# Summary of Voting System Software Change Issue

Last Wednesday, the Secretary of State directed election officials in 159 counties to wipe all of the existing software and prior election data from 34,000 BMDs and replace it with new, uncertified, untested software that was hastily written by Dominion over the prior weekend.

Georgia's voting systems, including software, require 1) certification by the federal Election Assistance Commission, 2) testing by approved labs, 3) testing by a state certification agent, 4) certification by the SOS prior to purchase, 4) acceptance testing after all modifications or repairs, and 5) election-specific Logic and Accuracy testing. Even if this was deemed a "de minimus change", the EAC must provide written approval prior to implementation (see attached notice)

The new Dominion system's certification is voided by installing new software that is not certified. Counties are not permitted to conduct elections with uncertified software.

With LAT already delayed more than 10 days, and in-person voting beginning Oct. 12, election supervisors across the state simply followed instructions – without fully considering the consequences and legal-noncompliance

- ***Potential for new, unintended problems*** - in complex systems like election equipment, last-minute "small" changes can introduce serious errors, not detectable for weeks, and resulting difficult-to-foresee consequences.
- ***Increased security risk*** - replacing the software now, on the eve of the election, creates numerous vectors by which an attacker could introduce malicious changes into BMDs state-wide.
- ***Invalid elections*** - use of the BMDs with modified and uncertified software violates several GA statutes, creating valid conditions for election results to be challenged and possibly overturned.

The attached letter from Bruce Brown, counsel for the Coalition for Good Governance to Fulton County attorney Cheryl Ringer spells out various laws Georgia Election Boards will violate if they use the touchscreen BMDs as planned.

The attached declaration submitted in federal court by Dr. Alex Halderman, a world leader in the study of security in voting systems, outlines the security risks. Additionally, internationally respected cybersecurity expert Harri Hursti filed a declaration Sunday on the dangers of the software being installed, also attached.

County Election Boards are ultimately accountable for running elections in compliance with law, and certifying the results. Counties will be blamed for problems that derive from using BMDs with uncertified software, even though the SOS directed it.

Today, the problem is confined to the BMDs – but once they are deployed, there is potential to put the entire system at risk.

Counties have the authority, and indeed the responsibility, to set aside the altered BMDs, and use ballots marked by pen for most in-person voting – reserving use of the BMDs for voters needing assistive devices. Clearly the modified BMDs are "impossible" and "impracticable" to use in a legally authorized way.

# Bruce P. Brown Law

October 3, 2020

**By Email**

Cheryl Ringer
Office of the County Attorney
141 Pryor St., SW
Suite 4038
Atlanta, Georgia 30303

Re: Fulton County Board of Elections' Ongoing Violations of State Law

Dear Cheryl:

The Fulton County Board of Elections has made many recent and welcome efforts to make voting more convenient and accessible. We enthusiastically commend such efforts. Given the Secretary of State's numerous reckless decisions regarding the upcoming election, however, Fulton is being lured into serious violations of Georgia's Election Code, as detailed below.

This week the Secretary of State disclosed that all of the existing software (and data, including evidence, from prior elections required to be preserved) must be wiped from the BMDs and replaced with new, uncertified, untested software that was written by Dominion just this past weekend. Fulton is complying with the State's ill-considered instructions, despite the fact that such actions are in plainly in violation of the Georgia Election Code.

You and the Board Members will recall that the Secretary unfairly blamed the Board for the "complete meltdown" that was the June Presidential Primary. The Secretary is either deliberately setting up the Board again to take the blame for another meltdown, or is recklessly unable to deploy its new systems in compliance with state law or federal constitutional requirements. Either way, the Board should not, and as a matter of Georgia law, cannot, allow it to continue.

We are confident that if the Board is made aware of these statutory violations that it will immediately bring Fulton County into compliance. The Board can do so by invoking the provisions for O.C.G.A. § 21-2-281, which allow the Board to switch to hand marked paper ballots in the event that using the BMDs is ***impossible*** or ***impracticable***. The conditions are expanded by State Election Board Rule 183-1-12-.11(2) (c) stating that if the BMDs are ***unusable***, impracticable or impossible for voting (c), and 183-1-12-.11(2)(d) adding that if ***insufficient*** BMDs are available, hand marked paper ballots should be used.

