EXHIBIT

17

SUPPLEMENTAL DECLARATION OF HARRI HURSTI

Pursuant to 28 U.S.C. § 1746, I declare under penalty of perjury that the foregoing is true and correct.

1. My name is Harri Hursti. I am over the age of 21 and competent to give this testimony. The facts stated in this declaration are based on my personal knowledge, unless stated otherwise.

2. My background and qualifications in voting system cybersecurity are set forth in my December 16, 2019 declaration. (Doc. 680-1, pages 37 *et seq*). I stand by everything in that declaration, my August 21, 2020 declaration. (Doc. 800-2), and my August 24, 2020 declaration (Doc. 809-3)

Responses to State's Assertions

1. While the State attempts to minimize my experience with the Dominion Voting System used in Georgia, there are only a few independent voting system researchers with more hands-on experience than I have with key components of the Dominion Voting System elements. To my knowledge, no jurisdiction has permitted, and Dominion has not permitted, independent research, academic or otherwise, to be conducted on its systems, which greatly limits the number of people with any experience with the Dominion system.

2. For the last 4 years I have co-organized the DEF CON Voting Machine Hacking Village, which I co-founded. DEFCON in one of the oldest and largest annual security and hacker community meetings, attracting in 2019 over 30,000 participants into Las Vegas.

3. In the Voting Machine Hacking Village at DEF CON 27, we had a Dominion ImageCast Precinct device available for studying. In the publicly available DEF CON Voting Machine Hacking Village Annual Report of 2019, we outline on pages 18 and 19 the security weaknesses, vulnerabilities and exploitations of those discovered by the participants. Intentionally, the report does not disclose to the public the details of how the exploits were constructed, but rather provides a high-level overview of the discoveries. The underlining significance is that the people studying the machine had no prior knowledge or documentation of the system and yet achieved all discoveries in under 20 hours of working time. As co-organizer of the Village, I personally kept myself up to date with their work, including discoveries and details which were not reported in the annual report.

4. The State appears to challenge my opinion that the voting system server had not been hardened. (Doc. 834 at 5-6) My statements about the failure to harden the system and the accompanied pictures were referring to the Election Management and Tabulation Servers, specifically in Fulton County.

5. I declared that the servers *appeared* to not be hardened since at the time the only limited evidence available was my visual observation of device's user interface from a distance. The process of testing hardening is called penetration testing, which is a standard security practice. Subsequently, through Coalition Plaintiffs' discovery, on August 25, I obtained partial and time-limited event log files for both August 11th and August 25th.

6. A review and preliminary analysis of the log entries has since confirmed that services which would had been disabled in the hardening process are running on the server. The EMS server system logs I reviewed confirmed that services enabling remote access to the system entered into the running state on the EMS server. However, security log entries were are not available; these entries would have shown if remote access features were used. Fulton's EMS event log files for August 11th have a cut-off point at 17:31:50. The logs seem to be configured to run with maximum size, and then the log rolls over and the older log entries are lost. For example, one security log has 33,671 entries, and the first one is from 17:02:29, covering merely 29 minutes and 21 seconds of activities. This is a completely unacceptable practice. No acceptable practices would flood the security log this way. For example, at 17:03:49, a single second consisted of 258 security log entries of which 127 were consecutive logoff messages for ending sessions. This is called log flooding, and while it could be a result of

misconfiguration, it should always be investigated as an indication of irregularities, because, among other causes, it is a known method for attackers to destroy evidence.

7. I stand by my statement that the lack of security logs further strengthens my professional opinion of no confidence in the operations of the August 11th vote count, because the most basic feature of system security is missing-- an audit trail. The Windows log system is designed to split different entries into separate logs, and one log missing in most cases degenerates the value of all. The most basic security practices mandate maintaining and protecting reliable security logs, and this standard practice is not specific to election security. These are standard minimum practices which are essential parts of any good security practice in any system requiring cybersecurity.

Scanner and Tabulation Software Issues

8. I believe there is confusion in Georgia's election security conversation between the terms: scanner settings and election software vote-mark thresholds. Those are two separate settings, processed by separate software. Scanner settings do not affect image processing within the election software. Scanner settings are used by TWAIN API to configure the scanner and contain parameters which are of paramount importance when the thresholds are applied to produce a 1-bit image. The Dominion ballot image is a 1-bit image.

