Georgia Elections Data Destruction Audit

VOTERGA

This document provides never before published information about the destruction of Georgia elections data at the Kennesaw State University Center for Election Systems in the summer of 2017. It also audits the October 30th Secretary of State report that concludes the data destruction was standard procedure

Table of Contents

April 30, 2018
Garland Favorito
VoterGA Co-founder
garlandf@voterga.net
garlandf@msn.com
404 664-4044

1. Purpose

In 2017, Georgia's mission critical election data was found to be open and exposed on a public web server used to prepare every county and their voting machines for every election. When a law suit was filed, the Center for Election Systems (CES) at Kennesaw State University's (KSU) destroyed the elections data without assessing the impact of the exposure. The CES reports to Secretary of State (SOS) Brian Kemp. When informed about the data destruction, Secretary Kemp responded angrily on a Facebook post and Twitter feed, however, days later he completely reversed his position, and his office issued an investigative report that concluded the data destruction was *"standard procedure".*

Since that time the people of the State of Georgia have been denied any explanation of why CES would place its mission critical data on a public web server, why Secretary Kemp would completely reverse his position in a matter of days and why the report would reach the conclusions that it did. This document will answer those questions and define the magnitude of the breach that may have occurred. It provides an independent, high level audit of the procedures and suppositions in the SOS report that concluded destruction of elections data without a breach assessment was *"standard procedure".*

2. About the Author

Garland Favorito is a co-founder of *Voters Organized for Trusted Election Results in Georgia* (VoterGA) and Elections Director of the Constitution Party of Georgia. VoterGA is a nonpartisan, non-profit, all-volunteer organization dedicated to restoring the integrity of Georgia elections. Its primary objective is to advocate for verifiable, auditable and recount-capable voting in Georgia. It also advocates for fair and equal ballot access for all Georgia citizens.

Mr. Favorito is a career Information Technology (IT) professional with over 40 years of in-depth experience in internet systems design, business systems analysis, database administration, application development, systems integration, systems life cycle methodologies, computer programming, project management, and multi-factor security for financial transactions. His experience centers on medium- and large-scale mission-critical applications in nearly all facets of American business. His industry experience includes banking, financial systems, health care, accounting, manufacturing, inventory, purchasing, retailing, utilities, telecommunications, insurance, software development and the service industry.

Mr. Favorito also has 15 years of volunteer involvement in regards to Georgia's voting machines, dating back to 2002 before the state purchased and implemented the machines. His election integrity activities include research, analysis, documentation, and presentations involving Georgia's current voting systems. He is recognized throughout most of the state as a leading expert on the usage of, and risks involved with, Georgia's voting machines.

3. Election Procedures

The Center for Election Systems (CES) at Kennesaw State University (KSU) prepares the Georgia voting system for each election that has been conducted to date. CES creates ballots, poll book files and Global Election Management Systems (GEMS) election databases for each county. It also provides technical support for each election. CES distributes the files to each county prior to an election. Each county loads the database it receives onto its GEMS server and programs each voting machine memory card. The memory cards are then loaded into each voting machine to record the results for voters. Each county typically downloads voter data contained on the poll book file and exports the data onto flash cards that are loaded into each precinct poll book. The poll book file is used to verify voters on Election Day and create a voter access card that voters load into voting machines to tell the machine that they are authorized to cast one vote. The voting machine then displays the ballots to voters and accepts their selections from the touch screen.

(See Appendix A)

Poll workers also use the poll books to create voter access cards for early in-person voters. However, CES does not load the poll book files with voter data for in-person early voting. Early in-person voters are verified using a central database before the poll worker uses the poll book to create a voter access card for the voter. The central database also records that the voter is voting at the early voting location to prevent subsequent double voting at a different location.

