CURLING, et al. v. KEMP, et al.
Civil Action File No: 1:17-CV-02989

EXHIBIT 1
DECLARATION OF MERRITT BEAVER

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 FILE

NO. 1:17-CV-02989-AT

DECLARATION OF MERRITT BEAVER

Pursuant to 28 U.S.C. § 1746, MERRITT BEAVER, Chief Information Officer in the office of the Secretary of State for the State of Georgia, declares as follows:

1. I make this Declaration in support of a response by Secretary Kemp, the State Election Board, and the members of the State Election Board to motions for preliminary injunction filed in the above-styled matter *of Donna Curling, et al., v. Brian Kemp, et al,* (Civil Action No. 1:17-cv-2989-AT).

2. I am the Chief Information Officer for the Office of the Georgia Secretary of State and have held that position since January 2014. I have over twenty-five years of experience in software and information technology with special attention to information privacy. I have had numerous IT roles in the healthcare industry

focused on protecting patient information, including with McKesson, GE Medical, and HealthPort. I have a Six Sigma Black Belt certification in process improvement that I earned while I was at General Electric. I have a BS in Electrical Engineering from Virginia Tech and an MBA from Keller Business School.

3. I write this affidavit to discuss some the actions that the Secretary of State's office has taken regarding election security. Election security is the top priority of the office and has been for a long time. While plaintiffs only talk about the mechanism by which voters cast ballots, election security is much broader than that. Our elections system includes a voter registration database, an air-gapped system for building ballots, and numerous other components, including on online voter registration tool, an online voter information page, and election night reporting page, and Direct Recording Electronic (DRE) voting machines used for casting ballots.

4. The security of our voting system depends on much more than the voting mechanism. Even before the federal government declared election infrastructure as national critical infrastructure, we treated it as critical infrastructure.

5. We protect our systems through multiple, redundant layers of security with contingency plans in place. We utilize top-private sector vendors as well government partners to monitor our networks 24/7 for any unusual traffic, to

continuously scan our networks, to provide multiple firewalls, and to encrypt data. Two-factor authentication is required for all users (both state and county) to access the voter registration application, and it is equipped with frequent password change requirements, brute force and inactivity account disabling, and DDOS and SQL injection defenses. We also have a complete off-site backup disaster recovery system and offline backups stored in case we have to revert to a previous version of the database. We take every reasonable precaution to protect our systems from a cyber-incident, including conducting regular cyber assessments with penetration testing, agency-wide cybersecurity training and phishing campaign assessments. We also have contingency plans in place in the event of an incident.

6. After the incident at KSU, we moved those operations in-house to the Secretary of State's office. At that time, we reviewed every process that KSU did for security vulnerabilities and other improvements. The way that KSU stored and transmitted data is not the way that those tasks are undertaken now. We continually add security procedures to improve processes. We also monitor our vendors' cybersecurity, including performing cybersecurity assessments and penetration testing on vendors. If a vendor is not performing sufficiently to our security standards, we cease doing business with that vendor.

7. Moving to paper ballots for the voting mechanism would not add one iota of protection to the state's voter registration database, air-gapped ballot building network, or other online tools such as election night reporting.

8. Moving to paper ballots in such an abbreviated time frame could potentially damage Georgia's election security. We have many years of experience of protecting the current system, but we do not have personnel that have dealt with the security surrounding a paper ballot environment. While it is certainly possible to build a system to adequately protect a paper ballot environment, properly doing so requires the right personnel, processes, and time for testing and validation. Without each of those in place prior to moving to a new system, security would be unmanageable.

9. Using optical scanners that were designed for low volume in a high volume environment would likely break those scanners.

I declare under penalty of perjury that the foregoing is true and correct to the best of my ability.

Executed this 13th day of August, 2018.

MERRITT BEAVER
Chief Information Officer in the office of the Secretary of State for the State of Georgia