9. Election software processing starts from that 1-bit image (also known as “bi-level image”, and thresholds used to determine the mark thresholds are applied to that image. As the original image and majority of the information captured by the scanner is permanently lost in the conversion into a 1-bit image, the election software settings cannot overrule the scanner settings, but the scanner settings can de facto overrule the effectiveness of the election software settings. EXHIBIT E to my August 24 declaration shows the user instructions and a picture of the interface used by the user to verify and select scanner settings. The voter mark threshold value is not part of this user interface, as that is applied later in the election software against the images. The method of storing and applying the later values, inside a database or without, are irrelevant. The process of acquiring the image and preprocessing is separate and a precursor in election software activities.

10. The images obtained from Fulton County via Coalition Plaintiffs’ discovery make it clear that the ballot scanner itself does not process the ballot with fixed values in image processing prior to the election software. This is evident from Exhibit A. These are scanning the printed ovals on the paper ballots – as these are industrially produced in a printing process of the ballot, there should be no difference whatsoever how the scanner images those black ovals.

11. However, as the examples show, not even the identical printed ink registers uniformly the same on the ballots – and therefore neither will the vote the

voter casts. This also demonstrates one of the reasons why fixed threshold values alone for election software vote mark determination cannot solve the problem as the State Election Board is attempting to do. These values would be applied against the input image, which is not reliably reflecting the markings on the paper ballots. The scanner does not produce uniform images from the ballots. The root cause of this behavior is unclear.

12. Any attempt to merely re-bracket the thresholds (as the State Election Board is attempting) to a seemingly more reasonable standard without considerable research will continue to result in valid votes not being counted because of poor quality images are being used as the source document for electronic counting.

Explanation of Ballot Scanning Technology

13. The modern scanner does not take a picture of the paper. It illuminates the paper with 3 different colors - in essence taking 3 separate gray-scale images from the paper in different lighting. The next step is to combine, in software, these 3 images by assigning colors into the gray-scales and processing those to create an approximation of what the human eye would had seen. While the scanner observes red, green and blue equally, the human eye does not. The human eye is more sensitive to green than other colors and therefore the software is not taking the image as reported by the sensors, but processing that image to

correspond the human eye. This phase of the process includes many algorithms to create the image and clean the image by removing artifacts.

14. The resulting color image can be converted to gray-scale image and further to 1-bit, bi-level, black-or-white images. In this phase colors are again assigned values. Even darkest of yellow is not black, but darkest of blue can be very close to black. With these values, the colors are collapsed into values from 0 to 255 representing how relatively dark the human eye would see the color. The last step is typically just further cutting the into black-or-white by assigning white to all pixels under 50% gray and black to over 50% gray. As a result, a marking which is unquestionably clear to human can end up to be plain white, that is, no visible marking at all.

15. By the late 1970s, this 1-bit bi-level image processing was found unacceptable with early fax machines. To compensate the loss of image information, fax machines employed a technique called rastering to emulate gray-scales in 1-bit images. However, Dominion ballot image files do not employ this long available technique to compensate the effects loss of data.

16. I shall describe how dynamic settings adjust contrast in the grayscale and wash out information from the 1-bit image as a result. Historically, very often the documents being scanned are not originals, but were photocopies of the originals or copies of the copies. To improve the quality of pre-deteriorated

material, dynamic settings for brightness and contrast were developed to "wash out" the defects caused by copying, like white background not being white and black not being black and a variety of speckles that appear across the paper. In essence, the goal is to make the text easier to read by the human eye by removing anomalies and weaker markings. When this kind of techniques are applied and then the image converted to black-or-white pixels, the image becomes brittle, and intentional markings being lost.

17. While this process is useful for making text on this page easier to read, it can degrade human markings on a ballot. The human brain with the experience recognizes the markings better, when excess markings are removed – in contrast, Dominion software utilizes no intelligence and merely tries to calculate a value to make the determination. Therefore, this family of image enhancement features is not compatible with the approach chosen by the developers of the Dominion system.

18. Excerpts of the ballot vote targets in the Exhibit A are not degenerated as result of production for this document. These are degenerated this way in the original images obtained from Fulton County. While it is unclear what caused the failure to scan the vote target identically from identical sources, this kind of quality difference between documents is typical for dynamically adjusting

parameters. When the input material is not uniform, it cannot be measured in later process with fixed thresholds.

Fulton County Election Preparation Center August 25 observations

19. I visited the Fulton County Election Preparation Center ("EPC") on August 25 from 10:50am to approximately 5pm. I had visited the Center multiple times and am generally familiar with their equipment configuration.