When the poll close precinct workers print copies of the voting machine tapes that include the vote-count totals for each contest. They post one copy of each machine tape on the door of the precinct building where the election took place so that it can be viewed by the public. The precinct workers remove the memory cards with the votes cast on each machine and place them in a sealed envelope with a copy of the machine tapes. The precinct manager and assistant then hand deliver the sealed envelopes to the county elections office for processing.

Fulton County operates three upload points. They are at the North Annex, South Annex and the Roswell City Hall. The precinct manager and assistant take the envelopes to one of the upload points. Each precinct card is checked in according to its assigned number and then uploaded to the county elections database for accumulation.

County election officials accumulate the results, print out statements of votes cast and export the results for publishing. The results then appear on the county web sites for public consumption. In 2012, Secretary Kemp executed a contract to publish its state election results through Clarity Elections results publishing software (ENR), which is produced by Tampa-based SOE Software. SOE was a subsidiary that had just been acquired by the privately owned Spanish company SCYTL in January of that year. Many of the counties now use the Clarity software to report their votes.

4. Election Preparation Security

The Georgia election procedures described above represent a centralized approach to election preparation as opposed to a decentralized approach where counties prepare their own election databases and may maintain their own county voter registration lists. While there are operational advantages to a centralized approach, it is subject to a **single point of attack.** Thus, any proposal to move the central election preparation location from KSU to the SOS office **cannot solve all the vulnerability problems** this audit identifies.

(See Appendix A)

The CES has prepared election data for every county since our electronic voting systems were implemented in 2002. Every county prepares every voting machine for every location using data received from CES. Therefore, **an attacker who gains access to the central election preparation system can compromise it with malware that could swap votes from one candidate to another in any race of any Georgia election.**

Counties have no security procedures to verify that the election databases and voting registration information that they receive from central preparation is free of malware. Therefore, **a central point attacker can launch a statewide vote swapping attack without access to any voting machine**. Any such malware can easily be programmed to take effect only when voting machines are operated in Election Mode.

CES Director Merle King, Professor Britain Williams, who oversaw installation of the Georgia voting systems, and Princeton Dr. Ed Felton, who hacked the same type of system in front of the U.S. Congress, all acknowledged under oath in depositions or court testimony that the voting systems can be programmed to count differently in Election Mode than in Test mode.

Since the counties test voting machines in Test Mode and then switch them to Election mode for an election, **Logic and Accuracy testing that counties perform cannot detect vote switching malware that the counties may receive from any central preparation facility.**

5. Vulnerability Discovery

On August 24, 2016, a Bastille Threat Research Team member named Logan Lamb discovered a major vulnerability at CES. Lamb was formerly a cybersecurity researcher at the Oak Ridge National Laboratory in Tennessee. He decided to view the CES public web site, *Elections.Kennesaw.edu,* in preparation for a research project. His affidavit tells a remarkable story.

Lamb stumbled upon folders of voting system files that could be accessed to hack an election. He ran a script that surprisingly downloaded 15 Gigs of data. Lamb noticed CES was using an out of date version of a Drupal content management system. That version has a major **security flaw** called "Drupalgeddon" which allows intruders to take control of a site.

On August 28, after realizing and verifying the magnitude of his discovery, Lamb emailed CES Executive Director Merle King. On August 29th they had a brief conversation about it. Lamb stated that King thanked him, assured him that the issues would be remediated and asked him to remain quiet. However, Director **King did not ensure all vulnerabilities were corrected and never notified the Secretary of State's Office (SOS)**.

In late February, Lamb told a colleague Christopher Grayson about what he discovered. Grayson determined that the vulnerability had not been properly remediated, and the **Drupal flaw still existed** on the unencrypted portion of the site. Lamb tweaked his script and found that he could still access the same files he originally did and newer files as well. This time Grayson contacted security instructor Andy Green at KSU. Green confirmed that he could traverse the critical election directories without authenticating since they had no password protection. He contacted KSU's Chief Information Security Officer Stephen Gay who is also the Director of University Information Technology Services (UITS). UITS prepared an Incident After Action report that was completed on April 18th. That report described actions to take to prevent a reoccurrence of the incident.

