DECLERATION OF DR. NAVID KESHAVARZ-NIA

I, Navid Keshavarz-Nia, declare as follows:

1. I am 59 years old and have been a resident of Temecula, California for one year. Previously, I resided in the Washington DC metropolitan area for nearly forty years. I have personal knowledge of the contents of this Declaration and if called as a witness, I could and would testify competently as to their truth.
2. I have a Bachelor's degree in Electrical and Computer Engineering and a Master's degree in Electronics and Computer Engineering from George Mason University, a Ph.D. degree in Management of Engineering and Technology from CalSouthern University and a Doctoral (Ed.D) degree in Education from George Washington University. I have advanced training from the Defense Intelligence Agency (DIA), Central Intelligence Agency (CIA), National Security Agency (NSA), DHS office of Intelligence & Analysis (I&A) and Massachusetts Institute of Technology (MIT).
3. I am employed by a large defense contractor as a chief cyber security engineer and a subject-matter expert in cyber security. During my career, I have conducted security assessment, data analysis and security counterintelligence, and forensics investigations on hundreds of systems. My experience spans 35 years performing technical assessment, mathematical modeling, cyber-attack pattern analysis, and security counterintelligence linked to FIS operators, including China, Iran, North Korea, and Russia. I have worked as a consultant and subject-matter expert supporting the Department of Defense, FBI and US Intelligence Community (USIC) agencies such as the DIA, CIA, NSA, NGA, and the DHS I&A supporting counterintelligence, including supporting law enforcement investigations.
4. The USIC has developed the Hammer and Scorecard tools, which were released by Wiki Leaks and independently confirmed by Lt. Gen Thomas McInerney (USAF, retired), Kirk Wiebe, former NSA official and Dennis Montgomery, former CIA analyst). The Hammer and Scorecard capabilities are tradecrafts used by US intelligence analysts to conduct MITM attacks on foreign voting systems, including the

Dominion Voting System (DVS) Democracy Suite and Systems and Software (ES&S) voting machines without leaving an electronic fingerprint. As such, these tools are used by nefarious operators to influence voting systems by covertly accessing DVS and altering the results in real-time and without leaving an electronic fingerprint. The DVS Democracy Suite Election Management System (EMS) consists of a set of applications that perform pre-voting and post-voting activities.

5. I have conducted data collection and forensic analysis using a combination of signals intelligence (SIGINT), human intelligence (HUMINT) and open source intelligence (OSINT) data associated with Chinese and other Foreign Intelligence Service (FIS) operators targeting US critical infrastructures. In that capacity, I have also conducted ethical hacking to support USIC missions.

6. I have performed forensic analysis of electronic voting systems, including the DVS Democracy Suite, ES&S (acquired by DVS), Scytl/SOE Software, and the Smartmatic systems used in hundreds of precincts in key battleground states. I have previously discovered major exploitable vulnerabilities in DVS and ES&S that permit a nefarious operator to perform sensitive functions via its built-in covert backdoor. The backdoor enables an operator to access to perform system updates and testing via the Internet without detection. However, it can also be used to conduct illicit activities such as shifting votes, deleting votes, or adding votes in real-time (Source: DVS Democracy Suite EMS Manual, version 5.11-CO::7, P.43). These events can take place through the Internet and without leaving a trace.

7. During my career, I have studied network communication reports that show DVS data being transferred to Internet Protocol (IP) addresses registered to Scytl in Barcelona, Spain. The results showed that Scytl maintained its SOE Software servers in a Barcelona data center for disaster recovery and backup purposes. In 2020, the SOE Software data center was moved to Frankfurt Germany where I believe 2020 election data was transferred.

8. Dominion Voting Systems (DVS) Corporation was founded in 2003 in Toronto, Ontario, Canada, by John Poulos and James Hoover. The company develops proprietary software and sells electronic voting

hardware and software, including voting machines and tabulators, throughout the United States and other parts of the world. DVS reportedly had a strategic relationship with Venezuela's Bitza Corporation, which was 28% owned by the former President Chavez. Intelligence reports indicate that the DVS/Bitza software was co-developed in Venezuela to alter vote counts to ensure President Chavez (and later, President Maduro) were guaranteed to win an election. The combined DVS/Bitza software was used in numerous countries such as Bolivia and Philippines to forge election results to favor a specific candidate. Subsequently, DVS and its international partners, including Diebold/ES&S (later acquired by DVS), Scytl, SOE Software/eClarity and Smartmatic to establish a global monopoly.

9. Reports show that DVS is comprised of several companies which obfuscate its true organizational and ownership structures. The DVS companies include: 1) Dominion Voting Systems International Corporation, a Barbados corporation; 2) Dominion Voting Systems, Inc., a Delaware corporation; and 3) Dominion Voting Systems Corporation, a Canadian corporation. Similarly, Smartmatic is comprised of: 1) Smartmatic International Corporation, a Barbados corporation; 2) Smartmatic USA Corporation, a Delaware corporation; 3) Smartmatic International Holding B.V, a Netherlands corporation; and 4) Smartmatic TIM Corporation, a Philippines corporation. Based on my counterintelligence experience in USIC, I conclude that corporate structures were partially designed to obfuscate their complex relationships, especially with Venezuela, China and Cuba; and impede discovery by investigators.

