Missouri State Highway Patrol

INCIDENT # 210537534
SPECIAL INVESTIGATION
COLE COUNTY
DESE SPECIAL

INCIDENT REPORT

ORIGINAL REPORT

SUPPLEMENT 1 - INTERVIEW OF PAM KEEP DAVID DURNOW

SUPPLEMENT 2 - INTERVIEW OF THERESA FROMMEL

SUPPLEMENT 3 - INTERVIEW MALLORY MCGOWIN

SUPPLEMENT 4 - CONTACT WITH ATTORNEY JOSEPH MARTINEAU

SUPPLEMENT 5 - CONTACT WITH ATTORNEY ELAD GROSS

SUPPLEMENT 6 - INTERVIEW JOSHUA RENAUD

SUPPLEMENT 7 - INTERVIEW DOCTOR SHAJI KHAN

SUPPLEMENT 8 - CASE CLOSED

Missouri State Highway Patrol

Incident: 210537534

RMS Report Number: R008617792

Incident details:

Incident Type:	SPECIAL INVESTIGATION
Incident time:	2021/10/14 06:44 - 2021/10/19 16:21
Reported time:	2021/10/14 18:13
Incident location:	JEFFERSON CITY, COLE MO
Incident status:	Closed
Status date:	2021/10/29
Summary:	COLE COUNTY - DESE SPECIAL - CFS 210537534

Involved Officers:

- Dispatched officer; Reporting officer / SUBLETTE, P. / #832 / Missouri MAH / Officer / GHQ DDCC DIGITAL FORENSICS INVESTIGATIONS (1510 East Elm Street, Jefferson City, Cole MO United States of America)
- CAD operator / FIEDLER, L. / #C125 / Missouri MAH / Police civilian / TROOP C RADIO COMMUNICATIONS (891 Technology Drive, Weldon Springs, St. Charles MO United States of America)
- Assisting officer / SEABAUGH, K. / #1150 / Missouri MAH / Officer / GHQ DDCC TROOP F CRIMINAL INVESTIGATIONS UNIT (1510 East Elm Street, Jefferson City, Cole MO United States of America)

Involved Persons:

Name: RENAUD, JOSHUA **Gender:** Male

Classification: Suspect **DOB:** [redacted] (42)

DL:

SID: **FBI:**

Address: [redacted]

Telephone: [redacted]

Height: **Weight:** **Build:**

Race: White **Hair Color:** **Eye Color:**

Tattoos/Marks:

Alias names:

Involved Addresses:

- Incident address / JEFFERSON CITY, Missouri

ORIGINAL REPORT
DATE OF REPORT - OCTOBER 14, 2021

1. On Thursday, October 14, 2021, at about 0644 hours, Captain Paul Kerperin contacted me with information he had received about sensitive data, teacher's social security numbers, being exposed via a public website of the Missouri Department of Elementary and Secondary Education (DESE). Captain Kerperin directed the Digital Forensic Investigative Unit to investigate the matter.

2. I was provided with a copy of two emails which were sent from Josh Renaud, JRenaud@post-dispatch.com, to a general DESE email address, communications@dese.mo.gov. The first email showed it was sent on Tuesday, October 12, 2021, at 1052 hours local time, from Reporter Josh Renaud to DESE reporting the situation and requesting a follow-up contact. The second email showed it was sent on Tuesday, October 12, 2021, at 1134 hours local time, from Reporter Josh Renaud to Mallory McGowin at DESE, providing step by step instructions on how to recreate the scenario he said he did to locate teacher's social security numbers on the DESE web application.

3. Copies of the two emails from Reporter Renaud are attached to this report.

4. This investigation is ongoing.

P. D. Sublette, Master Sergeant
Division of Drug and Crime Control

PDS:lab

Attachment:
0.1 Emails

SUPPLEMENT 1 - INTERVIEW OF PAM KEEP DAVID DURNOW
DATE OF REPORT - OCTOBER 14, 2021

1. On Thursday, October 14, 2021, at about 1030 hours, I contacted Chief Information Officer (CIO) Jeff Wann via telephone. CIO Wann directed me to call him and Deputy CIO Paula Peters. Deputy CIO Peters relayed to me information which was in the emails from Reporter Renaud. Deputy CIO Peters arranged for me to meet with Office of Administration (OA) Information Technology Services Division (ITSD) Client Service Manager Pam Keep.

2. On Thursday, October 14, 2021, at about 1115 hours, Corporal Kyle Seabaugh and I met with Ms. Keep in her office in the Jefferson Office Building. David Durnow, an OA ITSD Application Developer, who was working on the web application at the focus of this investigation (https://apps.dese.mo.gov/HQT/CredentialListerChecker.aspx?) joined us via a Cisco WebEx meeting on Ms. Keep's computer. Mr. Durnow said the Missouri Department of Elementary and Secondary Education (DESE) application at the focus of this investigation had already been removed from the public website. Mr. Durnow, using an offline copy of the website which showed how it would have looked early on Tuesday, October 12, 2021, showed us the website and walked us through the process used to obtain the data, just as described in Reporter Renaud's email to DESE.

3. While discussing the steps listed by Reporter Renaud which explained how to access the social security numbers, we were able to see the steps taken firsthand. It was learned, by accessing the website, any user could click on a specific school district, which brought up a list of teachers associated with that specific district. When a specific teacher was selected, the user could click the submit button to view information about that specific teacher. It appears this is the purpose the DESE web application, so school districts, teachers themselves, parents, or anyone could view teacher data, which was considered public information.

4. Ms. Keep and Mr. Durnow told me once on the screen with this specific data about any teacher listed in the DESE system, if a user of the webpage selected to view the Hyper Text Markup Language (HTML) source code, they were allowed to see additional data available to the webpage, but not necessarily displayed to the typical end-user. This HTML source code included data about the selected teacher which was Base64 encoded. There was information about other teachers, who were within the same district as the selected teacher, on this same page; however, the data about these other teachers was encrypted.

5. Ms. Keep said the data which was encoded should have been encrypted. Ms. Keep told me Mr. Durnow was reworking the web application to encrypt the data prior to putting the web application back online for the public. Ms. Keep told me the DESE application was about 10 years old, and the fact the data was only encoded and not encrypted had never been noticed before.

6. During Mr. Durnow's demonstration, he showed how it is possible to obtain the personal information for all teachers but suggested this would require the user to go to each teacher one at time to obtain the information. Using the private local test environment on Mr. Durnow's computer, I captured screenshots as he went through the steps provided in Reporter Renaud to document the steps. These are attached to this report.