However, on April 27th the SOS office claimed they did not have such a report in response to VoterGA's Open Records Request (ORR). That request asked for documents the SOS received from KSU in regards to a voting database breach on or about March 1st. VoterGA obtained the UITS assessment on May 3rd with an ORR to KSU. But in the June 7th paper ballot lawsuit hearing, the SOS legal counsel refused to acknowledge authenticity of the KSU security assessment!

6. Magnitude of Vulnerability

In the two previously described accesses of the *Elections.Kennesaw.edu* server**,** Lamb's scripts found unprotected on this CES public web site **essentially everything needed to hack an election without detection and without physical access to any voting machine**. That included:

- A current copy of Voter Registration database containing names, addresses and social security numbers for 6.7 million voters;
- Current Elections database(s) that are sent to counties to accumulate the results of an election;
- Windows executables that any recipient can use to create elections databases;
- PDFs of memos containing recent Election Day supervisor passwords;
- Training videos on how to download files, put them on memory cards and insert them into county voting machines.

In addition, Lamb explained that the Drupal content management system security flaw allows an attacker to take control of the web site and its server. **The attacker then has free reign with the system to execute, create, modify and delete anything** on the *elections.kennesaw.edu* server. These critical vulnerabilities may have provided the ability for an attacker to penetrate into the internal CES network where other data servers resided.

The vulnerabilities were found to exist between August, 2016 and March, 2017 which includes the November, 2016 election. However, they have existed **at least** since the web server was installed in 2013 and possibly much longer. To date, CES have been unable to determine when Drupal was first installed.

In response to Logan Lamb's attempt to help the CES, the Georgia General Assembly created and passed Senate Bill SB315, a whistle blower **prosecution** law. The bill **criminalizes** intentional unauthorized access to a public web site. After the legislation passed in late March 2018, 13 Georgia Tech professors wrote a letter to Governor Deal citing the reasons he should veto the measure.

7. UITS Incident Response

On August 29th, 2016, the day that Logan Lamb had a conversation with Merle King to explain the server vulnerabilities, CES director Michael Barnes emailed Chief Information Security Officer Stephen Gay to request he black list the IP addresses of Lamb and Bastille. The intent was to block them from any public access to their server but Barnes later retracted his request when he realized it was *"inappropriate".*

After being warned of the vulnerabilities, UITS notified KSU's Chief Information Officer and established firewall rules to block external access to the elections server. On March 2, they copied logs, seized the server and notified the University System of Georgia. On March 3, Mr. Gay gave the server Federal Bureau of Investigation (FBI) which investigated Lamb to make sure no crime was committed. After interviewing Lamb, they concluded that the incident did not escalate to the point of breach. However, **the FBI has no means to rule out domestic hackers making other breaches of the elections server in prior months or years, nor would they be familiar enough with CES elections data to make such a forensic assessment.**

On March 15th 2017, Barnes sent an email to Gay requesting that he retrieve Elections server data files for ballot building, workflow databases and operation manuals because **CES had just realized after two weeks that they had no backup of the elections server.** On the same day, Gay asked the FBI to return the server. The FBI returned it to Gay on March 17 and the files that had been exposed to cybersecurity risks were returned to CES. It is inconceivable that CES had no standard back up procedures for the mission critical elections data on this server or their internal server.

On March 31st KSU's Tammy DeMel issued a media statement with **three false or deceptive phrases**:

- *"Kennesaw officials report there is no indication of any illegal activity…"*

While there was no illegal activity when Logan Lamb accessed the server, **Kennesaw officials never performed a forensic risk assessment that would have determined whether or not any prior illegal activity occurred** as a result of the vulnerabilities that Logan Lamb identified.

