] *> +like 10/24/2024 7:45 PM*

Other reviewed Teams messages did discuss the passwords being published, but the conversations were about the CDOS response to the problem and working to mitigate the risks from it. The CDOS response to this is outside the scope of this investigation, so they were not reviewed further.

Thursday, December 12, 2024

DA's Office staff, including Inv Brodzinski, completed reviewing the data on Employee 7's and Employee 5's laptops and all emails provided by CDOS. No emails were found to be relevant to this investigation, except for one that showed the Jira work ticket requesting the Voting System Inventory be published. All other emails were about unrelated topics or the response to the discovery that the passwords had been published. No messages were found about posting the file initially. Likewise, nothing was found on any of the provided laptop computers about posting the file initially. Copies of the Voting System Inventory were found, but no evidence suggested Employee 7 or Employee 5 knew the file contained hidden tabs.

Inv Brodzinski interviewed Employee 8, Ballot Access Manager at CDOS, in person at the DA's Office. The interview was recorded on BWC and added to this case in Evidence.com. Inv Brodzinski believes that Employee 8 answered questions openly and honestly and was neither withholding information nor lying about information. The interview was briefly interrupted by someone entering the conference room to say hello, not realizing we were conducting an interview.

The recorded video and its associated transcript can be reviewed verbatim on Evidence.com. This report will cover only significant parts of the conversation. They will not necessarily be discussed in the order they were discussed with Employee 8. Employee 8's statements seem consistent with those outlined in the Baird Quinn report.

Employee 8 works as the Ballot Access Team Manager and does not work with personnel from the Voting Systems Team. He does not use the Voting System Inventory and is unfamiliar with how it is maintained. He did approve Employee 5's publication request ticket on Jira. However, he did not review the file before approving it and said he would not recognize if anything were wrong with the file if he had; it is not something he's very familiar with. He has received no training on when or how to approve Jira web requests and knows of no policies related to that. He was given approver-level access when he became a manager, but he does not think Employee 7 has approval access. Employee 8 approved the ticket as a matter of reflex- his team members have had to wait days for something to be approved, so he automatically approves any that come to him via email so other people don't have to wait for things to be published.

Employee 8 knows of no political or ideological views Employee 5 might hold that would motivate him to publish these passwords purposefully. The interview was concluded.

Monday, December 16, 2024

Inv Brodzinski interviewed Employee 6, webmaster for CDOS, and Employee 4, Senior Voting Systems Specialist at CDOS. They were interviewed separately, and both interviews were recorded via BWC. Those recordings and their auto-generated transcripts are available on Evidence.com. Their statements will not be reviewed in-depth here, except that they were consistent with what was already known in this investigation and offered no new insight as to why or how these passwords were posted.

Employee 6 only closed out the work request ticket requesting the file be published and was a part of the response to take the file done. Employee 4 had nothing to do with either posting the file or taking it down but is familiar with the Voting System Inventory since it's a file used by his team. Neither had any reason to think Employee 5 knew the hidden tabs were in the worksheet or had any ideological motivation to attempt to subvert the integrity of the election process. Employee 4 created the original Access database that first housed the inventory, and Former Employee 1 was the one who created the Excel version. Employee 4 did not know the hidden tabs were in the worksheet until they were discovered in October.

Tuesday, December 17, 2024

Throughout this investigation, Colorado District Attorney's Offices have received sworn affidavits from individuals and organizations requesting an investigation into the published passwords. These have been forwarded to the Denver DA's office by agreement. All are stored in Evidence.com. Almost all of them are nearly identical in format and content, except for information related to the affiant. Inv Brodzinski reviewed these and found that none offer new information on how or why the passwords were published, whether the passwords were knowingly published, offer no investigative leads, and none are from within the City and County of Denver.

Wednesday, December 18, 2024

Inv Brodzinski spoke to Employee 11 on the phone. The conversation was brief and not recorded. Inv Brodzinski inquired about the specific statute or election rule that required the CDOS to publicly post the Voting System Inventory (See conversation with Employee 11 from November 5, 2024). Employee 11 stated he was mistaken when he previously said there was a specific rule, but it was made public historically through multiple administrations in the CDOS. There is a rule that requires the counties to provide the data to the CDOS, but no rule or statute requires the CDOS to make a Voting System Inventory public.