7. Ms. Keep said Mr. Durnow would preserve a copy of the websites source code as it appeared prior to this issue being brought to their attention.

8. Copies of screen captures, and webpage source code are attached to this report.

9. This investigation is ongoing.

P. D. Sublette, Master Sergeant
Division of Drug and Crime Control

PDS:lab

Attachments:
1.1 Screenshots
1.2 Webpage Source Code

SUPPLEMENT 2 - INTERVIEW OF THERESA FROMMEL
DATE OF REPORT - OCTOBER 14, 2021

1. On Thursday, October 14, 2021, at about 1500 hours, I met with Deputy Chief Information Security Officer (CISO) Theresa Frommel who works in the Office of Administration (OA) Office of Cyber Security and arranged a meeting with her and two of her co-workers. Corporal Seabaugh and I met with her in her office in the Truman Office Building. Deputy CISO Frommel told me they initially reviewed the past two weeks of logs showing the volume of web traffic to the website address of the Missouri Department of Elementary and Secondary Education (DESE) application at the focus of this investigation. She stated the traffic looked normal and nothing stood out to them that would indicate there was a surge of traffic to the site.

2. I met with Deputy CISO Frommel again on Friday, October 15, 2021, at about 1500 hours. She told me they reviewed network traffic and for the DESE website for the past 90 days and did not see any abnormal activity or anything of interest with the website. She provided a random sample of what data is captured by the OA firewall logs when anyone accessed a website administered by OA. The data in this sample is not directly related to this specific investigation, but rather a sample of the type of data captured.

3. A copy of the sample log data is attached to this report.

4. This investigation is ongoing.

P. D. Sublette, Master Sergeant
Division of Drug and Crime Control

PDS:lab

Attachment:
2.1 Firewall Log from OA

SUPPLEMENT 3 - INTERVIEW MALLORY MCGOWIN
DATE OF REPORT - OCTOBER 18, 2021

1. On October 18, 2021, at approximately 1030 hours, I interviewed Mallory McGowin in an office on the 6th floor of the Jefferson Building, located at 205 Jefferson Street, Jefferson City, Missouri. Mrs. McGowin is the Chief Communications Officer for the Communications Division of the Department of Elementary and Secondary Education (DESE). Mrs. McGowin has been in this position for approximately two (2) years.

2. I began the interview by asking Mrs. McGowin who controls the DESE website and the educator qualifications section. She stated while the educator qualifications section is a search tool on the DESE website, it was developed and is maintained by the Office of Administration's (OA) Information Technology Services Division (ITSD). She stated the education qualifications portal was primarily used by school districts to verify a teacher's certifications and or qualifications. She stated this section of the website is a public portal; however, there was also a secure side of the portal where a person would have to obtain credentials to log in and perform the searches. Mrs. McGowin stated the public portal is used by people who do not usually use the secure web applications on a regular basis and do not have credentials to log in on the secure side of the site. She stated this website was brought online in 2011, to help streamline public access to the information provided on the portal. She stated prior to the portal being brought online, people would have to call the DESE Office over the telephone to verify certifications and qualifications.

3. Mrs. McGowin advised when the DESE wanted to gather information and make it available through an online portal, they would have to work with ITSD to develop that application. She stated when this portal was developed, DESE worked with the ITSD to develop the portal so it would pull the information from the back-end database and make it available on the public portal. Mrs. McGowin stated there were two ways to verify certification information. She stated the user could navigate through a series of drop-down lists to select school year, region, specific schools, and eventually select an individual teacher from a picklist, and the teacher's certifications would be available to be viewed by anyone, and the teacher's social security number is not displayed. She stated while the search is being conducted, the HyperText Markup Language (HTML) source code is passing back and forth pulling the information through the verification process. HTML is a standardized system for tagging text files to achieve font, color, graphic, and hyperlink effects on World Wide Web pages (definition located using Google). Mrs. McGowin stated another way to search would be to use the teachers last name and the last four digits of their social security number. She stated this would pull the same information as the public portal only showing her certifications and not the full nine-digit social security number.

4. Mrs. McGowin advised DESE was made aware by Post-Dispatch Reporter Josh Renaud, when anyone was accessing the teacher's certifications web page, a person could press "Control U" or right click and select "View Page Source," select the view state data, copy, and paste that

into a decoder, and it would decode. After the view state data was decoded, it was revealed there was a line where "Educator SSN" was observed along with a nine-digit number. She stated for some reason, ITSD still had the full nine-digit social security number in the table they were using. She also stated they learned this was no longer "best practice" or "modern operating procedures" to use "view state", but view state was still being used on the application and the data was encoded and not encrypted. She stated her understanding was if the application was using "session state" instead of "view state" then unencrypted data would not have been publicly exposed.

5. I asked Mrs. McGowin if I was correct in saying the website was for DESE but it was maintained by ITSD, and she indicated that was correct. I asked her if the ITSD was within the Office of Administration, or if DESE had their on-information technology section, and she indicated it was within the Office of Administration. She stated in 2009, policy was changed to move all information technology services to the Office of Administration.

6. I asked Mrs. McGowin about the Educator Qualifications portal on the website. I asked her if a user had to have authorization to access it since there was a public and secure site, and for her to explain how it worked. She stated a school district would determine which employees need access to the secure side of the website. She stated school districts have employees who have secure access, and employees who do not. She stated the public portal would be for the people who did not have secure access, and stated it was implemented to streamline obtaining or viewing teacher certifications. I asked her if it was correct to say the school district determines who needs secure access and everyone else uses the public portal, and she indicated that was correct. She stated some school district employees have secure access but use the public portal, so they do not have to login. She stated the public portal was also used by other states to verify teacher certificates if a teacher in Missouri wanted to teach in a different state.

7. I asked Mrs. McGowin if a teacher or person could request secure access to the Educator Qualifications portal directly through DESE, and she stated she would have to verify that with their Office of Data Systems Management, if a school employee needed secure access as a function for their job, they could have access to the secure side of the portal. I asked her if I was correct in saying if a person had an account on the secure side of the portal, that access would be facilitated through the school district, and she indicated that was correct. Mrs. McGowin also stated if you had a secure access account, they should see any private identifying information for the teachers. I asked Mrs. McGowin if there would be a difference between what information could be accessed on the secure side versus the public side, and she stated there would not be with this specific application.

8. I asked Mrs. McGowin who receives the information from the school district regarding the accounts for secure access. She stated the information is sent to the Office of Data System Management within DESE. She stated the Chief Data Officer is Jeff Falter. While speaking with Mrs. McGowin, it was determined only school district employees would have access to the secure side of the portal. I asked her if Josh Renaud had an account on the secure side of the portal and she stated he would not because members of the media do not have accounts on the secure side and stated all of this occurred within the public portal. Mrs. McGowin confirmed this all occurred on the public website. She stated from what she has observed, Mr. Renaud did not access anything that was not publicly available, nor was he in a place he should not have been. She said Josh Renaud appears of have only accessed open public data.