- *"University officials were first notified of the situation on Tuesday, March 1…"*

UITS Chief Information Security Officer Stephen Gay was notified about Logan Lamb's first access on August 29th, 2016 when CES director Michael Barnes emailed him to request that Logan Lamb and Bastille be black listed.

- *"…and upon verification immediately contacted the Office of the Secretary of State…"*

No evidence has been found that anyone from CES or UITS notified anyone in the office of the Secretary of State about either of Logan Lamb's site accesses from August 28th, 2016 through the time of the March 31st media statement**.** However, the audit did discover that certain KSU staff members were under verbal order not to Email the SOS office without calling them first and discussing the Email to be sent. As evidence of this order, no Emails were found to exist to or from anyone at CES or UITS and the State Elections Director Chris Harvey. Thus, the Georgia State Elections Director appears to have no interest in the vulnerabilities, their impact or any remediation plan for them.

8. Elections Data Destruction

On April 18th, UITS published an Incident After Action Report for review. This report contained a 10 point action plan to improve security with software upgrades, infrastructure changes, physical security improvements, procedural adjustments and organizational restructuring. These action items generally represent standard best practices designed to prevent future security risks and data exposures.

However, the report contained only forward looking preventive measures. **There were no forensic action items to assess the impact of breaches that may have occurred as a result of vulnerabilities that had existed.** UITS would not have the ability to perform such forensics since CES represents the owners of election data and UITS does not command that type of application knowledge.

The Incident After Action Report listed action items to format and re-install the *elections.kennesaw.edu* server on the CES isolated network. Thus, the report provided authorization to destroy elections data without performing a forensic risk assessment on the data to determine if breaches had occurred in the past and what their impact might be. The report also targeted the *Unicoi.Kennesaw.edu* sever, a CES NAS server and a CES Epic server as surplus without instructions explaining how to handle their data. These CES internal network servers were never in FBI custody.

On April 24th, Stephen Gay routed the report to CES Directors Merle King and Michael Barnes requesting their review and copied KSU Chief Information Officer Lectra Lawhorne. There is no record that either CES director responded to the request to review the action plan despite being the owners of the data that the plan affected. **Thus, neither CES Director raised an issue with the destruction of their elections data despite the fact that they had known for over a month that they had no backup**. The CES Directors also allowed their elections data to be destroyed without performing a forensic risk assessment or any form of breach impact analysis on that data. There is no evidence that the CES Directors even considered such an assessment.

On July 3rd, 2017, a current lawsuit entitled Curling v. Kemp was filed. The complaint was readily available on July 5th, the next business day after the holiday. **On July 7th, UITS and CES destroyed all data on the *elections.kennesaw.edu* server.** On August 8th, the lawsuit was removed to federal court at the request of the office of the State Attorney General who then represented Defendant Kemp. The next day, August 9th, **UITS and CES destroyed all data on two internal servers using a process called degaussing that magnetically destroys the data.**

These actions were taken with implicit approval from the CES elections data owners. When it was completed, UITS Director Stephen Gay replied: *"That is fantastic news. Great work to all parties in closing the final recommendation from the Incident After Action Report"*

9. Secretary of State Reaction

When Secretary Kemp was informed that the elections data destruction had taken place, he stated in his October 26 Facebook post and Twitter feed that his office *"…had no involvement in this decision"*, and went on to say: ***"Not only did KSU officials fail to notify us when they first learned of the server's vulnerabilities, they failed to notify us again when they wiped the compromised server and the backup server."***

In the same October 26 Facebook and Twitter posts he continued to insist that *"…Georgia's elections are safe and our systems remain secure."* However, to date, he has yet to explain how he can know that given the vulnerabilities discovered and lack of breach assessment.