What follows a partial list of the Georgia statutes and Rules that the Board is currently violating:

1.   **<u>Illegal software is being installed on Fulton's BMDs (</u>**<u>violation of O.C.G.A. §§ 21-2-368(d); 21-2-379.24; 21-2-300(a)(3))</u>

Georgia law requires, at a bare minimum, that the following three steps be taken before voting system software may be used on election equipment:

First, O.C.G.A. §21-2-300(a)(3) requires that the system be certified by the federal EAC.  At this very moment, Dominion technicians, at the direction of the Secretary, are installing new software on Fulton's BMDs, software that Dominion has confirmed to Judge Totenberg has *not* been certified by the EAC.  This is *not* just a "patch" or revision: the prior election software is being wiped from the equipment and replaced in its entirely by new, uncertified, untested software.  This software has never been run in any election in any jurisdiction—not even a mock election—and was written this past weekend.

Second, Voting System Rule 590-8-1.01(d)(6) requires that, after the system is EAC certified, it be sent to a state certification agent for further testing and a report. With no EAC certification, this of course has not occurred.

Third, Voting System Rule 590-8-1.01(d)(7) requires that, after the state certification agent issues its report, the Secretary of State must make a determination whether to certify the system. Certification of new voting systems is required by O.C.G.A § 21-2-379.24.  The Secretary certified the prior BMD system, but not the system that Dominion technicians are installing on Fulton's BMDs this week.

Further, O.C.G.A. § 21-2-368(d) requires the Fulton Board: "At least ten days prior to any primary or election, including special primaries, special elections, and referendum elections, the election superintendent shall verify and certify in writing to the Secretary of State *that all voting will occur on equipment certified by the Secretary of State*."

Early voting begins in ten days and this Board has not, and cannot, make the necessary certification without misrepresenting the undisputed facts.

These are not hyper-technical or bureaucratic requirements, but mandatory provisions of Georgia law that were enacted to protect the security and reliability of the voting systems and voters' constitutional rights to cast an accountable ballot.  Untested and uncertified software can create errors in the operation and tallies of the BMDs and can carry bugs and malware into the database that can affect absentee ballots, reporting capabilities, and possibly pollbooks.

2. **Fulton is not conducting mandatory acceptance testing of the new software** (violation of Election Rule 183-1-12-03(1))

The Secretary of State's Voting Systems Rule 590-8-1-.01(d)(8) states, "[a]cceptance tests shall be performed in the user's environment to demonstrate that the voting system as delivered and installed is identical to the system that was certified by the State and satisfies the requirements specified in the procurement documents."

State Election Board Rule 183-1-12-03(1) states: "Upon the receipt of new, repaired, or upgraded components of the voting system, including electronic ballot markers . . . the election superintendent of the county is responsible to check that an acceptance test has been performed on the device in accordance with standards issued by the Secretary of State. No component of the voting system shall be placed into service until such time as the unit satisfactorily passes the prescribed acceptance tests."

Crucially, this Election Rule gives the *Board* the responsibility of assuring that satisfactory acceptance testing has been conducted. But Fulton has not done *any* acceptance testing or generated any of the required documentation. The Board is about to "place into service" components that have *not* passed "the prescribed acceptance tests," in complete violation of this Rule.

3. **Fulton is failing to conduct complete Logic and Accuracy Testing** (violation of O.C.G.A. §§ 21-2-379.25 (a) and (c))

O.C.G.A. §§ 21-2-379.25 (a) and (c) require that the county "verify that **each** device is properly recording votes and producing proper ballots," and that "the superintendent shall have **each** electronic ballot marker tested to ascertain that it will correctly record the votes cast for **all offices and on all question**."

Testing being conducted by Fulton, based on the Secretary's guidance, does not comply with this statute because it fails to "have each electronic ballot marker tested … for all offices and on all questions." As laid out in detail in the *Curling v. Raffensperger* litigation and discussed extensively in recent conferences with the Court where this Board was represented, the Secretary's procedure for LAT falls far short of the minimum statutory requirements that this Board is obligated to obey. The Secretary of State's representative testified in a recent hearing that conducting the LAT on BMD units at the levels required by statute is **impractical** and too time consuming to accomplish. The Board, however, remains legally obligated to voters to ensure that the statutorily required LAT be conducted.

