IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

DONNA CURLING, ET AL., **Plaintiffs,** **v.** **BRAD RAFFENSPERGER, ET AL.,** **Defendants.**	**Civil Action No. 1:17-CV-2989-AT**

COALITION PLAINTIFFS' REPLY BRIEF ON EVIDENTIARY PRESUMPTION ARISING FROM SPOLIATION OF EVIDENCE

Answering the State Defendants' Introduction and Background

Employing language that can only be described as Orwellian, the State Defendants attempt to sanitize their violations of the law by referring to their spoliation of evidence as "repurposing." (Doc. 558 at 2). "Repurposing" is code for wiping servers and destroying data, much like shredding documents "repurposes" them into trash.

One of the risks of not trading in the truth is that you tend to forget the stories you have previously told. In January 2018, the then-Secretary of State Brian Kemp was anything but defending destruction of the CES servers. Rather, on January 13, 2018, in Hall County, Georgia, Kemp said the decision to wipe the servers was

"really incompetence on their part that we had no knowledge of."[1] In October 2017, KSU told the Associated Press that the server wipe was "standard operating procedure," while Kemp's office said at the time it was "undeniable ineptitude."[2] Now the State Defendants deny the undeniable ineptitude and defend the indefensible decision.

Whether the State Defendants or their agent, KSU, had plans to purge data prior to the filing of this litigation has no affect upon the State Defendants' obligations that arose the moment they knew litigation was likely.[3] As this Court has already noted, after the State Defendants were on notice of the litigation ***and removed the case to federal court***—and had already destroyed all data on the 'elections.kennesaw.edu' server, the State Defendants, directly or through their

---

[1] *See* https://www.gainesvilletimes.com/news/kemp-universitys-blunder-led-elections-server-issue/ Interestingly, to counsel's knowledge, Governor Kemp never suggested during the campaign, as lawyers for the State Defendants do now, that the wiping of the CES servers and the destruction of evidence was perfectly acceptable.

[2] *Id.*

[3] The State Defendants completely ignore in their brief the Coalition Plaintiffs' argument that, pursuant to O.C.G.A. §§ 21-2-52 and 21-2-73, the State had an independent statutory obligation to retain all records of the election for a period of 24 months--no mention, much less a denial. So, the notion that it was standard operating procedure to destroy evidence related to the outcome of elections within months of the elections constitute willful disregard of the law—as appears to be the State's wont.

agents, wiped a second server, the 'unicoi.kennesaw.edu' server, further destroying relevant evidence.

The State Defendants complain that Rule 7(b)(1) of the Federal Rules of Civil Procedure, requires that requests for court orders be made by motion. Actually, the Rule provides as follows:

> A request for a court order must be made by motion. The motion must:
>
> (A) be in writing unless made during a hearing or trial;
> (B) state with particularity the grounds for seeking the order; and
> (C) state the relief sought.

The Coalition Plaintiffs' spoliation brief was filed in support of Plaintiffs' Preliminary Injunction Motion, was in writing but offered during a hearing, and states the relief sought. The last sentence of the brief reads: "Defendants' spoliation of evidence should minimally result in a presumption that the evidence destroyed by Defendants would tend to prove the merits of Plaintiffs' claims *and should weigh heavily in the Court's assessment of whether to grant injunctive relief*." The filing satisfied all the requirements of Rule 7(b)(1).

Having no argument with any factual or legal merit, the State Defendants claim that the Coalition Plaintiffs "apparently shared their Brief with reporters ahead of time, because a reporter contacted the Secretary of State's office immediately

after filing seeking comment and outlining the contents of the brief." (Doc. 558 at 3-4). Not that it matters, but the Coalition Plaintiffs hereby certify to the Court that they did not share the brief with the press ahead of its submission. It is also worth noting that many legal reporters subscribe to Pacer, and the brief was filed at 1:30 PM on July 25, 2019. The email from Ms. McDonald with the Daily Report was sent to the Secretary of State's office at 3:11 PM. The Coalition Plaintiffs credit Ms. McDonald with sufficient reading acuity to absorb a 20-page brief in an hour and forty-one minutes.

Answering the State Defendants' Argument
The Relevant Evidence on the CES Servers

The State Defendants contend that "Plaintiffs' original claims had nothing to do with any election that occurred while the CES webserver was in use." (Doc. 558 at 11 n.5). The State Defendants point out that the wiped servers were taken out of service in March 2017, while the Coalition Plaintiffs' claims initially related to the April and June 2017 special election and runoff for the Sixth Congressional District.

Recalling the timeline here is useful: CES became aware of Chris Grayson accessing the 'elections.kennesaw.edu' server on March 1, 2017.[4] On March 2,

[4] *See* CES/KSU memorandum re March 1, 2017 incident, attached hereto as Exhibit "A."

2017, the KSU University Technology Services ("UTIS") Information Security Office "pulled apache and Drupal logs…and seized the 'elections.kennesaw.edu' server."[5] On March 3, the FBI was contacted, and FBI took possession of "the impacted server," indicating that only a single server was turned over to the FBI.[6]

The State Defendants state in footnote 1 of their Response that there were three servers in use at CES: (i) a ballot building GEMS server; (ii) an EPIC server that generated information used in ExpressPoll check-in machines; and (iii) the 'elections.kennesaw.edu' server (recently renamed the "webserver" by State Defendants) "that was used for occasionally transmitting information to counties." For clarity, the Coalition Plaintiffs will continue to refer to the server as it has been referred to throughout the litigation: 'elections.kennesaw.edu.'