9. I asked Mrs. McGowin if they knew about the educator social security numbers being in the source code prior to this incident and she stated they did not. She stated Mr. Renaud's discovery of this incident is what brought this to light. She stated after this was brought up, she started checking the view state data to see if it would be something DESE staff would do. She stated it was an error or oversight when ITSD developed the application. She stated from what DESE could see, this vulnerability had existed since the application was built. I asked her how an application development would work, if they formed a committee, or if they had someone that worked with ITSD, and she stated Mr. Falter would be better to answer that question. She stated form her understanding, they have a committee that brings changes to website to ITSD. She stated DESE had points of contact within their department for ITSD employees to contact for website related issues or changes. Mrs. McGowin stated DESE will test the function of a website, or application after it has been developed, however they are not a part of the security or maintenance of the website, which would be handled by OA's ITSD, they only operate in the function of the website. Mrs. McGowin indicated the points of contact between OA ITSD and DESE would be DESE's Office of Data System Management.

10. I stated to Mrs. McGowin if a person was on the public site, say a parent, checking the certifications for a teacher in the school for their child, when they performed this search, a teachers social security number was sitting there that people did not know about. She stated she did not believe it could be said that simple. She stated each teachers' certifications are available to be viewed when a person conducts a search, and that no private identifying information would be listed while viewing the certifications. I clarified with her I meant it would be available to be viewed if they performed the steps sent to her, and she stated that was correct. She stated the vulnerability would have been there since 2011, when the application was implemented. I asked her if this had ever been brought up before, and she stated not in the two years she had worked at DESE. She stated employees who have worked at DESE since 2011 have said the same thing.

11. I asked Mrs. McGowin why she thought this happened. She stated she did not know. She stated DESE collects a lot of data, but they as an agency the need to improve in the manner in which they explain the data. She stated the Post-Dispatch has the capability and resources to develop their own applications to make this data publicly available. She stated the Post-Dispatch has previously developed an application where a user can look up the salary for any public-school employee. She stated she initially thought when she was contacted, that was what they were trying to develop. She stated she has since spoken with ITSD employees, who have stated they did not believe they would have accessed this information to build a database like she was talking about. She stated from what she understands, Mr. Renaud taking the view state information and putting it into a decoder, would not have been necessary to create a dashboard.

12. Mrs. McGowin stated she received the email from Mr. Renaud on October 12, 2021, at 1052 hours. She stated Mr. Renaud informed them he had located a vulnerability and requested clarification on who he needed to share this information with so they could see it, and also requested an interview with someone regarding the vulnerability. She stated he advised the Post-Dispatch was going to run a story in 24-48 hours but wanted to let them know so they could remedy the situation before the article was published.

13. She stated she called Mr. Renaud approximately thirty minutes later and advised him to send her the information regarding the vulnerability because she handles media inquiries for DESE.

She stated he sent her the steps regarding how view the vulnerability. She stated she followed the steps and observed what he was talking about. She stated after she performed the steps, she called Mr. Renaud back and asked how he found the vulnerability, and she stated he said he was "poking around their data and found it." She stated he advised he was a data person and developer at the Post-Dispatch, and she assumed he was searching through data to possibly develop another dashboard or tool.

14. She stated she received the email on October 12, 2021, at 1052 hours, and then set up a Webex meeting at noon, then she called him at 1126 hours, and advised him to send the instructions to the DESE media inquiry email address. I asked Mrs. McGowin how many teachers were in the database and she stated the data would have dated back to 2005, and the total number would be approximately 576,000. Mrs. McGowin then provided me with a copy of the first email sent by Mr. Renaud to DESE media inquiry email. She stated she received the instructions from Mr. Renaud at 1134 hours. She stated she replicated the process, realized there was an issue, but had no way to corroborate the number she was viewing was the actual social security number, so she contacted an employee who would have access to that information, and had the number verified to confirm it was an actual person's social security number. She stated this occurred at about 1200 hours, and then she attended the meeting she had arranged. She stated she advised other staff members in the meeting of the situation, and a member of DESE's Office of Data System Management went to their ITSD representatives and told them to turn the search tool off. She stated the search tool was disabled at 1223 hours.

15. While speaking with Mrs. McGowin about the ease of the steps provided to her by Mr. Renaud, she stated the process was not difficult. Mrs. McGowin then agreed to print the emails between her and Mr. Renaud, which were then provided to me. I asked Mrs. McGowin if she knew why the teacher's social security numbers were encoded instead of encrypted, and she stated she did not know. She stated based on what she had heard over the past few days, when the website was brought online in 2011, that practice would have been okay. She stated since then, that process is no longer considered "best practice." She stated vulnerability scans are conducted on the websites, but this particular vulnerability would not be detected. She stated Vericode scans are performed regularly, and the reports they received did not show vulnerabilities.

16. I stated to Mrs. McGowin it was my understanding the website was developed in 2011, and that portion of the website had not been updated since 2011, and she indicated that was her understanding. She stated DESE was working to ascertain what the vulnerability scans actually test for. I asked her, based on what she was told, it would be best to encrypt the data, rather than encode it, and she stated that was correct. She then spoke of a process DESE was working on to change the way teacher's certifications would be pulled from the database, and also stated the public search tool was still disabled.

17. I asked Mrs. McGowin if they could place a monetary value on the data Mr. Renaud viewed, and she stated Mr. Renaud advised her in his email that he verified with three different teachers that their data was exposed. She stated she did not know whose information could have been viewed over the last 10 years. I asked her if anyone had contacted them regarding their identity being stolen and she stated they had not. She stated statutorily they are required to notify anyone whose data would have been compromised. She stated they did send an email to the education community notifying them of the possible exposure. I asked her if the three people Mr. Renaud

referenced contacted them, and she stated to her knowledge they had not. I asked Mrs. McGowin if she was aware of any data breach before on the website, and she stated not to her knowledge. She stated she was aware of someone's personal identifying being leaked via other means, but not this way.