4.    **<u>Fulton is failing to review accuracy of the election database</u>**
      (violation of Rules 183-1-12-.19 (5); 183-1-12-07(1))

Election Board Rule 183-1-12-07(1) states that "the election superintendent shall review the electronic databases used to generate ballots for correctness and accuracy."

Election Board Rule 183-1-12-(.19)(5) requires that "the county election superintendent shall provide to the Secretary of State or his or her designee a final copy of the election management system database for the county."

Again, in this Rule the State Election Board has transferred the responsibility for database review to this Board. We do not believe that Fulton is conducting the required database review for accuracy of its voluminous contents and configuration of the ballots and tabulation instructions, as required by the Election Code, or that it is sending a final corrected database to the Secretary prior to the election.

5.    **<u>Violation of absolute secrecy in voting</u>** (O.C.G.A. §§ 21-2-379.22(5) and 21-2-70)

O.C.G.A. § 21-2-70  directs this Board to guarantee the secrecy of the ballot:

> Each superintendent within his or her county or municipality shall exercise all the powers granted to him or her by this chapter and shall perform all the duties imposed upon him or her by this chapter, which shall include the following: . . .
>
> **(13)** To conduct all elections in such manner as to ***guarantee the secrecy of the ballot.***

The large well-lit BMD displays, however, advertise Fulton voters' votes to others in the polling place.  O.C.G.A. § 21-2-379.22 further provides:

> No electronic ballot marker shall be adopted or used in primaries or elections in this state unless it shall, at the time, satisfy the following requirements: . . .
>
> **(5)** Permit voting in ***absolute secrecy*** so that no person can see or know any other elector's votes, except when he or she has assisted the elector in voting, as prescribed by law;

Fulton's failure to take necessary action to ensure ballot secrecy not only is violating voters' rights but also invites challenges to the outcome because the secrecy of the ballot is not being guaranteed.

### Security failures

There are numerous gravely serious security failures at EPC that must be addressed. We have detailed some of them in our pleadings in the Curling case, and we continue to offer, without response from this Board, to have a meeting with the Board or management to share our concerns in more detail.

### Remedy Provided by the Election Code

The Georgia Election Code provides for adopting hand marked paper ballots instead of BMDs in cases like this one where it is impossible or impracticable to do so. Given that it is impossible to use the system and comply with many mandates of Georgia law, it is the duty of the Board to adopt hand marked paper ballots, which can be read with the optical scanner and thoroughly audited. Georgia statutes (O.C.G.A. §§ 21-2-281, 21-2-334) call for this solution, and recent SEB Election Rule 183-1-12-.11(2)(c)-(d) specifically supports its application when BMDs are impractical to use.

We would very much like the opportunity to discuss our concerns with you and the Board and urge the Board to not install or use this unreliable, untested and illegal system.

Please let me know if you have any questions.

Sincerely,

Bruce P. Brown

cc:    Kaye Burwell
       David Lowman
       Marilyn R. Marks
       Cary Ichter
       Robert A. McGuire

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

|  |  |
|---|---|
| **DONNA CURLING, ET AL.,** <br> **Plaintiffs,** <br><br> **v.** <br><br> **BRAD RAFFENSPERGER, ET AL.,** <br> **Defendants.** | **DECLARATION OF** <br> **J. ALEX HALDERMAN IN** <br> **SUPPORT OF MOTION FOR** <br> **PRELIMINARY INJUNCTION** <br><br><br> **Civil Action No. 1:17-CV-2989-AT** |

Pursuant to 28 U.S.C. § 1746, J. ALEX HALDERMAN declares under penalty of perjury that the following is true and correct:

1.      I hereby incorporate my previous declarations as if fully stated herein. I have personal knowledge of the facts in this declaration and, if called to testify as a witness, I would testify under oath to these facts.

2.      I was present via teleconference for today's proceedings and heard the testimony of Dr. Eric Coomer and Mr. Gabriel Sterling regarding the State's intention to make unplanned, last-minute changes to the software that operates Georgia's BMDs. This surprise development alarms me, for several reasons.

3.      First, changing voting equipment software on such short notice is far from routine, particularly barely a month before a Presidential election. This is

because altering the software risks unintentionally introducing new bugs, and it would provide an attractive vector for attackers seeking to spread malware.