Also in the same Facebook and Twitter posts on Thursday, Secretary Kemp announced: ***"Earlier today we opened an internal investigation on this new incident at KSU. Those responsible at KSU should be held accountable for their actions."***

Throughout his posts, Secretary Kemp expressed anger at those actions by UITS and CES. He called the actions ***"reckless behavior", "inexcusable conduct", "gross incompetence"*** **and** ***"undeniable ineptitude".*** Almost immediately, the Attorney General **resigned** from defending the Secretary in Curling v. Kemp while citing a conflict among the Defendants. By Monday, October 30, Secretary Kemp's legal counsel, Ryan Germany, produced a report stating that **the elections server data destruction was *"standard procedure".***

10. Secretary of State Investigation

The two page SOS investigative report was completed in less than three business days. It contains a brief summary and conclusion based on a two paragraph timeline and two paragraphs of analysis.

The report indicates that **no one at CES ever gave the SOS office a copy of the elections data returned from the FBI even though that data is property of the SOS office and subject to its retention policies** according to the KSU CES contract with the SOS office.

The report also indicates that the **SOS office was still unable to obtain a copy of that elections data from the FBI data six months after they had returned the *elections.kennesaw.edu* server to KSU**.

The report did not consider the destruction of data on the internal server *uncoi.kennesaw.edu* and falsely assumed that the FBI had that data as well.

The report concluded:

(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. "*

11. SOS Investigation Procedural Defects

The SOS investigation into the critical elections data destruction was initiated and carried out in a manner **conflicting with the SOS's own standards and procedures in conducting election related investigations** for many reasons:

Investigator Background:

The background of the report author is inconsistent with that of a typical SOS elections investigator:

- Ryan Germany is the Chief Legal Counsel to Secretary Kemp and not an Elections Investigator;
- Ryan Germany's experience at the Secretary of State's office primarily involves securities investigations and not elections investigations;
- Ryan Germany has never been sworn to an oath of office as a Chief Elections Investigator would typically be despite Georgia case law indicating that he is required to do so as a public officer (O.C.G.A. 16-10-1).

Reporting Procedures Ignored:

As an investigator, Germany ignored standard SOS election investigation procedures and reporting:

- He failed to identify who the complainant for the investigation is although indications are that it was Secretary Kemp;
- He failed to identify the respondent groups or individuals at KSU who were being investigated as part of the data destruction;
- He failed to identify who ordered the destruction of elections data and who approved it;
- He failed to identify the elections that were impacted by the data destruction;
- He failed to include the *"After Action Report"* he referenced as an exhibit;
- He failed to disclose any individuals who he contacted to investigate the data destruction as would be the normal procedure in any elections investigation;
- **He initiated no communications with anyone at CES or UITS to investigate the matter during the investigation time period** according to a VoterGA Open Records Request**.**

Investigation Substance:

Germany conducted the investigation in less than three business days and produced only a two page report despite the critical nature of the data destruction. In addition:

- He failed to investigate why CES, as data owners, did not object to the data destruction;
- He failed to investigate why CES had no backup of either server containing mission critical elections data;
- He failed to investigate why CES did not know they had no backup two weeks after the incident;
- He failed to investigate why no forensic assessment of the server was conducted to assess the impact of the data;
- He failed to investigate why UITS and CES violated standard SOS data retention policies even after being warned by Chief Legal Affairs Counsel Jeff Milsteen;
- He failed to acquire a copy of destroyed data but claimed it was available at the FBI;

12. SOS Investigation Conclusion Defects

As a result of the procedural anomalies listed above, the few conclusions reached in the report have serious fallacies:

First, the conclusion *"The concern that the data was lost is unfounded"* because "*…the FBI retained an image of the data on those servers…*" has proven to be **false.** The FBI possessed only one server and never took possession of any of the three other CES servers that held CES data. That data was destroyed by August 9th without CES instructions for data disposition. Germany was unable to obtain an image copy of the *elections.kennesaw.edu* public server from the FBI by his own admission and he never established the disposition of the data on the other three servers.

Secondly, the conclusion that *"the narrative asserted in the media that the data … is no longer available is completely false and without merit"* also has proven to be **false.** If such a narrative was asserted, it would certainly have merit since the elections data was not available and the availability of the other CES data was never established. Thus the lack of transparency should be a concern not just to the media but to every Georgia voter.