18. I then asked Mrs. McGowin about her communications with Mr. Renaud. She confirmed she had communicated with him via email and phone. She stated she called him on October 12, 2021, at 1240 hours, after the meeting, which was the second time she spoke with him on the phone. She stated this was when she asked him who he shared the information with, and he advised the three teachers he used to verify the information, and the University of Missouri-St. Louis Cybersecurity faculty member. She stated he advised they would delay the story until the vulnerability was mitigated. She stated she called him at 1841 hours, that evening to advised him the vulnerability checks were still being conducted and requested they delay the publishing of the article to close of business on October 13, 2021, to allow more time for the vulnerability checks to be completed, to which he stated he would have to check with his editor. She stated Mr. Renaud contacted her at 1905 hours, and advised they would hold publishing the story, but requested a status check on October 13, 2021, at noon, to which she agreed. She stated she contacted him at noon on October 13, 2021 and advised him the security scans should be completed by end of business on Wednesday October 13, 2021. She stated Mr. Renaud advised the story was set to published on Thursday, October 14, 2021, and set to be published online the night of Wednesday, October 13, 2021. She stated Mr. Renaud requested an interview and a written statement, to which she stated she would make arrangements to accommodate. She stated at approximately 1300 hours, on October 13, 2021, she was advised a criminal investigation was being initiated. She stated she was told DESE legal counsel would be in contact with the Post-Dispatch legal counsel.

19. She stated she contacted Mr. Renaud and requested the contact information for their legal counsel. She stated after this the Post-Dispatch editor called, and she did not answer. She stated she provided DESE's legal counsel the Post-Dispatch editor's information and advised them of the situation.

20. I asked her if she was aware of any schemes by anyone related or involved in the investigation to exploit data or data breaches. She stated she was not aware of any other schemes.

21. I asked Mrs. McGowin if I could view the text message conversation between her and Mr. Renaud to which she agreed. I viewed the conversation and captured a picture of the conversation. I asked her if she had been in contact with Mr. Renaud prior to this incident. Mrs. McGowin conducted a search of her computer and located five (5) emails related to school data in the St. Louis area. All the emails were related to public information and Mrs. McGowin provided me a copy of the emails.

22. I asked Mrs. McGowin if she was advised at any time if the Post-Dispatch, or Josh Renaud wanted anything in exchange to not publish the information, and she stated they did not. I asked her if I was correct in the facts; they were contacted and advised of the vulnerability, the Post-Dispatch was going to run a story but they were notifying them so they could fix it before the story ran, DESE contacted the Post-Dispatch and advised them the security checks were not going to be completed in time, and requested they move the publishing date back to which they

agreed, and then they were advised a criminal investigation was going to take place and she stated that was correct.

23. I asked her if I needed to know anything else and she stated the decoder he used during the process is the first one on the list if you Google the decoder.

24. This interview was recorded using my patrol assigned digital voice recorder. The following items are attached to this report:

a. A copy of the audio recording.
b. A copy of the emails provided to me by Mrs. McGowin.
c. A copy of the picture of the text message conversation between Mrs. McGowin and Mr. Renaud.

25. This investigation remains open.

K. A. Seabaugh, Corporal
Division of Drug and Crime Control

KAS:lab

Attachments:
3.1 Archived Emails between Mallory McGowin and Josh Renaud
3.2 Emails between Mallory MacGowin and Josh Renaud

Media Attachments:
3.1 Mallory McGowin Interview
3.2 Text Message

SUPPLEMENT 4 - CONTACT WITH ATTORNEY JOSEPH MARTINEAU
DATE OF REPORT - OCTOBER 19, 2021

1. Between October 14, 2021, and October 19, 2021, Corporal Dustin Reed, Cole County Prosecuting Attorney William Locke Thompson, and I were in contact with Attorney Joseph Martineau, who is employed with the Lewis Rice Law Firm located in St. Louis, Missouri. Mr. Martineau is the legal counsel who represents the St. Louis Post-Dispatch and Josh Renaud regarding this investigation. During communications with Mr. Martineau, several points were discussed regarding arranging a time to conduct an interview with Post-Dispatch employee Josh Renaud and the voluntary disclosure of documents by Mr. Renaud relating to this investigation.

2. Ultimately, on October 19, 2021, arrangements were made through Mr. Martineau for an interview to be conducted with Mr. Renaud and to obtain the documents they agreed to release. The interview was set for October 22, 2021, at approximately 0930 hours, at the Lewis Rice Law Firm, located on the 25th floor of 600 Washington Avenue, St. Louis, Missouri.

3. Also during the communications with Mr. Martineau, Corporal Reed, Prosecutor Thompson, and I received a letter drafted by Mr. Martineau regarding the circumstances of this investigation. This letter is attached to the interview report for Josh Renaud.

4. This investigation remains open.

K. A. Seabaugh, Corporal
Division of Drug and Crime Control

KAS:lab

SUPPLEMENT 5 - CONTACT WITH ATTORNEY ELAD GROSS
DATE OF REPORT - OCTOBER 22, 2021

1. Between October 15, 2021, and October 22, 2021, I was communicating with Attorney Elad Gross regarding arranging a time to interview Dr. Shaji Khan. Mr. Gross is the attorney for Dr. Khan for the purposes of this investigation. Dr. Khan is employed with the University of Missouri-St. Louis.

2. Ultimately arrangements were made to interview Dr. Khan at the St. Louis Bar Association located at 555 Washington Avenue, St. Louis, Missouri, on October 25, 2021, at approximately 0930 hours.

3. This investigation remains open.

K. A. Seabaugh, Corporal
Division of Drug and Crime Control

KAS:lab

SUPPLEMENT 6 - INTERVIEW JOSHUA RENAUD
DATE OF REPORT - OCTOBER 22, 2021

1. On October 22, 2021, at approximately 0858 hours, I interviewed Joshua Renaud in a conference room at the Lewis Rice Law Firm, located on the 25th floor at 600 Washington Ave., St. Louis, Missouri. This interview was arranged and coordinated with Joseph Martineau, who is employed by the Lewis Rice Law Firm and is the retained counsel for the St. Louis Post-Dispatch and was present during the interview.

2. I began the interview by asking Mr. Renaud how he is employed, and he stated he is the Newsroom Developer for the St. Louis Post-Dispatch. He stated his job-related duties involve him putting together interactive graphics for newspaper and website, graphics for the print newspaper, maps, and charts. He stated he also builds news apps for crime tracking, COVID-19 maps, public salaries database, school guides, which are standalone news websites. He stated he also does data gather and data analysis for reporters. He stated he has been employed with the Post-Dispatch full time since 2005 to 2006. Mr. Renaud stated he graduated with a degree in Communications from the University of Missouri-St. Louis.