4.      Second, even if the intended changes are "de minimis" (as Dr. Coomer testified), meaning they involve differences in a small number of lines of source code, the update process necessitates completely replacing the most important part of the BMD's software. Dr. Coomer testified that Georgia must install a new "APK"—the Android application package that contains nearly all of each BMD's Dominion-authored software—onto each of some 33,000 machines across 159 counties. Given the accelerated timeline, there is no practical way to reliably inspect the APKs and determine that the only change to BMDs' functionality is the intended fix, or that the change does not introduce new bugs or even malicious behavior.

5.      Third, in complex computerized systems like Georgia's election equipment, last-minute changes, even seemingly small ones, can introduce serious and difficult-to-foresee consequences. That is why rigorous testing of such changes is essential to ensure correct operation. An infamous recent example where such testing was cut short was the Boeing 737 Max aircraft. Boeing made a small last-minute software change to correct a single problem and inadvertently created a much

2

more dangerous failure mode that reportedly led directly to two fatal crashes.[1]

6.      By analogy, what Dominion and Georgia are proposing to do is like redesigning an aspect of an airplane that is about to take off. The rapid deployment of this change will necessitate omitting or cutting short even the ineffectual testing and security measures used during the initial rollout of the BMDs. Unlike the software it replaces, the new software will not have been subject to EAC testing or Pro V&V's full Georgia certification tests. There also is no indication that it will undergo acceptance testing to confirm that the correct software has been installed. Although, as I previously testified, these steps have limited utility for security, they at least help guard against bugs and human error that could otherwise undermine results or render equipment inoperable on election day and during early voting. If the change does create unforeseen problems, the result would be hugely disruptive. There already is too little time to safely modify Georgia's BMD software *once* before the November election, and there is certainly not enough time to modify it *twice* if problems caused by the first change need to be corrected—especially if the problems are not discovered until election day.

---

[1] Jack Nicas, Natalie Kitroeff, David Gelles and James Glanz, "Boeing Built Deadly Assumptions Into 737 Max, Blind to a Late Design Change," *The New York Times* (June 1, 2019).

7.      Finally, this last-minute software replacement compounds my previous concerns about the vulnerability of Georgia's BMD-based system. As I have already testified, malicious modifications to the BMDs' software could undermine the integrity of election results in multiple ways, including by changing either the barcodes alone or both the barcodes and the human readable text, with the result that election outcomes could be changed without detection. Replacing the software now, on the eve of the election, creates a vector by which an attacker could introduce malicious changes into BMDs state-wide. Malicious code could be introduced by what the defendants and their election experts often refer to as an "insider" at Pro V&V or by attackers who compromised the company's systems. It could also be introduced by modifying the software update package as it is being distributed to the state and onward to counties, or as the counties are copying it to machines across the state. As I previously testified, merely checking the hash of the software by using the BMDs' build-in features would not be sufficient to detect malicious alterations. The late-breaking nature of the change further increases the odds that such an attack would succeed, because whatever procedural protections are in place regarding software updates will need to be applied on a vastly accelerated basis involving every Georgia county, likely hundreds of personnel, and tens of thousands of machines.

4

8.      I am especially perplexed that the State has decided to accept these risks, because it would appear, based on today's testimony, that simple procedural changes could correct the asserted problem without any changes to the software. Dr. Coomer characterized the user-interface problem as occurring only once each time a BMD is powered on and operated. If this is the case, the State should be able to simply instruct poll workers, after turning on each BMD, to print a test ballot and trigger the aberrant behavior before voters begin using the machine. By Dr. Coomer's description, the problem would not occur again until the BMD was rebooted. Dominion could correct the underlying software after the election, leaving time for a complete battery of critically important tests. That Georgia has chosen to accept the much greater risks of a last-minute software change suggests that the problem or problems being addressed may be more complex than has been described, making a hasty, untested fix all the more dangerous.

I declare under penalty of the perjury laws of the State of Georgia and the United States that the foregoing is true and correct and that this declaration was executed this 28th day of September, 2020 in Ann Arbor, Michigan.

_____

J. ALEX HALDERMAN

5

## DECLARATION OF HARRI HURSTI

Pursuant to 28 U.S.C. § 1746, HARRI HURSTI declares under penalty of perjury that the following is true and correct:

1.      This declaration supplements my prior declarations (Docs. 680-1, 800-2, 809-3, 860-1, 877, and 923-2) a nd I stand by the statements in those declarations.