The State Defendants' guileful efforts to diminish the importance of the "impacted server" ('elections.kennesaw.edu') are belied by the description of that server by Michael Barnes, Director of CES, when attempting to retrieve data from the server then in the possession of the FBI. Mr. Barnes explained:

---

[5] *Id.* It is troubling that the State Defendants, who, as will be seen, apparently scoured the KSU memo closely, failed to mention to the Court in their Response that logs were pulled from the server and have failed to produce any such logs to the Court or Plaintiffs.

[6] *Id.*

> We would like to retrieve certain records from elections.kennesaw.edu that support our daily office activities, items such as inventory records, workflow databases used during our ballot building efforts, and operation manuals….We would like to retrieve the entire cesuser directory if possible. [7]

That request was passed from Mr. Barnes to Steven Gay at KSU, who, in turn, forwarded the request to FBI Special Agent William D. Ware, II. In his forwarding email, Mr. Gay explained that CES did "not have a backup" of the seized server.[8] This exchange of emails exposes two areas of concern regarding the State Defendants' candor with the Court: First, the emails seriously call into question the State Defendants' misleading description of the elections.kennesaw.edu/webserver. One is left to wonder how a server that, as described by the State Defendants, only "occasionally transmit[s] information to counties" would support "[CES's] daily office activities…[and] workflow databases used during…[CES's] ballot building effort." Additionally, throughout the Response brief, the State Defendants refer to the Unicoi server as a backup server,[9] but Mr. Gay's email indicates that CES had

---

[7] *See* March 15, 2017 email from Mr. Gay to Mr. Barnes and from Mr. Gay to Mr. Ware, which was identified in the Barnes Deposition at Exhibit 21, attached hereto as Exhibit "B." (CGG0000026).

[8] *See id.*

[9] *See* Response brief, Doc. 558 at 9, 10, and 11.

no backup for the data on the impacted server that Mr. Barnes was requesting. Which leaves open the issue of what unique data the Unicoi server contained, as it is undisputed that it was wiped and destroyed with the FBI having made no image of it.

The State Defendants' contention that the elections.kennesaw.edu server had no relevant data stored on it is troubling on many additional levels. First, the contention ignores that, as Mr. Barnes email reveals, the data in the elections.kennesaw.edu server was most likely used to build ballots for the April and June 2017 elections. Erroneous or malicious code embedded in the server long before the April and June 2017 elections could have affected the outcome of those and later elections when data and directories salvaged from the elections.kennesaw.edu server was returned to the Secretary of State and used by Mr. Barnes to support "daily office activities."

In his affidavit,[10] Logan Lamb summarized the type of relevant working files on the elections.kennesaw.edu server and described ballot building and pollbook files accessed by Lamb that are consistent with the example list of files residing on that server prepared by Michael Barnes of CES. (Doc.507 at 61-62).

[10] (Doc. 2-1 at 91, 93)

Additionally, the State Defendants' argument suggests that they do not understand that for months (or perhaps years) prior to the April and June 2017 elections, the elections.kennesaw.edu server was open to any malevolent actor who possessed even moderate computer skills. Had any malicious code been downloaded into the CES servers that were being used to build ballots in March 2017 or before, the entire election system could have been infected for any election until such time as that code was detected and remediated. The fact that the CES servers were taken off line in March 2017 in no way changes that fact. And any record of who accessed the CES servers, when they were accessed, or mischief that was done with them when they were accessed has now been destroyed. This is not hypothetical; Logan Lamb and Chris Grayson both accessed the system without authorization or detection, fortunately wearing white hats.

The FBI Image

The State Defendants contend that the FBI made an image of the "impacted server"—the only server the FBI took possession of. The Unicoi server—the server the State Defendants refer to as a backup server, which according to Mr. Gay, did not backup directories used to support CES's "daily office activities"—was also

wiped. ***The State Defendants never explain why the Unicoi server was wiped and never offer a rationale for why doing so was not sanctionable spoliation.***[11]

The State Defendants note that the FBI currently has an image of the drive of the elections.kennesaw.edu server, but the State Defendants have avoided taking possession of that image. Counsel for the State Defendants served a notice of intent to subpoena a copy of the image but then decided not to issue the subpoena.[12] Then from October 2017 through the present date, the State Defendants have assiduously avoided taking possession of the image. On July 8, 2019, Kristine Green of the FBI advised counsel for the State Defendants as follows:

> I spoke with one of our investigators and he confirmed that he has the blank hard drive the State provided. Shortly after we received the drive, ***the State's counsel requested we temporarily discontinue the request to copy the drive***. We can re-initiate the request now, if necessary. I would like a letter of representation and notarized

[11] Apparently, the State Defendants have concluded that they can avoid the problem of the spoliation of the Unicoi server by dismissing it as a backup to the elections.kennesaw.edu server hoping everyone will thereafter forget about it. The State Defendants have made no showing that the Unicoi server had no unique data on it, and Mr. Gay's email to Mr. Ware indicates that the elections.kennesaw.edu server had no back up.

[12] *See* Exhibit "G" to initial Spoliation Brief (Doc. 548) and related text.