Thirdly, the conclusion that *"KSU IT acted in accordance with standard IT procedures…"* is also false at least in regards to CES IT personnel operating at KSU. When critical application data may have been breached**, standard IT procedure would be to conduct a forensic risk assessment** to determine the impact and remediate any potential issues. **Furthermore, no standard IT procedure would recommend destroying data without a backup.**

A standard, high level, sample IT risk assessment procedure for a potential breach might be as follows:

- Identify the duration of the vulnerability exposure;
- Determine if an unauthorized breach occurred during the exposure window by using audit logs;
- Identify the source of the unauthorized breach using IP addresses of the potential attackers;
- Define when the unauthorized breaches may have occurred using log timestamps;
- Assess the impact of any unauthorized breach on the application and its data owners;
- Implement a remediation strategy to compensate for the unauthorized breach

Fourth, data related activities *"in accordance with standard IT procedures"* require KSU to abide by **data retention policies** of their contract with the SOS office. Article V requires KSU to maintain all records and return them to physical custody of the SOS office. KSU has no contractual authority to delete data without contacting **SOS personnel who are the election data owners** for approval.

Finally, no conclusions of any kind should be reached without investigating and reporting as to why CES placed mission critical elections data on a public web server, why no backup of either of the two CES servers existed and why no forensic assessment of the exposed elections server was conducted to assess the impact of the potential breach.

13. Conclusion

The CES vulnerabilities identified by Logan Lamb, and the subsequent destruction of elections data without a forensic risk assessment, represent **the greatest potential election fraud in Georgia history**. CES data preps every county and every county uses CES data to prep every voting machine for every election. **Virtually any vote in any election could have been changed for a period of years without detection and without physical access to any voting machine.**

In spite of the seriousness of the danger, the SOS office chose to produce a rather frivolous 2 page report to investigate the issues outlined in this general audit. The audit defines well over a dozen procedural deviations and investigative oversights in the brief two page report. These deviations and oversights are so significant that they render the SOS report as **not credible**.

Furthermore, this audit has shown that all conclusions reached in the SOS report are essentially false based on actual evidence and standard IT forensic procedures. While it could be argued that UITS followed standard IT procedures in producing the Incident After Action Report, the same Is not true for CES IT personnel. CES Directors must be considered culpable in several ways:

- They left mission critical elections data on a publicly exposed web server in conflict with basic internet design security procedures;
- They failed repeatedly to secure the election data once it was placed on that server;
- They failed to maintain a proper back up of their critical elections data;
- They failed to realize they had no backup of their elections data for two weeks after an incident;
- They allowed mission critical elections data to be destroyed without a backup;
- They allowed critical elections data to be destroyed in conflict with SOS data retention policies;
- They failed to perform a forensic risk assessment defining the impact of vulnerabilities revealed;
- They allowed critical elections data to be destroyed despite having no forensic risk assessment.

The SOS report never seriously considered any of these failures and thus must be considered fraudulent.

Some CES and SOS staff members are likely to have committed violations of law in regards to the destruction of elections data. For example, public officers who deface public records or are in any way connected with defacing the property may have committed a crime [O.C.G.A. 45-11-1 (a), (b)] Secretary Kemp has stated that individuals inappropriately involved in these events “should be held accountable for their actions”. Instead, the SOS office appears to have brought the flawed centralized process described and some key culpable CES personnel in house. Neither will solve the problems identified in this audit.

The SOS report content and corresponding investigation are serving the purpose of protecting CES personnel who report to the SOS office and SOS personnel who should have been providing proper oversight. Thus, the deficiencies in the report illustrate that the SOS office initiated and continues to participate in a **cover-up** of the elections data destruction and the magnitude of vulnerabilities that existed.

14. Appendix

A. CES Central Election Prepping Illustration