20. I was at EPC to conduct scanner testing using the original voter marked ballots that were rejected for scanning and hand duplicated in the June 9, 2020 election, as agreed with Fulton County in the discovery process. I was accompanied by Marilyn Marks and later in the afternoon by Rhonda Martin, of Coalition for Good Governance.

21. The Dominion technician (Dominic) had full operating control of the system as he had before during my visits on August 11 and August 17. Fulton County employees seem to have little to do with operating the server component of the system and little familiarity with it.

22. The failure of accountable election officials to have direct control of the voting system with proper administrative controls that prevent vendors and third parties from accessing the system is a troubling sign to voting system security

experts. Allowing vendors to operating voting systems greatly exacerbates the already lax security conditions and insider risks.

23. Before the scanning of the ballot started, Dominion technicians pulled up a new scanner options screen on the server monitor. I had not seen that screen before, nor had I seen references to it in the Dominion system documentation.

24. The computer driving the high-volume mail ballot scanner has a different Windows configuration than other election tabulation servers I observed before at EPC. This further elevates the suspicion that in addition to lack of system hardening, version management of the operating system has not been performed.

25. The high-volume ballot scanner scanned between 64 and 70 ballots per minute on the longer uninterrupted runs.

26. When Dominic tried to upload scanned ballots from the ICC (high volume) scanner computer to the central tabulation computer, the same or very similar issues observed August 11 and August 17 repeated starting 11:40 am. (Exhibit B)

27. Dominic and other staff members started reading screen logs recorded on August 11 to understand what had happened. On the election night when I was observing the operations, Dominic was not involved with the troubleshooting, as he was performing operations with IPC uploads. The server logs I was provided through discovery revealed that the issue had already happened August 11 earlier

than I observed on the Election night. The logs revealed that operators had attempted to process ballot images for a period of time ending at 5:31:50 pm, and the same issues had appeared then too. Due to the fact that the logs end at 5:31:50 pm, I cannot compare the logs to the errors I observed on the election night. (Exhibit C)

28. The system operators were comparing log entries for August 11 and August 25. I got the clear impression that the issue had appeared on August 11 more than once, and was encountered on August 11 before I arrived to observe. The logs I reviewed revealed repeated errors of this nature.

29. The privileges observed on the screen reveal that Dominion staff members operating the server have privileges to delete individual log events and filter log entries for selective saving. This means that the logs produced now cannot be trusted to accurately reflect the history of transactions on the server. The most basic security practice is to never let the operators have privileges to delete or alter log events, because that makes supervision impossible and performing forensics difficult, if not impossible. In addition, trustworthy logs are essential to detect and deter malicious software or intrusion.

30. In the troubleshooting efforts, Dominic opened a Windows command line window. This told me that he has a level of sophistication typical for power users.

31. The troubleshooting followed the same trial-and-error pattern until 12:15pm. At that time, a Dominion employee again walked behind the rack and rewired something and inserted an USB stick behind the server. After rewiring, the Doninon employees started using the same screen as previously used as the main operating computer to access and directly interact with the main server on the rack. This server appeared to have yet another Windows configuration, and potentially version. (Video Exhibit E shows that the operations behind the rack cannot be observed and Exhibit F shows the new screen layout consistent with Windows Server user interface and distinctly different from Windows 10)

32. In the troubleshooting, the user list was displayed, and the list included account "Guest," which is one of the first things removed when a server is hardened. It is possible that the account has been disabled, but the standard practice is to remove the account to ensure that it will not get inadvertently reactivated in the future. (Exhibit G)

33. Dominic opened a text file containing the key passwords into the election system which was visible on the screen. It is completely unacceptable practice to have the passwords stored in clear text in the very system which is protected by the passwords in question. This is like posting the combination of a safe in a Post-it notes on safe door. This further reinforces the conclusion that even

the most basic security principles and best practices are ignored in Fulton County's election server operation. (Exhibit H – the actual passwords blurred)

34. Dominion staff wound down their efforts to troubleshoot the issue.

35. I requested the images of the test ballots that we had created on the scan test on August 17. Those images were created by the IPC (precinct) scanner we were using. Dominic, the Dominion employee, offered the excuse that the scanner does not record images and showed me server directory with no images. I countered him, telling him that the scanner needs to capture images in order to be able to process barcodes (votes). I furthermore pointed out that he had on August 17 loaded the memory card without checking "load images" option. He showed the dialog box, and "load images" was unchecked and when I asked him to check the box, it turned on. At Exhibit I is a photograph I took of the unchecked boxes showing the options of loading only results or images and audit logs as well.