3. I asked Mr. Renaud when this situation started. He stated it began on the Thursday prior to the article being published, which was determined to be October 7, 2021. I asked Mr. Renaud to explain how he located the vulnerability on the website. Mr. Renaud stated one of his job duties is to help with data gathering. He stated there was a reporter who asked for his assistance in gathering data on teacher's certifications. He stated the reporter wanted to run analysis on teacher certifications to see if a news story was there to be published. He stated the reporter used a forum to run teachers to check for teacher certifications (the Department of Elementary and Secondary Education (DESE) website, Educator Qualifications Portal). He stated its a public facing tool to look up teacher certifications. I showed Mr. Renaud the DESE website and asked if this was what he used, and he stated that was the main site, and he used the public forum.

4. Mr. Renaud stated to answer the certifications questions regarding the story, they needed to build a data set. He stated he was assisting with aggregating the data so they could run analysis on it to look for trends or patterns that could lead to a story. He stated as he was doing this, he stated he needed to look at the source code to see the best way to collect this information, and in doing so he located what he thought was a social security number for an educator. He stated he located a parameter that was labeled "Educator SSN" and a nine-digit number below it, which at face value appeared to be a social security number. He stated he was shocked because he was not looking for it and did not expect to find that information. I asked him how long it took him to locate this information, and he stated he was unsure but estimated approximately two (2) hours.

5. I asked him what he did next. He stated this was not the only thing he was working on but notified a supervisor. He stated they determined, if this was true, there was a story there, and

they needed to notify DESE about the discovery of the security vulnerability. He stated he continued with the data collection and reached out to one source who was a teacher and verified the information they were looking at was their social security number. He stated on Monday October 11, 2021, he finished the data collection, but could not notify DESE due to it being a federal holiday. He stated on Monday, October 11, 2021, he contacted Professor Shaji Khan to verify his findings and speak with him about the information located. He stated he also contacted two other teachers, whom he knew personally, to verify the information he located on the website. He stated after talking to the teachers he knew; this confirmed their suspicion that the website was exposing social security numbers.

6. Mr. Renaud stated when he contacted Professor Khan, he (Professor Khan) stated he would not participate if they were planning to publish the article prior to notifying DESE, which he stated they were going to notify DESE prior to publishing of the article. Mr. Renaud stated this is a standard cybersecurity practice called responsible disclosure. He stated after speaking with Professor Khan, he sent him the same steps he had sent to Mallory McGowin. He stated Professor Khan replicated the process and wrote him back stating he located a major security flaw on the page, and that social security numbers were being exposed on it. He stated he did not go through the process with him. Mr. Renaud stated he assumed Professor Khan replicated his process but was unsure of the exact steps he used. Mr. Renaud stated he sent the steps to Professor Khan on the night of Monday, October 11, 2021, and received verification on the morning of Tuesday, October 12, 2021, he had located the security flaw.

7. Mr. Renaud stated after he received confirmation from Professor Khan, he emailed DESE and ended up communicating with Mallory McGowin at DESE and notified them about the security flaw. I asked Mr. Renaud to explain his communications with Mrs. McGowin. He stated he thought most of their communication was via telephone. He stated Mrs. McGowin did not say much, but Tuesday and Wednesday he was trying to work toward an interview and DESE and OA were going through their systems to determine if there were any other security flaws. He stated she called him after the first email, she thanked him for telling them about the vulnerability and they had not been aware of it. He stated he told her he wanted an interview from someone with DESE and a technology person from DESE, or ideally someone from OA ITSD to speak on the vulnerability, and answer questions they could publish. I asked him if he was going to ask about the development of the website or the cybersecurity, and he stated he was unsure, but stated probably a little of both. He stated they were more interested in the scope of it and how long this had been going on because they had been estimates around 100,000 educator's social security numbers could have been compromised. He stated he thought it could have been more than that because he was only thinking about the current year, and he stated he observed information indicating other years of information and possibly retiree's social security numbers were in the database.

8. I asked him if he would have conducted the interview himself, and he indicated it would have been him. I asked Mr. Renaud about the timeline discussed with DESE. He stated in the initial email they indicated they would like to run the story within 48 hours. He stated during their conversation, they later asked them to delay the story due to them still checking security features and he stated he told Mrs. McGowin they were not wanting to harm anyone so if they needed more time it was okay. Mr. Renaud reiterated they were willing to hold the article until the problem had been corrected.

9. Mr. Renaud stated he spoke with Mrs. McGowin multiple times on Tuesday, October 12, 2021, and Wednesday, October 13, 2021. He stated on Wednesday, while he was speaking with Mrs. McGowin, he was attempting to make arrangements to conduct an interview and he asked if they had located any other security flaws. He stated Mrs. McGowin told him as far as she knew, this was the only application where this was located. He stated Mrs. McGowin texted him on the afternoon of Wednesday, October 13, 2021, and asked for the legal counsel's contact for the Post-Dispatch. He stated after he received the message, he told his editor, who attempted to contact her, but she did not answer.

10. I asked Mr. Renaud questions regarding the source code and the purpose of him looking at it on DESE's website. He again reiterated he was building data for analysis and viewed the source code to discover how the forum worked. I asked him about the data located within the source code, which would be encoded. I asked him to walk me through how he would go about turning that into usable data to be read. He stated he regularly sees encoded information and knew webpage information was encoded. I asked him if it was normal practice to view source code information for building databases and he stated it was and referred to it as "data journalism." He described it as collecting publicly available data and running analysis on it to determine if there were trends.

11. While reviewing the timeline of the events with Mr. Renaud, he spoke of the difference between a breach and a vulnerability or an exposure. He described a breach would be someone logging into a computer system they did not have access to pull information out. He described an exposure as something anyone could have found. I asked him if some of the data he looked at was encoded versus encrypted and he stated he only looked at encoded data anyone else could have seen. He stated he did not look at any encrypted data because he did not have any passwords. He stated nothing he looked at was encrypted and he did not decrypt anything.

12. I asked him if he had computer experience, and he stated he completed computer science classes but did not have a computer degree, nor did he have a minor or major in computer science. Mr. Renaud stated the forum was a public forum and anyone that used it could have accessed the same information. He stated he thought they did a good public service bringing this to DESE's attention and was proud of the way The Post-Dispatch handled it.

13. I asked Mr. Renaud how he was sorting information when accessing the public portal. He stated he was only wanting information for the St. Louis area. He said he did that by using drop down boxes and selecting certain areas. He said another way was if you knew the educators last name and last four digits of their social security number. He stated he did not have any of that information, he used the public portal with the dropdown boxes. I asked Mr. Renaud when he looked at the source code, if every teacher in the drop boxes social security number was visible, and he stated the page would only let you look at one educator at a time so only one social security number was there at a time.