2.      I arrived at the Fulton County Election Preparation Center ("EPC") on October 1, 2020 around 3:45pm. I was there in my capacity as an expert engaged by the Coalition Plaintiffs to conduct a Rule 34 inspection. (Exhibit 1) . I was accompanied during part of my visit by Marilyn Marks of Coalition for Good Governance.

3.      My goal for this observation and inspection was to review the ongoing updating of the Dominion software for Fulton County ballot marking device ("BMD") touchscreen units to ICX software version 5.5.10.32. It is my understanding that Fulton has an inventory of over 3,300 BMD touchscreens, all of which are to be updated with this software. A number of the machines were in the EPC warehouse and were staged to be updated or marked after the update had been completed.

4.      Upon our arrival, Ms. Marks and I were informed by Derrick Gilstrap, the manager of EPC, that all of the people working to upgrade the devices were

1

Dominion technicians. Mr. Gilstrap stated that he did not feel comfortable installing a last-minute software change, and did not want Fulton County staff to be responsible for installing it.  He told us that he told Dominion to conduct this operation, prior to having his staff install the November 2020 election programming and Logic and Accuracy testing ("LAT").

5.      Mr. Gilstrap told us that after the software update step that LAT would immediately begin, and made no mention of Acceptance Testing that should occur prior to LAT.

6.      Acceptance Testing is an almost universally mandated basic test of the hardware and software when a change or repair to either has been made before counties are permitted to install election programming and deploy voting system components. Acceptance testing must be performed on each unit, and cannot be performed on a sample basis. Fulton's failure to conduct such testing should be a serious warning sign of further recklessness in the installation of inadequately tested software.

7.      Mr. Gilstrap stated that Dominion had started the software update project with four workers, but soon realized that the task would take extended periods of time.   Mr. Gilstrap stated that Dominion had accordingly increased the workforce to 14 and expected the installation work to be completed on Monday, October 5.

2

8.      The new software was contained on USB sticks.  However, there was no inventory management present for the USB sticks. There also was no inventory control for the technician authorization smartcards, which provide access to the controls of the touchscreen. Workers did not sign or otherwise document when they took possession or returned the technician cards and software upgrade USB sticks. Those items were in an open plastic bag which was sometimes placed on table, and sometimes carried around the working area by the manager. Anyone was able to pick up a USB stick or drop them there freely, permitting the easy substitution of USB sticks containing malware or to leave the premises with copies of the software update.

9.      Some workers worked one BMD touchscreen machine at the time, while others simultaneously worked on 2 or 3 machines. There was no accountability for how many sticks and technician smart-cards each worker had in their possession. Clearly, the USB sticks were not considered to be security sensitive items at all.

10.     Some of the workers had instructions for software update visible in their pockets, while others did not seem to have the instructions readily available. One worker showed me the instructions, but it was different from the instructions I had seen that were sent to the counties. None of the technicians that I observed were following the instructions as they installed the new software.

3

11.     Technicians were not following a common process, and they all made their own variations on the workflow.  In my experience, this can negatively affect the quality and reliability of the software installation.  Many workers were texting and making phone calls while working and not focusing on their work. As a result, I observed repeated human errors such as skipping steps of the process.

12.     Some workers consistently took an extra step to destroy previous application data before uninstalling the old version of the software. Uninstalling software packages results in destroying application data, but that is known to be unreliable in old versions of Android. The step they took is ensuring, among other things, destruction of forensic evidence of Fulton's use of the equipment in prior elections.

13.     To avoid destruction of all forensic evidence from the BMDs, a number of images of the electronic data contained on the BMDs should be taken from a sample of them before installation of the new software.

14.     As part of the updating process, the workers are directed to enable the "Install from Unknown Sources" setting. This is an insecure mode because it turns off the operating system verification of trusted sources and therefore allows software from any source to be installed. During the 45 minutes of my observation, I observed that many units had been left in insecure mode. I estimate 15% of the units were already in the insecure mode when the work began on them, having

4

been left that way during the last software installations, or because of interim tampering.

15.     As described before, most workers I observed were not focusing on the work they were tasked to do, and as result, they were accidentally skipping steps. I observed that, as result of these human errors, the units were erroneously left in the insecure mode either by the workers skipping the step to place the machine into the secure mode after upgrade, or doing the step at such a fast pace that the system did not register the touch to toggle the switch and the worker did not stop to verify the action.