> signature from the Secretary of State's office before I actually turn over the drive.[13]

After the State Defendants asked the FBI to suspend efforts to make a copy of the drive, current counsel did provide the FBI will a letter of representation and a request for a copy of the image of the drive. Nine (9) days later, on July 17, 2019, at the Coalition Plaintiffs' counsel's urging, Mr. Belinfante followed up with Ms. Green, explaining that "Plaintiffs are the ones that have requested the drive."[14] Mr. Belinfante did mention that there was an upcoming hearing, but he did not suggest that the FBI expedite the request so that the Court would have access to information concerning the contents of the server at the hearing. The State Defendants, absent the urging of the Coalition Plaintiffs' counsel's cajoling, have little apparent interest in accessing the image. In any event, there may never be any way of knowing if the FBI's image is an accurate, unaltered or complete image of what KSU destroyed months later. This is one of the many reasons why the State's action is so prejudicial.

---

[13] *See* July 8, 2019 email exchange between Kristin Green and Josh Belinfante, attached hereto as Exhibit "C."

[14] *See* July 17, 2019 email exchange between Josh Belinfante and Kristin Green, attached hereto as Exhibit "D."

The State Defendants Attempt to Shift Blame

The State Defendants attempt to shift blame for their wrongdoing, claiming that the Coalition Plaintiffs knew of the State Defendants' plans to "repurpose" the servers pointing to a number of writings that revealed that intent. *See* Response, p. 10. Remarkably, in support of this argument, the State Defendants point to Exhibit "A" attached hereto, the April 18, 2017 CES/KSU memorandum, as the document that put Plaintiffs on notice of the fact that they were planning to destroy evidence. The relevant portion of the memo is buried at page 3 where the subject of replacing certain IT assets is mentioned. Among the listed assets is "elections.kennesaw.edu," which the memo proposes to "Format and reinstall on CES Isolated Network at NAS." No part of that language reveals any intent to wipe the server without making a copy. [15]

The memo also lists "unicoi.kennesaw.edu," which the memo recommends for "Surplus." Again, the notion of wiping the server without retaining a copy is nowhere mentioned. Nonetheless, these references translated into what the State

[15] The State Defendants also point to an email summarizing a KSU IT staff meeting referencing an instruction to "Wipe R610." *See* Response, Doc. 548 at 10. Of course, the Coalition Plaintiffs and their counsel would have had no way to know what that meant.

Defendants refer to as the "Coalition Plaintiffs [having] full knowledge of the plans for the servers." The memo put no person on notice of the plans to wipe the servers.

The Coalition Plaintiffs' initial brief points to no fewer than ten (10) written warnings the State Defendants were given to preserve all documents and data. But apparently the State Defendants believe that their purported announcement of a plan to violate the Election Code, to ignore their preservation duties, to disregard Plaintiffs' demands for preservation, and to evade this Court's orders regarding preservation absolves them of legal responsibility to do what the courts demand of the most unsophisticated layperson—scrupulous preservation of all relevant evidence.

The State Defendants next protest that Plaintiffs (and apparently the Court) were insufficiently specific about what data and devices they were obligated to maintain. The suggestion that the allegations in the initial Complaint, filed on July 3, 2017, did not disclose that the vulnerability of the 'elections.kennesaw.edu' server was central to the claims in the case is stunning. The first eight substantive pages of the Complaint set forth in detail the vulnerabilities of the 'elections.kennesaw.edu' server discovered by Logan Lamb and confirmed by Chris Grayson. The Complaint makes more than 50 references to one or both of the two destroyed servers. In spite of that, the State Defendants argue that "[t]he webserver and its backup were

completely irrelevant to any claims in the initial Complaint, filed on July 3, 2017." (Doc. 558 at p.9). That assertion is nothing short of astonishing.

Furthermore, the Director of CES, Michael Barnes, acknowledged that he received notice from counsel for KSU to preserve all documents before the servers were wiped. (Doc. 472-10 at 86). When asked whether he knew that the servers would be wiped, Barnes acknowledged that he knew that the servers might be "reused in some capacity." (Doc. 472-10 at 112).[16]

The State Defendants' assertions that they did not understand that they should not destroy evidence that would disclose who had accessed the system, when they accessed the system, and what they did while in the system is unfathomable. Moreover, the notion that it is incumbent upon Plaintiffs to identify for the State Defendants the elements of their election hardware that contain evidence relevant to the outcome of elections is intellectually dishonest. Indeed, the State Defendants acknowledge, in a footnote, that the "State Defendants ha[d] an obligation to preserve anything relevant to the claims beyond what was specifically listed" in preservation

[16] According to the Response brief, notice of re-use should have been notice of future spoliation to the Coalition Plaintiffs. If that is correct for a third party like the Coalition, it should have been abundantly clear to Mr. Barnes, as the Director of CES, what was about to happen to the servers, and given the notice he had of the State's preservation duties, he was obliged to ensure that the servers were not wiped. Obviously, he failed to discharge that duty.

letters.[17] The State Defendants' suggestion that they are somehow absolved of their failures to discharge well-known preservation obligations because Plaintiffs did not describe the election system in sufficient detail is, at once, sad and risible.

Next, the State Defendants announce they have taken a "consistent position that past election data on memory cards and internal memory of DREs is not erased by subsequent usage."[18] The State Defendants' position confuses consistency for accuracy. As the Coalition Plaintiffs indicated in their opening brief, the State Defendants' position regarding overwriting DRE internal memory and memory cards is "utter nonsense," according to cyber-security experts specializing in election

---

[17] *See* Response, p. 11 n. 5.