14. I asked Mr. Renaud if they do this type of work at the office or at his house or home, and he stated both. I asked him if while they were creating these databases, if they did this on a secure computer network or would they do this type of work on a laptop at their desk, and he stated on a laptop at their desk. I asked him where they would store this type of data or if it was secured, and he stated they do not build databases of private information, so they do not have a need to have it secured. I asked Mr. Renaud if all this was done using the public website, a computer,

and he indicated that was correct. I asked him what kind of computers they use, and he stated they use multiple types of computers, but indicated it was a desktop. I asked him if anyone else discovered this with him and he stated no one else discovered this with him. I asked him if they were using a Virtual Private Network (VPN) while doing this type of research, and he stated they used their corporate network.

15. I asked Mr. Renaud how he treated the social security numbers he located. He stated he called the person on the phone and spoke to them and verified the numbers. I asked him if he would be willing to tell me the names of the persons he used to verify the information, and he indicated they were confidential sources and declined to provide their information. I asked him if the sources had expressed any issues to him regarding identity theft issues and he stated he had not been informed of any issues from them.

16. I asked him about his intention for this information when this was discovered, and he again confirmed he was gathering the information for analysis. At this point Mr. Martineau stated he wanted it to be clear, the purpose was to build a database of teacher certifications not social security numbers. Mr. Renaud again confirmed for them to put the data from the website into the database, he needed to view the source code. Mr. Renaud stated he did not know where DESE's building is located. He stated the last time he was in Jefferson City was in 2016 for robotics event at the House of Representatives.

17. During the interview, Mr. Martineau provided me with printouts of the email communications between Mr. Renaud and Mrs. McGowin, and Mr. Renaud and Professor Khan. He also provided me with a printout of the text message conversation between Mr. Renaud and Mrs. McGowin. Mr. Martineau indicated there were other documents preserved relating to the editorial process and internal Post-Dispatch communications.

18. I asked Mr. Renaud why he thought this happened. He stated he thought it was because they were using the number as an identification in the backend of their database. I asked him if that would be normal from what he has seen and stated it would not be. He stated from what he has seen, the private information would be held in a separate table that does not talk to the web.

19. I asked him if he remembered previous contacts with Mrs. McGowin, and he stated he did not. I asked him if knew Professor Khan prior to this, and he stated he did not. I asked him if any other cybersecurity contacts got back with him, and he stated they did not get back with them in time. I asked him if he sent the process to anyone else, and he stated he sent it to Professor Khan and Mrs. McGowin. He stated he would have preferred to send the process to an actual tech person but was instructed to send it to Mrs. McGowin via DESE's media inquiry email.

20. I asked him if he took any of this information out of the office, and he stated he did some work at home. He stated he has a home computer and remotes into his computer at the Post-Dispatch Office.

21. Mr. Martineau asked if he could clarify a couple points with Mr. Renaud. Mr. Martineau asked Mr. Renaud if everything he looked at was on DESE's public website, and Mr. Renaud stated, "Yes." Mr. Martineau asked Mr. Renaud if he thought he was authorized to view that website and view what was on it, and Mr. Renaud stated, "Yes. It was a public website that had

been around for years." Mr. Martineau asked Mr. Renaud if he was looking for social security numbers, and Mr. Renaud stated he did not intend to find any social security numbers. Mr. Martineau asked if he intended to find any social security numbers, and he indicated he did not. Mr. Martineau asked if Mr. Renaud retained any social security numbers, and he stated he did not. Mr. Martineau asked Mr. Renaud if he disclosed the social security number's he located to anyone other than three people who the number belonged to, and he indicated he did not. Mr. Martineau asked Mr. Renaud if he possessed the social security numbers on a storage device or piece of paper, and he indicated he did not. Mr. Martineau asked Mr. Renaud if he retained any of the social security numbers and he stated he did not.

22. Mr. Martineau stated if clarification was required on information obtained later if they would speak with me again and he stated they wanted to cooperate and would be open to the option of speaking with me again.

23. This interview was recorded using my patrol assigned digital voice recorder. Mr. Martineau also recorded the interview using the recording device installed in the conference room.

24. The following items are attached to this report:

a. A copy of the audio recording.
b. A copy of the email communications and text messages provided to me by Mr. Martineau.
c. A copy of the letter drafted by Mr. Martineau addressed to Corporal Dustin Reed, Cole County Prosecuting Attorney Locke Thompson, and myself.

25. This investigation remains open.

K. A. Seabaugh, Corporal
Division of Drug and Crime Control

KAS:lab

Attachments:
6.1 Emails provided by Josh Renaud's Attorney
6.2 Letter from Post-Dispatch Attorney
6.3 Screenshots

Media Attachment:
6.1 Joshua Renaud Interview

SUPPLEMENT 7 - INTERVIEW DOCTOR SHAJI KHAN
DATE OF REPORT - OCTOBER 25, 2021

1. On October 25, 2021, at approximately 0939 hours, I interviewed Shaji Khan at the St. Louis Missouri Bar Association, located at 555 Washington Avenue, St. Louis, Missouri. The interview was arranged through Dr. Khan's attorney, Elad Gross, who was present for the interview. Dr. Khan was interviewed in reference to Josh Renaud contacting him to verify and comment on security vulnerabilities located on the Department of Elementary and Secondary Education's (DESE) website, specifically the Educator Qualifications Portal.

2. I began the interview by asking Dr. Khan how he was employed and his education levels. Dr. Khan stated he had two undergraduate degrees, a master's degree in Computer Science, and a PhD in Business Administration with an emphasis in or on Information Systems. He stated he has been teaching since 2007, but became faculty in 2014. He stated he currently teaches cybersecurity at the University of Missouri-St. Louis. He stated he created the cybersecurity programs at the university, created cybersecurity courses taught at the university, developed cybersecurity laboratories, and teaches cybersecurity and cybersecurity ethics courses at the University of Missouri-St. Louis.

3. I asked Dr. Khan when Mr. Renaud contacted him regarding the security vulnerability, he located on DESE's website, and he stated he was contacted on October 11, 2021. He stated when he received the first email from Mr. Renaud, he went to the Post-Dispatch's website to verify Mr. Renaud was actually a reporter. Dr. Khan stated it was not uncommon for him to receive media contacts, and he always verifies the person is a real reporter before contacting them. He stated the email indicated he had unexpectedly located something, and he would like Dr. Khan to verify it and comment on it. He advised he informed Mr. Renaud he did need to verify what he found, but he must also disclose it responsibly. He stated he informed Mr. Renaud he would verify the information and comment on it only if confirmed he would not publish the story before the State of Missouri had a chance to take it down. He advised his first rule of business in his field is, "Do no harm." Dr. Khan stated he has made some disclosures in the past, and he stated you must notify them and give them time to fix the problem.