36. When I asked if he could now reload the memory card with our test ballots, he refused to do so, telling me that he been trained to only load results on the server from the card and not to load the images or the audit logs of the precinct scanners. He further explained that he will load the images only if "his boss from Dominion" tells him to do so and recommended that someone call his boss.

37. From this point on, it become clear that Dominic (Dominion staff) was considered to be in charge of the election server operation and accepted

commands only Dominion management, not Fulton election officials. He repeated the same to county officials saying, "if I am told by my boss to do so, then I will".

38. And around 1 pm we left for lunch while Dominic stated that he had to go visit the Dominion office to get help with the loading of images.

39. When we returned, the server had a screen revealing Microsoft warning message that the software has not been activated – commonly a hallmark of unlicensed "pirated" software. This message can also activate if a substantial part of the server hardware is replaced, causing Windows to consider it to be another computer other than the one the system was licensed for. (Exhibit J)

40. I later watched Dominic shut down all computers other than the server. Yet the network switch in the rack lit to indicate repeating bursts of traffic. Computers which are connected to the Internet frequently transmit data, but I was repeatedly told that the rack network is air gapped. When all computers other than the server were off, and nobody was operating the server, what was causing the traffic bursts is unexplained. It is normal that network switch blinks periodically when server is looking for appliances and other Plug and Play (PnP) devices, but continuous bursts do not fit into that pattern. (Video Exhibit H)

41. When Dominion people realized my interest on the network switch lights, they locked the rack, closing the mesh doors in front of the machines, obscuring visual access.

42. Later Fulton County election official Ralph Jones came to explain that Dominion refused to "give *their* ballots" to us or allow anyone to "use *their* software" to produce records for me for either the test ballots or the June 9 duplicated ballots we had scanned. This statement made no sense to me, because my understanding based on publicly available information is that the county has licensed the software for their use and the voted ballots and images under no circumstances are the property of Dominion.

43. Later I was furnished what was supposed to be the log files for the day's (August 25) activities. A quick look revealed that the logs were not August 25th logs but instead logs of August 11th ending about 5:32pm. After asking for a correction, I realized that, unbeknownst to me, one more Dominion employee had arrived and was troubleshooting in Derrick Gilstrap's office. They again went behind the rack and eventually wrote an USB stick, which was taken out of my view to the office where the additional Dominion employee was working. About 5 minutes later, I was brought USB stick with the August 25th logs.

44. I have been able to start the preliminary analysis of the logs, and the first discovery is that both the August 11th and August 25th logs are incomplete. In the case of the August 25th logs, the logs end at about 12:25pm, shortly after the Dominion employee walked behind the rack and while the activities were still ongoing before adjourning for the lunch. No activities during lunch break were

recorded, while the screens when we returned showed that subsequent activities had taken place

Conclusions from August 25 EPC visit

45. Dominion staff has total control over the server and its logs and therefore the logs are no longer trustworthy. Furthermore, when recent logs were copied for us, they were taken out of view for enough time for a capable person to have ample of time to clean those logs.

46. Fast security log rotation is unacceptable. If there is a secondary storage where the completed logs are stored, those should have been produced to us. Without security logs, it is not possible to determine when remote access software was activated or the activities on the election night.

47. Frequently bursting network traffic when the system was mainly shut down is suspicious and should be investigated.

48. Excuses claiming that the images are not recording, followed by the refusal to load the images is suspicious. If there were no images on the card, a logical action would be to demonstrate that by attempting to load the images to show that there is nothing, instead of claiming that they cannot do so if not ordered by Dominion, even if Fulton County so instructs.

Logic and Accuracy Testing

49. The State Defendants seem to misunderstand the importance of basic functional Logic and Accuracy testing of voting machines. The BMD touchscreens, printers and scanners are all easily hacked and subject to erroneous ballot building and malfunction and should not be deployed into the polling places until each machine has been tested for its ability to accurately register a vote for each candidate in each race and to register an undervote in each contest. The system is far too unreliable to conduct sample counts testing as little as a vote for one candidate for an entire precinct's machines.

50. Although Mr. Chris Harvey said in his declaration (Doc 834-3 ¶¶6-7) that testing all choices on all machines is "overly burdensome and unnecessary because it would require creating and printing" an extremely large test deck. The size of a test deck would rarely be unwieldy, but more importantly, BMDs require testing at minimum level of casting a vote for each position for each race. The cost of such inconvenience and labor expense for standard Logic and Accuracy Testing of BMDs should be factored into the purchase decision, and not shortcut after the fact, furthering diminishing the security of the system.

This 1st day of September, 2020.

Harri Hursti