16.     The State Defendants and Dominion have repeatedly overstated the value of their hash test, but my observation showed that they themselves are not relying on such test as a control measure.   Dominion workers are not even checking the hash value.  I deliberately followed many workers when they processed the units. During over 45 minutes of observation, none of the workers took the step of verifying the hash value. Some workers did not realize that the upgrade had failed and the mistake was only caught by persons who were closing the cabinets when and if they looked at the software version numbers before closing the doors.

17.     I also observed random errors that were not caused by humans. For example, software sometimes refused to uninstall because the uninstall button was

disabled, or the installation silently failed.  The technicians treated devices with issues by simply rebooting them.  Technicians made no effort to diagnose or document the cause of the issues. The casual nature of dealing with the irregularities caused me to conclude that these abnormal incidents are commonplace.

18.    Based on my observations of the software update, I would anticipate that these machines are likely to behave inconsistently in the polling place, depending on a number of factors including the care taken in the software installation process.

19.    The current abbreviated LAT protocol adopted by Fulton County and the State cannot be relied on to identify problems created by the new software or its installation (or other problems with programming and configuration unrelated to the new software). Even if counties were conducting the full LAT required, it is but one step that is needed, and is quite insufficient for ensuring the reliability of the BMD touchscreens—which at the end of the day, simply cannot be done.

20.    In my professional opinion, the methods and processes of adopting and installing this software change is completely unacceptable.  The methods and processes adopted by Dominion and Fulton County do not meet national standards for managing voting system technical problems and remedies, and should not be accepted for use in a public election under any circumstances.

21.     It is important that full details of the software change made be available for analysis and testing to determine the potential impact of the changes. I concur with Dr. Halderman's opinion in Paragraph 8 of his September 28, 2020 declaration (Doc. 923-1), in which he states that if the problem is as limited as described by Dominion, it could have been addressed with far less risk by the State without making an uncertified, untested software change.

22.     In my opinion, the installation of the last-minute software change adds intolerable risk to the upcoming election, and the simple solution of removing the BMD units from the process and adopting hand marked paper ballots is imperative.

23.     I note that I wanted to document the upgrading process, but Mr. Gilstrap told me that I was prohibited from taking photographs or video. I showed him the Rule 34 inspection document and pointed out the paragraph permitting photographing. He read that carefully but told me that he needed to clear that with his superiors before I could start taking pictures.  He never cleared this with his superiors while we were there.

I declare under penalty of the perjury laws of the State of Georgia and the United States that the foregoing is true and correct and that this declaration was executed this 4th day of October, 2020 in Atlanta, Georgia.

Harri Hursti

**U.S. Election Assistance Commission**

Voting System Testing and Certification Program

1335 East West Highway, Suite 4300

Silver Spring, MD. 20910

# Notice of Clarification

## NOC 19-01: Software De Minimis Changes
**Issued by Program Director, November 15, 2019**

## Section of Certification Manual to Be Clarified:

### Testing & Certification Program (Cert) Manual, Version 2.0

3.4.2    De Minimis Change - Defined. A de minimis change is a change to a certified voting system's hardware, software, TDP, or data, the nature of which will not materially alter the system's reliability, functionality, capability, or operation. Under no circumstances shall a change be considered de minimis if it has reasonable and identifiable potential to impact the system's performance and compliance with the applicable voting Standard.

3.4.3    De Minimis Change – Procedure. Manufacturers who wish to implement a proposed de minimis change must submit it for VSTL review and endorsement and EAC approval. A proposed de minimis change may not be implemented as such until it has been approved in writing by the EAC.

3.4.3.1    VSTL Review. Manufacturers must submit any proposed de minimis change to a VSTL and the EAC for review and endorsement. The Manufacturer will provide the VSTL: (1) a detailed description of the change; (2) a description of the facts giving rise to or necessitating the change; (3) the basis for its determination that the change will not alter the system's reliability, functionality, or operation; (4) upon request of the VSTL, a sample voting system at issue or any relevant technical information needed to make the determination; (5) document any potential impact to election officials currently using the system and any required notifications to those officials; (6) a description of how this change will impact any relevant system documentation; and (7)