[18] *See* Response brief, Doc. 548 at 15. The State Defendants argue that the Coalition Plaintiffs have known this is the State's position for years. And since the Plaintiffs' very first preservation notice, Plaintiffs have demanded that the State "suspend the Defendant entities' data destruction and back up tape recycling policies." *See* July 10, 2017 preservation demand from Bryan Ward to State Defendants' counsel, attached as Exhibit "C" to Coalition Plaintiff's initial brief, Doc. 548. If the concept of "backup tapes" did not sufficiently covey the hope that storage media would be preserved, the message also demands the retention of "other storage media." Exhibit "E" to the Coalition Plaintiffs' initial brief specifically demanded preservation of all memory cards and DREs as of December 21, 2017, as did Exhibit "F" on June 21, 2018. In short, the State Defendants have blithely been destroying evidence for years—in violation of retention statutes cite in footnote 1 *supra*—and for more than two years the Coalition Plaintiffs have been demanding that they stop.

security.[19] First, the cited authority for the position, the Declaration of Mr. Barnes, more specifically states that the re-use of DREs does not "automatically overwrite prior election information." Mr. Barnes implicitly acknowledges that if the internal memory is already full, data within the internal memory will be overwritten, and same appears to be correct for memory cards.[20]

Additionally, Mr. Barnes, who holds a masters degree in Public Administration and no technology degrees, is not qualified to address technology issues. Dr. Richard A. DeMillo, however, has, and Dr. DeMillo reported in his November 21, 2018 declaration that "Preserving the electronic data in the internal memory of the DRE requires that no new election data be written onto the hard drive of DRE machines, no further use after the close of the election, including recounts, and that the DRE machines thus preserved be strictly physically secured and not deployed to polling places."[21] Dr. DeMillo further explained that he is unaware of any support for the

---

[19] https://whowhatwhy.org/2018/11/20/georgia-runoff-will-likely-contaminate-voting-machines-as-evidence/ (hereinafter "Georgia Runoff Contaminates Voting Machines") attached to Spoliation Brief as Exhibit "I" at 7-8.

[20] *See* Doc. 558, Barnes Dec. at ¶¶ 6-7.

[21] *See* DeMillo Declaration, ¶ 19, attached as Exhibit "J" to the initial Spoliation Brief.

State Defendants' position that "data from prior elections cannot be erased, overwritten, or otherwise lost when a new election is carried out."[22]

The bottom line is that the State Defendants are either attempting to mislead the Court or they are intentionally ignorant of the effects of their policies on the preservation of evidence. Either way, bad faith is established. The State Defendants do not know what evidence has been overwritten and destroyed because they stubbornly refuse to acknowledge the facts. As the Federal Circuit explained in *Micron Tech., Inc. v. Rambus, Inc.*, 645 F.3d 1311(Fed. Cir. 2011), "If it is shown that the spoliator acted in bad faith, ***the spoliator bears the "heavy burden" to show a lack of prejudice to the opposing party*** because '[a] party who is guilty of ... intentionally shredding documents ... should not easily be able to excuse the misconduct by claiming that the vanished documents were of minimal import.'" *Id.* at 1328 (*citing Anderson v. Cryovac, Inc.,* 862 F.2d 910, 925 (1st Cir.1988); *Coates v. Johnson & Johnson,* 756 F.2d 524, 551 (7th Cir.1985) ("The prevailing rule is that bad faith destruction of a document relevant to proof of an issue at trial gives rise to

[22] *See* First DeMillo Declaration, ¶ 23. Dr. DeMillo also declared that "[a]ll DRE machine electronic data must be preserved. Random sampling of DRE machines for preservation is not sufficient for safe-guarding of electronic evidence required to be used in discovery. *Id*. at ¶ 25.

a strong inference that production of the document would have been unfavorable to the party responsible for its destruction")).

The same can be said of the State Defendants. They have a statutory duty to preserve election materials, even when there is no litigation. They have ignored that. They knew the CES system was wide open to unauthorized access and that the only way to restore confidence in election integrity was to preserve servers, DREs, memory cards and all data. They ignored that. They received repeated warnings from Plaintiffs and the Court to preserve evidence. They ignored that. The State is powerful, but that does not mean it answers to no one.

In sum, the State Defendants' destruction of evidence increases the likelihood that Plaintiffs will succeed on the merits, providing further support for their Motion for Preliminary Injunction.

Respectfully submitted this 1st day of August 2019.

/s/ Cary Ichter
CARY ICHTER
Georgia Bar No. 382515
cichter@ichterdavis.com
ICHTER DAVIS LLC
3340 Peachtree Road NE,
Suite 1530
Atlanta, Georgia 30326
Tel.: 404.869.7600
Fax: 404.869.7610

/s/Bruce P. Brown
Bruce P. Brown
Georgia Bar No. 64460
BRUCE P. BROWN LAW LLC
1123 Zonolite Rd.
Suite 6
Atlanta, Georgia 30306
(404) 881-0700

/s/ Robert A. McGuire, III
Robert A. McGuire, III
Admitted *Pro Hac Vice* (ECF No. 125)
ROBERT MCGUIRE LAW FIRM
2703 Jahn Ave NW, Suite C-7
Gig Harbor, WA 98335
T: (844) 318-6730

/s/ Ezra D. Rosenberg
Ezra D. Rosenberg
John Powers
Co-Director, Voting Rights Project
Lawyers' Committee for Civil Rights Under Law
1500 K Street, NW, Suite 900
Washington, DC 20005
(202) 662-8345 (office)

Attorneys for Coalition for Good Governance

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

DONNA CURLING, ET AL., **Plaintiffs,** **v.** **BRIAN KEMP, ET AL.,** **Defendants.**	**Civil Action No. 1:17-CV-2989-AT**

CERTIFICATE OF COMPLIANCE

I hereby certify that the foregoing document has been prepared in accordance with the font type and margin requirements of LR 5.1, using font type of Times New Roman and a point size of 14.