4. Dr. Khan stated Mr. Renaud asked if he sent him the HTML code, could he verify it, and Dr. Khan advised he could not because that was not how it worked. Dr. Khan then stated before he agreed to verify and comment, he again reiterated he confirmed with Mr. Renaud they would not publish the article prior to notifying the State of Missouri and allowing them to correct the problem. He advised, Mr. Renaud told him they were going to notify the state of the problem, then were planning on running the story 24 to 48 hours later. He indicated he wanted to verify this was enough time, so he consulted with the media staff at the University of Missouri-St. Louis with initial suspicions of the article possibly being published before the state was notified. He stated the media staff said it was up to Dr. Khan if he wished to proceed with the process, and

advised him to call Mr. Renaud, so Dr. Khan emailed Mr. Renaud his phone number and asked him to call him.

5. Dr. Khan advised when he spoke with Mr. Renaud, he (Dr. Khan) advised Mr. Renaud the last time he notified the Chief Security Officer of the State of Missouri of an issue he located on a website, it took the state approximately six months to fix it and he (Mr. Renaud) needed to make sure the state at least took the application offline before the article was published. He indicated he also advised Mr. Renaud he needed to ensure the teachers were not harmed during this process. He again stated after Mr. Renaud informed him, he would not publish the article before the state had taken the application offline, he agreed to verify the process and advised Mr. Renaud he followed standard disclosure practices. Dr. Khan asked Mr. Renaud to explain to him how to replicate the situation. Dr. Khan indicated he was not going to take Mr. Renaud's word for how he did it, and he would not do exactly what he did. He stated Mr. Renaud then sent him the steps to replicate the process. Dr. Khan then explained standard practice for disclosures in the cybersecurity field. He indicated you do not just tell the person there is a problem, you specifically tell them where the problem is occurring.

6. Dr. Khan stated he completed the process in a few minutes and advised when he initially looked at the steps and saw the term "view state" he already knew where this was going. He stated this has been a continual problem they have seen for the past 10 to 12 years. He stated he was then able to verify the flaw and during this process, he asked for the specific application. Dr. Khan advised he does not click on links sent to him and wanted the specific application to verify he could access it from a public site. He stated he was able to navigate to the Educator Qualification portal and verified the flaw. He indicated he then emailed Mr. Renaud and advised him when he published the article to not specifically detail the flaw. He stated he told him this to keep "bad actors" from trying to exploit security vulnerabilities. Dr. Khan stated this specific problem has been known for so long it was "mind boggling" that it still existed in the state application. He stated he told Mr. Renaud the State of Missouri should do a thorough audit of all applications. Then he stated he commented this was a common problem, and something he shows his students while teaching. He advised he also informed Mr. Renaud his (Dr. Khan's) comment is contingent upon Mr. Renaud verifying the number he was actually seeing was social security numbers. He stated Mr. Renaud emailed him and said he had confirmed the numbers were social security numbers with a few teachers he knew. He also advised Mr. Renaud asked him what the teachers should do, and he stated there was not much they could do except monitor their credit, and if they observed something, they should place a freeze on their credit. He stated teachers should start questioning why someone would need your social security number. He stated social security numbers were never meant to uniquely identify people, they were created to keep track of who gets social security benefits at what time. He stated currently people use them as an identifier and people should be skeptical of telling anyone their social security number.

7. Dr. Khan stated after he commented he moved on and stated he thought it would be a good case study for his students. Dr. Khan advised a few days later he was contacted by the Post-Dispatch Editor and was asked about the difference between encoding and encryption. He indicated when he was called, he was unaware of a press releases and the comments made by Governor Parson. He stated the editor advised him Mr. Renaud was taking scrutiny for the story, so Dr. Khan said he researched it and saw what he described as "the Governor's crazy reaction." He stated when he read DESE's press release, he saw where they referenced a "hacker" took

three records and spun it in a manner in which a normal teacher would be glad it was only three and theirs was not affected. He advised this is a dangerous thing to do and described it as "irresponsible at best, and illegal at worst." He advised when an organization is responsible for a security breach, he stated they are bound by law and required to tell the affected individuals what happened and give them an indication of how much data was in danger. He stated when DESE told them only three people's information was accessed and it looks like nobody else was affected, it was actually wrong because there was no way to determine whose social security number was able to be accessed that way. Dr. Kahn described this as a breach in confidentiality which he stated was something you cannot take back. He stated, given this security flaw, when your personal information is out, there is no taking it back so you could not tell people their data was not affected. He stated the way the information was spun was "ridiculous at best." He stated he never expected this to be big news.

8. I asked Dr. Khan to explain the difference between encoding and encryption. Dr. Khan advised this particular application was a public website so anyone could access this website and look at a teacher's credentials. He indicated when someone searched for a teacher, their data was sent from the server to the browser and was "literally sitting right there." He stated within this data, they were embedding social security numbers. He advised this data is encoded which translates the format of the data from one form to another. He indicated when this done for Hypertext Transfer Protocol (HTTP) which is the protocol for sending data back and forth, there are some characters that do not translate so the data is encoded to meet formatting requirements. He indicated encoding means "one format to another" and again stated the purpose of formatting is to "meet formatting requirements of sending data from one place to another." He advised that encoding does nothing to hide sensitive data, and that is not its purpose. He then made the following analogy, if a person walks into a room and shouts their social security number in Chinese, and if anyone in the room understands what they said, they are charging that person with unauthorized access. He stated it is well known the "view state" information is encoded, not encrypted. He advised a better way to do this, would be to encrypt the data. He stated encryption would be once you scramble the data, you could not view it without the decryption key, which would be how you protect sensitive data. He indicated with how this process was occurring, the server sent the information to the browser, which he advised was a problem. He indicated using social security numbers in this manner, sent the social security number of the person to every person who viewed their information on the website. He stated a better way would have been to encrypt the data in the view state. He advised a better way would be to ask why they would need to send a person's social security number to a person's browser? He stated that did not make sense.

9. I asked Dr. Khan if it was common knowledge in his field to know that "view state" information is encoded, and he indicated it was. I asked him to rate the computer level of a person to access this data and he advised to anyone who has done web application development, it would be like a basic "101." He stated most people do not know what their computer is doing. He stated for someone in the security field, this would be one of the worst mistakes they could make.

