The Office of Secretary of State

INVESTIGATION REPORT

Subject: KSU Deletion of CES Server Data

Date of Incident: July 7, 2017

Location of Incident: KSU CES

Date Reported: October 30, 2017

Name of Investigator: Ryan Germany

I was asked to look into the allegations that data was deleted from servers housed at the KSU Center for Election Systems. I have reviewed applicable documents and spoken to various involved parties. After doing so, I conclude that:

(1) KSU IT's actions in repurposing the server in question were consistent with standard IT practices and were not undertaken to delete evidence.

(2) The concern that the data is lost is unfounded. The indication is that the FBI retained an image of the data on those servers as part of their investigation. Our office has taken all applicable steps to get a copy of that imaged data.

TIMELINE

On Tuesday, October 24, 2017, our office learned that KSU IT erased the data and re-purposed the server after the alleged March 1, 2017 security incident. Our office did not direct that action, was not consulted prior to that action, and had no knowledge it was taking place. KSU IT took this action in conjunction with an After Action Report that was generated by KSU IT. That report states that KSU IT, within 60 minutes of receiving knowledge of the alleged vulnerability, had blocked access to the server. The next day, KSU IT physically took possession of the server. On March 3, 2017, the FBI took possession of the server as part of their investigation into the alleged security incident. On March 17, 2017, the FBI returned the server to KSU IT. The server in question has not been used for elections since KSU IT was notified of the potential vulnerability on March 1, 2017, and it is not a necessary component to Georgia's election system.

The alleged March 1, 2017 security incident led to the creation of an After Action Report within KSU, and on April 18, 2017, it was recommended that the server be "formatted and reinstalled on CES isolated network." That recommendation was completed on July 7, 2017. Neither KSU IT nor CES consulted with or notified our office of their actions identified in the After Action

Report. I have discussed the KSU After Action Report with SOS IT and have determined that KSU IT acted pursuant to standard IT principles following a security incident with no indication of improper motivation or intent.

ISSUES WITH TIMELY COMMUNICATION

Confusion surrounding this issue could have been avoided with better communication between our office, CES, and the Attorney General's office. In an October 6, 2017 email, the Attorney General's office notified counsel for the other parties in the litigation that data had been deleted from servers at KSU. Our office was not alerted to this potential issue until the media began to ask questions about it on October 24, 2017. I recommend that we put in place procedures to ensure more timely communication on these issues from both CES and the Attorney General's office. Moving CES functionality inside the Secretary of State's office (a process that is currently underway and slated for completion by the end of 2017) will help alleviate that issue as it relates to CES.

AVAILABILITY OF THE DATA

All current indications are that the FBI has an image of the data that was on the server. On Friday, October 27, 2017, SOS Elections Director delivered a hard drive to the FBI for the FBI to upload a copy of the data to ensure its safekeeping. It is not likely that the data on those servers has any relevance to plaintiffs' claims in the litigation, and the concern that the data was lost is unfounded. It appears it will be available for use in the litigation. The process of getting the data from the FBI is ongoing.

CONCLUSION

After reviewing this situation, it is clear that:

(1) KSU IT acted in accordance with standard IT procedures without any oversight, permission, or direction from the Secretary of State's office.

(2) The concern that the data was lost is unfounded. Current indication is that the FBI retained an image of the data on those servers as part of their investigation and that it will be available for use in the ongoing litigation.

(3) Given those conclusions, the narrative asserted in the media that the data was nefariously deleted and is no longer available is completely false and without merit.

CRG