/s/ Cary Ichter
Cary Ichter

EXHIBIT A

KENNESAW STATE UNIVERSITY
UITS Information Security Office

Center for Election Systems
Incident Date: March 1, 2017

Background

On Wednesday March 1st at 9:29pm, a member of the KSU UITS Information Security Office was contacted by a KSU faculty member regarding an alleged breach of data on the elections.kennesaw.edu server. UITS staff validated the vulnerability and notified the CIO regarding the incident. The data contained hosted on the identified server was outside the scope of student information and no student records are associated with this alleged breach. Log analysis identified that the largest file identified contained voter registration information for 6.7 million individuals.

Actions Taken

Within an hour of initial contact, the vulnerability was confirmed and firewall rules established to block access to elections.kennesaw.edu. On March 2, 2017, UITS-ISO pulled apache and Drupal logs, reported incident to USG, reset passwords, and seized the elections.kennesaw.edu server. On March 3, 2017, the FBI was engaged and the impacted server was turned over to FBI for investigation.

IT staff which were reporting within the Center for Election systems were realigned to report within the University Information Technology Services Information Security Office and a walkthrough of the area performed to validate the isolated internal network's segregation from the public network. The elections backup server – unicoi – was removed from the Center and physically secured within UITS ISO Evidence Storage.

On March 30th, KSU employees (President Olens, CIO, AVP Strategic Communications, Legal Counsel, CISO, CES Representatives) met with the FBI and US Attorney's Office regarding the outcome of the Federal Investigation. Chad Hunt shared that the investigation had yielded no data that "escalates to the point of breach". KSU Released a statement to the media on 3/31/17 as follows:

> **KENNESAW, Ga (Mar. 31, 2017)** –Kennesaw State officials report there is no indication of any illegal activity and that no personal information was compromised following unauthorized access of a dedicated server at the Center for Election Systems. KSU officials were briefed yesterday by the Federal Bureau of Investigation (FBI).
>
> University officials were first notified of the situation on March 1 and immediately isolated the server. Officials also contacted the Office of the Secretary of State and federal law enforcement, which prompted the FBI investigation. According to the FBI, the server was accessed by an outside security researcher. No student data was involved.
>
> "We are working with experts within the University System of Georgia and an outside firm to validate that KSU's systems are secured and meet best practice standards," said KSU President Sam Olens. "We greatly appreciate the speed and dedication of the FBI and the U.S. Attorney's Office in helping us resolve this issue."

KENNESAW STATE UNIVERSITY

UITS Information Security Office

Center for Election Systems

Incident Date: March 1, 2017

Financial Impact

None, although if it was determined that the data hosted on elections.kennesaw.edu was maliciously disclosed, the notification and credit monitoring would have been approximately $2 million.

Successes

The following list describes those actions or systems that worked as intended, or better than anticipated, during the execution of incident and breach response activities:

- The UITS ISO Incident Response process worked as intended, isolating the server and preserving evidence for later analysis and hand-off to federal authorities.
- The time between initial report and the server being isolated was approximately 60 minutes.
- The open dialog between the faculty incident reporter and the Office of the CIO staff facilitated timely notification and rapid response time.
- Having regular conversations with Legal Affairs, Strategic Communications, Center for Election Systems staff, and the Office of the CIO ensured that all parties were informed on developments, allowing for individual planning in each respective area.

Opportunities for Improvement

1. **Issue:** Poor understanding of risk posed by The Center for Election Systems IT systems. While a previous server scan and an external researcher had helped UITS understand the high threat level of CES systems, the lack of understanding the hosted data set led to an incomplete picture of the asset value. This resulted in the existence of a high risk server (High Asset Value / High Threat Level) which should have been prioritized.

Action Item(s): An objective 3rd party was hired to conduct a threat assessment for externally-facing applications. In addition, funding was secured to extend the current KSU vulnerability scanning engine to allow for external scans. Once these scans are complete, a thorough analysis of all vulnerable systems will quantify the threat level and remediation plans will be developed (and incorporated into remediation projects)

Action Item Owner(s): UITS Information Security Office

2. **Issue:** Elections webserver and Unicoi backup server are running a vulnerable version of Drupal and vulnerable to exploitation.

Action Items: Elections (externally-facing) was seized immediately and Unicoi (isolated network) was seized thereafter. Both were placed in ISO Secure Storage. UITS provisioned a dedicated virtual server, FS-ES, and business documents were moved to a newly provisioned server. This share is limited the CES subnet and CES Active Directory group users. Server administrators are limited to 2 UITS ISS Staff Members.

Action Item Owner: UITS-ISO, UITS-ISS, CES Staff

3. **Issue:** CES confidential data handling processes were not defined.

Action Items: Business processes were developed, documented, and implemented to ensure confidential data is handled appropriately. CES technicians were issued IronKey encrypted hard

drives and secure FTP transfers established with Georgia Secretary of State's Office. To date, all processes have been approved by the Georgia Secretary of State's Office.
Action Item Owner: UITS-ISO, CES Staff, Georgia Secretary of State Office

4. **Issue:** Center for Election System IT staff is not aligned with the University Information Technology Services, creating a scenario in which institutional risk could be accepted without CIO awareness.