10. I asked Dr. Khan about the steps sent to him by Mr. Renaud. Previously, Dr. Khan stated when he saw the "view source code" in the steps, he knew where this was going. I asked him to walk me through how he knew where the steps were leading. He advised he had seen a lot of these types of flaws before, and as soon as he saw the "view state" and encoding, he knew where

it was going. He stated he did not follow the exact steps sent to him, because he knew where it was going. He stated he wanted the steps sent to him so he could verify this was occurring on the public facing site. He indicated sometimes things are reported to be a problem but are not on the public side, so he wanted to ensure this was on a public site that he could find on his own without following instructions. He stated by the time he was done looking, he realized how bad the situation was and indicated the state needed to be notified immediately. I verified with Dr. Khan that although he was sent the link to the application, he found it on his own, and he indicated that was correct.

11. I asked Dr. Khan about his verification process. I asked him if he picked a random teacher from the list, or someone he knew. He advised he was not familiar with what DESE did, so he initially looked for someone he knew but then picked an educator in the area where he lived. He stated he then viewed the "view state" and found the data right away. I asked him if he contacted the teacher and he indicated he did not. I asked him if he knew the name of the teacher, and he advised he could look it up. I advised Dr. Khan if he would be willing to provide me with their information, I would like to contact that person to ask them about identity theft issues. Dr. Khan advised this problem had been going on for so long it would be hard to determine if the person had identity theft issues, to verify this was the source of the problem. He then talked about data attacks from nations such as China and Russia where they have breached databases containing personal identifying information. He indicated with this vulnerability he would find it hard to believe this information is not already out somewhere. He stated he would share the information, but it would be hard to link anything that may have happened with the identity theft to this issue.

12. Dr. Khan indicated he was not interested in disclosing people's private information. I asked him if he kept this information, and he stated he documented the vulnerability by capturing screenshots. He advised he saved the screenshots on an encrypted drive off the computer and off the network. I asked him if he was planning on using it for a teaching aide and he stated if he did, he would have redacted it. Mr. Gross stated they were waiting until we spoke with him before they did anything with it. Mr. Gross advised they were willing to get rid of it, they did not want to do anything before I spoke with Dr. Khan. Dr. Khan stated he did not have the thumb drive with him.

13. I asked Dr. Khan if this type of flaw was something commonly seen. He indicated this was a common problem. He advised in 2016, he wanted to verify his voter registration, so he Googled "check voter registration" on his smart phone. He stated he clicked on the Missouri Secretary of State's website and as soon as the page loaded, he observed the page was loading through "plain http" which he stated means there is no encryption and anything he types in there is free for anyone to see. He said he was not typing anything into the website, so he went and verified it on a computer. He stated the website was indexed in Google in this way, so anyone who Googled the Secretary of State's website, would be routed through that link which was and insecure Uniform Resource Locator (URL). He stated he emailed the Chief Security Officer and advised them of the problem and the fix for it. He stated he received an email thanking him for reporting the issue and was advised they would correct the issue. He stated while teaching classes, his students find security vulnerabilities on websites regularly. Dr. Khan indicated people look for security vulnerabilities are called Security Researchers and approximately 500,000 vulnerabilities are housed by the Federal Government in the National Vulnerabilities Database. He advised he receives regular updates regarding security flaws in programs that are

sent out to notify people. He also stated software updates are sent out to patch security flaws and advised to always update programs.

14. I asked him what type of device he used to verify this process and he indicated it was performed on a computer. I asked him if the computer had any special tools on the computer he used during this process and he stated he did not. He stated this process did not need any special tools. I verified with him again, this was all performed on a public facing website, not using any special tools to access any information that was not available there, and he indicated that was correct. Mr. Gross clarified this was not in an area which a required a log in or password and nothing was protecting the information.

15. I asked Dr. Khan about the term "hacking" which was brought up earlier. I asked him how he would characterize hacking, and he stated it was a broad term. I asked him if hacking would require someone to use special tools to access information in contrast to something from a public facing website. Dr. Khan indicated the hacking can span in a number of ways, and the process he was talking about required nothing. Dr. Khan advised he could imagine the flaws in the design process for why this happened and spoke of how security needs to be built into the process.

16. I asked Dr. Khan about him telling Mr. Renaud to not put the specific security flaw in the publication. I asked him if he knew Mr. Renaud knew the exact flaw, and he advised he did not know Mr. Renaud's level of understanding of the problem. He indicated he was only concerned if the view state information was sent out, every person in the cybersecurity field would know what he was talking about. Dr. Khan then began explaining information known in the Microsoft Documentation Security Briefing from 2010, where this specific issue was addressed, and people were advised to never put sensitive information in view state because you would be sending that information to every person that visits your site. He also advised they said if you have no choice but to put the information in there, the data must be encrypted.

17. I asked Dr. Khan if he discussed with Mr. Renaud what he was specifically doing when he found this information, and he stated he did not. Dr. Khan clarified he did not know what Mr. Renaud was doing, he had his own theories but stated nothing he saw raised any red flags about what Mr. Renaud was doing. I asked him if he receives media inquiries of this nature regularly, and he stated he does receive media inquiries, but this was the first time he had been asked to verify a security flaw process.

18. I asked him if he had ever been brought into testify in court as an expert and he indicated he had not. I made arrangements with Mr. Gross and Dr. Khan to retrieve a USB drive from them containing screenshots of Dr. Khan's process. Dr. Khan again stated he took screenshots to document the vulnerability.

19. This interview was recorded using my patrol assigned digital voice recorder. This interview was also recorded by Mr. Gross.

20. After conducting the interview, I met Mr. Gross and Dr. Khan at 1600 Clarkson Road, Chesterfield, Missouri. At approximately 1148 hours, I was provided a USB drive containing the screenshots from Dr. Khan.

21. The following items are attached to this report:

a. A copy of the audio recording.
b. A copy of the screenshots captured by Dr. Khan.
c. A copy of the timeline/litigation hold request and demand with contains links to the Microsoft Security Briefing provided to me by Mr. Gross which was prepared by Dr. Khan and Mr. Gross.

22. This investigation remains open.

K. A. Seabaugh, Corporal
Division of Drug and Crime Control

KAS:lab

Media Attachments:
7.1 Screenshots from Dr. Khan
7.2 Dr. Shaji Khan Interview

SUPPLEMENT 8 - CASE CLOSED
DATE OF REPORT - OCTOBER 29, 2021

1. During the course of this investigation, I was in contact with Cole County Prosecuting Attorney William Locke Thompson. While communicating with Prosecutor Thompson, he indicated when the investigation was complete, he requested the investigative file be sent to his office for review.

2. This investigation is closed, and the investigative file will be sent to Prosecutor Thompson for review.

K. A. Seabaugh, Corporal
Division of Drug and Crime Control

KAS:lab