Action Items: CES IT staff reporting structure realigned to mirror UITS TSS model. CES IT staff will report directly to UITS-ISO while directly supporting the CES. Additionally, all processes will align with USG and KSU data security policies. Strategically, UITS is launching a project to engage all external IT in order to better understand university-wide IT risk.
Action Item Owner: UITS-ISO, CES Staff

5. **Issue:** Room 105a, the elections private network data closet, was not latching properly due to lock/door misalignment.

Action Items: CISO contacted Chief of Police to have lock and door aligned. Work was completed within one business day. ISO to develop processes to review access logs on a scheduled basis.
Action Item Owner: UITS-ISO. KSU UPD, CES Staff

6. **Issue:** The elections private network data closet contains a live network jack to the [redacted] (Public network)

Action Items: UITS-ISO should acquire color-coded Ethernet Jack block-outs to "lock" all ports in the data closet to the public network AND to "lock" all ports to the private network outside the data closet. Key's should be maintained by ISS and ISO, necessitating consulting with UITS staff before connecting devices.
Action Item Owner: UITS-ISO, UITS-ISS

7. **Issue:** A number of IT Assets within the Center for Elections Systems have reached end-of-life and need to be replaced or migrated to different infrastructure.
    1. Rackmount UPS Battery backups (one displaying warning light)
    Recommendation: Replace batteries as needed and move under UITS ISS management
    2. 3com Switches – Age 10+ years -- No Support – L2 only
    Recommendation: Replace and move under UITS ISS management
    3. Dell 1950 (Windows Domain Controller) – Age 10+ years
    Recommendation: Surplus
    4. Dell PowerEdge R630 – Age 1 year
    Recommendation: Migrate services from Dell 1950 and move under UITS ISS management on CES Isolated Network
    5. EPIC – Vision Computer – Age Unknown – Ballot creation box
    Recommendation: Continue as ISO/CES managed
    6. EPIC Files – Dell 1900 – Age 6+ years – Ballot backups
    Recommendation: Surplus
    7. NAS – Dell 1900 – Age 6+ years – CES Isolated Network NAS
    Recommendation: Surplus
    8. elections.kennesaw.edu - Age 5 years - Dell PowerEdge R610

EXHIBIT "A"

Recommendation: Format and reinstall on CES Isolated Network as NAS

9. unicoi.kennesaw.edu – Age 6+ years. Dell PowerEdge 1950
Recommendation: Surplus

10. Web server backup
Recommendation: Surplus

Action Item Owner: UITS-ISO, UITS-ISS, CES Staff

8. **Issue:** An operating system and application security assessment has not been conducted on the CES Isolated Network

Action Items: UITS-ISO should perform a stand-alone security assessment of the CES Isolated Network using a laptop-based scanning engine. Servers and workstations should be hardened based on the scan results and regular testing of the network scheduled.
Action Item Owner: UITS-ISO, UITS-ISS, CES Staff

9. **Issue:** A wireless access point was found when UITS did a walkthrough of the CES House

Action Items: Understanding the risk that a wireless access point presents to the CES isolated network, UITS-ISO should prioritize CES for wireless network upgrade and put guidelines in place which prohibit the use of non-KSU wireless devices in the house.
Action Item Owner: UITS-ISO, UITS-ISS

10. **Issue:** Inconsistent port colors in House 57. Data outlets throughout the building have different color bezels to indicate which network is public and which is private:

Red = analog voice/phone
Green = KSU data public network
Blue = Elections private network
White = Elections 2nd private network

Since the original cabling installation the two private networks established for elections now act as a single private network. In room 105a, the blue cables terminate to one patch panel and the white cables terminate to another patch panel. They have connected jumpers from both of these patch panels to the same switch thus eliminating any separation by the colors Blue or White.

Action Items: Jacks for the public and private network should be reinstalled to conform to campus color standards. Additionally, jacks from the public and private networks should be on different panels. The total cost of this change will be approximately $3,000.
Action Item Owner: UITS-ISO, UITS-ISS

EXHIBIT B

From: Stephen Craig Gay
To: Ware, William D. II (AT) (FBI)
Subject: Fwd: Request for data retrieval
Date: Wednesday, March 15, 2017 1:51:26 PM

Agent Ware,

We received the request below from the Center for Election Systems regarding data contained on the seized server which they do not have a backup of. What is the possibility of having the data extracted and us picking it up?

Thank you for your consideration of this request.
Stephen

----- Forwarded Message -----
From: "Michael Barnes" <mbarne28@kennesaw.edu>
To: "Stephen C Gay" <sgay@kennesaw.edu>
Cc: "Steven Dean" <sdean29@kennesaw.edu>, "Merle King" <mking@kennesaw.edu>
Sent: Wednesday, March 15, 2017 1:41:25 PM
Subject: Request for data retrieval

Stephen,

As discussed earlier today, we would like to retrieve certain records from elections.kennesaw.edu that support our daily office activities, items such as inventory records, workflow databases used during our ballot building efforts, and operation manuals. These data are located in the cesuser user directory at /home/cesuser. We would like to retrieve the entire ccsuser directory, if possible.

Thanks,

Michael Barnes
Director
Center for Election Systems
Kennesaw State University
3205 Campus Loop Road
Kennesaw, GA 30144
ph: 470-KSU-6900
fax: 470-KSU-9012

EXHIBIT "B"

EXHIBIT C

Cary Ichter

From: Josh Belinfante <Josh.Belinfante@robbinsfirm.com>
Sent: Monday, July 8, 2019 3:02 PM
To: Green, Kristine Z. (AT) (FBI)
Cc: Vincent Russo; Bryan P. Tyson (btyson@taylorenglish.com); Germany, Ryan
Subject: RE: Georgia Voting Device Litigation

Thanks again.

JB

ROBBINS
Josh Belinfante
ROBBINS ROSS ALLOY BELINFANTE LITTLEFIELD LLC
500 Fourteenth Street NW
Atlanta, GA 30318
404.856.3262 (Direct)
678.701.9381(Main)
404.856.3250 (Fax)
www.robbinsfirm.com

Please visit our affiliated government relations practice: Robbins Government Relations
www.robbinsgr.com

From: Green, Kristine Z. (AT) (FBI) <kzgreen@fbi.gov>
Sent: Monday, July 8, 2019 3:01 PM
To: Josh Belinfante <Josh.Belinfante@robbinsfirm.com>
Cc: Vincent Russo <vrusso@robbinsfirm.com>; Bryan P. Tyson (btyson@taylorenglish.com) <btyson@taylorenglish.com>; Germany, Ryan <rgermany@sos.ga.gov>
Subject: RE: Georgia Voting Device Litigation

I will draft the request to our forensic folks today.

From: Josh Belinfante [mailto:Josh.Belinfante@robbinsfirm.com]
Sent: Monday, July 08, 2019 2:20 PM
To: Green, Kristine Z. (AT) (FBI) <kzgreen@fbi.gov>
Cc: Vincent Russo <vrusso@robbinsfirm.com>; Bryan P. Tyson (btyson@taylorenglish.com) <btyson@taylorenglish.com>; Germany, Ryan <rgermany@sos.ga.gov>
Subject: RE: Georgia Voting Device Litigation

EXHIBIT "C"

Agent Green:

Thank you again. Please find the attached documents responsive to your request. If you need anything else from us to begin copying the drive, please let us know.

Best regards,
JB

ROBBINS
Josh Belinfante
ROBBINS ROSS ALLOY BELINFANTE LITTLEFIELD LLC
500 Fourteenth Street NW
Atlanta, GA 30318
404.856.3262 (Direct)
678.701.9381(Main)
404.856.3250 (Fax)
www.robbinsfirm.com

Please visit our affiliated government relations practice: Robbins Government Relations
www.robbinsgr.com

From: Green, Kristine Z. (AT) (FBI) <kzgreen@fbi.gov>
Sent: Monday, July 8, 2019 10:57 AM
To: Josh Belinfante <Josh.Belinfante@robbinsfirm.com>
Cc: Vincent Russo <vrusso@robbinsfirm.com>; Bryan P. Tyson (btyson@taylorenglish.com) <btyson@taylorenglish.com>; Germany, Ryan <rgermany@sos.ga.gov>
Subject: RE: Georgia Voting Device Litigation

I spoke with one of our investigators and he confirmed that he has the blank hard drive the State provided. Shortly after we received the drive, the State's counsel requested we temporarily discontinue the request to copy the drive. We can re-initiate the request now, if necessary. I would like a letter of representation and notarized signature from the Secretary of State's office before I actually turn over the drive.
Thanks,
Kristy Green
770-216-3154

From: Josh Belinfante [mailto:Josh.Belinfante@robbinsfirm.com]
Sent: Wednesday, July 03, 2019 1:21 PM
To: Green, Kristine Z. (AT) (FBI) <kzgreen@fbi.gov>
Cc: Vincent Russo <vrusso@robbinsfirm.com>; Bryan P. Tyson (btyson@taylorenglish.com) <btyson@taylorenglish.com>; Germany, Ryan <rgermany@sos.ga.gov>
Subject: Georgia Voting Device Litigation

Ms. Green:

Good afternoon. My name is Josh Belinfante, and this follows up on an email I left earlier today. Along with Vincent Russo and Bryan Tyson, we represent the State of Georgia, the Secretary of State and other state defendants in the litigation styled *Curling, et al. v. Raffensperger*, et al., Civil Action No. 1:17-CV-2989 AT. We have succeeded John Salter and Governor Barnes as counsel for the State.

The Plaintiffs in the action recently asked about the status of an image of a server or computer that the FBI took possession of after an alleged hack of a Kennesaw State University system by persons challenging Georgia's voter system. It is our understanding that the FBI retains custody of the device, and that the State has previously provided the FBI with a different hard drive on which to copy the contents of the device that the FBI took custody of as part of its investigation.

Can you confirm that the FBI maintains the computer it took possession of as part of the investigation?

Can you let us know if the hard drive has been copied?

Thanks in advance for your assistance with this matter, and have a great Independence Day.

Best regards,
JB

Please note the new address.

ROBBINS
Josh Belinfante
ROBBINS ♦ ROSS ♦ ALLOY ♦ BELINFANTE ♦ LITTLEFIELD LLC
500 Fourteenth Street NW
Atlanta, GA 30318
404.856.3262 (Direct)
678.701.9381(Main)
404.856.3250 (Fax)
www.robbinsfirm.com

Please visit our affiliated government relations practice: Robbins Government Relations
www.robbinsgr.com

EXHIBIT "C"

EXHIBIT D

Cary Ichter

From: Josh Belinfante <Josh.Belinfante@robbinsfirm.com>
Sent: Wednesday, July 17, 2019 3:07 PM
To: Green, Kristine Z. (AT) (FBI)
Subject: Re: Georgia Voting Device Litigation

We have a hearing next week (Thursday and Friday). Plaintiffs are the ones that have requested the drive.

Thanks again,
JB

Sent from my iPhone

On Jul 17, 2019, at 3:04 PM, Green, Kristine Z. (AT) (FBI) <kzgreen@fbi.gov> wrote:

> I have put in a request to our forensics folks for a copy. I am out of town so I can't access the system to check the status of the request at the moment. I will be back next week. What is your timeline?
>
> -
>
> On Jul 17, 2019 1:49 PM, Josh Belinfante <Josh.Belinfante@robbinsfirm.com> wrote:
> Agent Green:
>
> Do you have a status update on this? The plaintiffs' counsel is asking.
>
> Thanks,
> JB
>
> Sent from my iPhone
>
> On Jul 8, 2019, at 3:01 PM, Green, Kristine Z. (AT) (FBI) <kzgreen@fbi.gov> wrote:
>
> > I will draft the request to our forensic folks today.
> >
> > ---
> > **From:** Josh Belinfante [mailto:Josh.Belinfante@robbinsfirm.com]
> > **Sent:** Monday, July 08, 2019 2:20 PM
> > **To:** Green, Kristine Z. (AT) (FBI) <kzgreen@fbi.gov>
> > **Cc:** Vincent Russo <vrusso@robbinsfirm.com>; Bryan P. Tyson (btyson@taylorenglish.com) <btyson@taylorenglish.com>; Germany, Ryan <rgermany@sos.ga.gov>
> > **Subject:** RE: Georgia Voting Device Litigation
> >
> > Agent Green:
> >
> > Thank you again. Please find the attached documents responsive to your request. If you need anything else from us to begin copying the drive, please let us know.
> >
> > Best regards,

EXHIBIT "D"

JB

Josh Belinfante
ROBBINS ROSS ALLOY BELINFANTE LITTLEFIELD LLC
500 Fourteenth Street NW
Atlanta, GA 30318
404.856.3262 (Direct)
678.701.9381(Main)
404.856.3250 (Fax)
www.robbinsfirm.com

Please visit our affiliated government relations practice: Robbins Government Relations
www.robbinsgr.com

From: Green, Kristine Z. (AT) (FBI) <kzgreen@fbi.gov>
Sent: Monday, July 8, 2019 10:57 AM
To: Josh Belinfante <Josh.Belinfante@robbinsfirm.com>
Cc: Vincent Russo <vrusso@robbinsfirm.com>; Bryan P. Tyson (btyson@taylorenglish.com) <btyson@taylorenglish.com>; Germany, Ryan <rgermany@sos.ga.gov>
Subject: RE: Georgia Voting Device Litigation

I spoke with one of our investigators and he confirmed that he has the blank hard drive the State provided. Shortly after we received the drive, the State's counsel requested we temporarily discontinue the request to copy the drive. We can re-initiate the request now, if necessary. I would like a letter of representation and notarized signature from the Secretary of State's office before I actually turn over the drive.
Thanks,
Kristy Green
770-216-3154

From: Josh Belinfante [mailto:Josh.Belinfante@robbinsfirm.com]
Sent: Wednesday, July 03, 2019 1:21 PM
To: Green, Kristine Z. (AT) (FBI) <kzgreen@fbi.gov>
Cc: Vincent Russo <vrusso@robbinsfirm.com>; Bryan P. Tyson (btyson@taylorenglish.com) <btyson@taylorenglish.com>; Germany, Ryan <rgermany@sos.ga.gov>
Subject: Georgia Voting Device Litigation

Ms. Green:

Good afternoon. My name is Josh Belinfante, and this follows up on an email I left earlier today. Along with Vincent Russo and Bryan Tyson, we represent the State of

Georgia, the Secretary of State and other state defendants in the litigation styled *Curling, et al. v. Raffensperger*, et al., Civil Action No. 1:17-CV-2989 AT. We have succeeded John Salter and Governor Barnes as counsel for the State.

The Plaintiffs in the action recently asked about the status of an image of a server or computer that the FBI took possession of after an alleged hack of a Kennesaw State University system by persons challenging Georgia's voter system. It is our understanding that the FBI retains custody of the device, and that the State has previously provided the FBI with a different hard drive on which to copy the contents of the device that the FBI took custody of as part of its investigation.

Can you confirm that the FBI maintains the computer it took possession of as part of the investigation?

Can you let us know if the hard drive has been copied?

Thanks in advance for your assistance with this matter, and have a great Independence Day.

Best regards,
JB

Please note the new address.

Josh Belinfante
ROBBINS ◆ ROSS ◆ ALLOY ◆ BELINFANTE ◆ LITTLEFIELD LLC
500 Fourteenth Street NW
Atlanta, GA 30318
404.856.3262 (Direct)
678.701.9381(Main)
404.856.3250 (Fax)
www.robbinsfirm.com

Please visit our affiliated government relations practice: Robbins Government Relations
www.robbinsgr.com

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

DONNA CURLING, ET AL., **Plaintiffs,** **v.** **BRIAN KEMP, ET AL.,** **Defendants.**	**Civil Action No. 1:17-CV-2989-AT**

CERTIFICATE OF SERVICE

I hereby certify that on August 1, 2019, a true and correct copy of the foregoing **COALITION PLAINTIFFS' REPLY BRIEF ON EVIDENTIARY PRESUMPTION ARISING FROM SPOLIATION OF EVIDENCE** was served on all counsel via the Court's ECF filing system.

/s/ Cary Ichter
Cary Ichter