10. According to NT Times, in April 2018, J. Alex Halderman from University of Michigan computer scientist demonstrated in a video how simple it is to rig a DVS machine. In the video, Dr. Halderman demonstrates how easy it is to rig the DVS machine. The name of the video is "I Hacked an Election. So Can the Russians." A caption next to the title read "It's time America's leaders got serious about voting security." (Source: https://www.c-span.org/video/?463480-4/washington-journal-j-alex-halderman-discusses-election-security)

11. Despite DVS's constant denial about the flaws of its systems, the company's ImageCast Precinct optical scanner system was totally hacked in August 2019. This occurred during the largest and most notable hacker convention, called DEFCON Voting Machine Hacking Village in Nevada. The DVS ImageCast Precinct is an integrated hybrid voting equipment by combining an optical paper ballot and ballot marking device to allow accessibility for the visually impaired. The system runs the Busybox Linux 1.7.4 operating system, which has known medium to high level exploitable vulnerabilities to allow remote attackers to compromise the VDS. (J. Moss, H. Hurtsi, M. Blaze et al., Voting Village Report, DEFCON Village Report in association with and Georgetown University Law Studies; Online Source: https://media.defcon.org/DEF%20CON%2027/voting-village-report-defcon27.pdf). The report indicated that "many of the specific vulnerabilities reported over a decade earlier (in the California and Ohio studies, for example) are still present in these systems today (A. Padilla, Consolidated report by California Secretary of State, Top-to-Bottom Review summary and detailed report, Page 4 (Online Source: https://www.sos.ca.gov/elections/ovsta/frequently-requested-information/top-bottom-review)

12. In 2019, a computer laptop and several USB memory cards containing the cryptographic key to access DVS systems were stolen in Philadelphia. The company disputes the risks posed by lost USB memory cards containing the cryptographic key. However, according to the election security expert Eddie Perez of the nonpartisan OSET Institute states "it is very common that a USB memory card has a wealth of information that is related not only to the configuration of the election and its ballot — and the behavior of the voting device — but also internal system data used to validate the election." I have previously analyzed the contents of the DVS and other voting system cryptographic keys. I believe that USB memory cards were used to facilitate administrative access to the backdoor to disrupt polling operations and impact ballot counting across MI, GA, PA, AZ and WI.

13. In 2018, NY Times conducted an investigation and concluded that DVS machines can be easily hacked. Subsequently, security experts conducted comprehensive security testing on DVS in August 2019 and

discovered innumerable exploitable vulnerabilities that do not require extensive technical skill to breach. The DEFCON report identified major exploitable security flaws in DVS that were shared with the vendor. However, there is ample indication that these problems were not resolved. Moreover, DVS maintains the position that its voting machines are fully secure. They continue to avoid transparency or make their software codes to be analyzed by independent security investigators. In turn, December 2019, Senators Elizabeth Warren, Ron Wyden and Amy Klobuchar, along with Democratic Representative Mark Pocan raised major concerns regarding security vulnerabilities in DVS machines.

14. In my expert opinion, the combination of DVS, Scytl/SOE Software/eClarity and Smartmatic are vulnerable to data manipulation by unauthorized means. My judgment is based on conducting more than a dozen experiments combined with analyzing the 2020 Election data sets. Additionally, a number of investigators have examined DVS and reported their security findings (J. Schwartz, Scientific American Journal, 2018; DEFCON 2019; L. Norden et. al, America's Voting Machines at Risk, Brennan Center for Justice, NYU Law, 2014) confirming that electronic voting machines, including DVS have glaring security weaknesses that have remained unresolved.

15. I have not been granted access to examine any of the systems used in the 2020 Election. However, I have conducted detailed analysis of the NY Times data sets and have discovered significant anomalies are caused by fraudulent manipulation of the results. In my expert judgment, the evidence is widespread and throughout all battleground states I have studied. I conclude the following:

    a. The vote count distribution in PA, WI, MI, AZ, NV, and GA are not based on normal system operation. Instead, they are caused by fraudulent electronic manipulation of the targeted voting machines.

    b. On approximately 2:30 AM EST, TV broadcasts reported that PA, WI, AZ, NV and GA have decided to cease vote counting operations and will continue the following day. The unanimous decision to intentionally stop counting by all 5 battleground states is highly unusual, possibly unprecedented and demonstrates prior coordination by election officials in battleground state. There would be no legitimate reason battleground states need to pre-coordinate election activities and stop on-going adjudication processes. However, is equally puzzling that the vote counting did not stop, as reported. In fact, it continued behind closed doors in early hours of November 4, 2020. This activity is highly unusually and demonstrates collusion to achieve desired results without being monitored by watchers.

c. When analyzing the NT Times data for the 2020 election, I conclude that the software algorithm manipulated votes counts forging between 1-2% of the precinct results to favor Vice President Biden. The software performed data alteration in real-time in order to maintain close parity among the candidates and without raising red flags. The specific software algorithm was developed by Smartmatic and implemented in DVS machines to facilitate backdoor access by a nefarious operator to manipulate live data, as desired.

d. The DVS Democracy Suite's ImageCast Central optical scanner failed to correctly verify and validate absentee ballots, as described in its own literature. There is reported evidence that the optical scanner accepted and adjudicated ballots that did not have signatures or other key features that is required for ballot validation and verification. This indicates that the DVS system configuration was modified to accept invalid ballots when they should have been rejected.

e. After the DVS ImageCast scanner validates a ballot, by design, it is required to tabulate and store the results in a cast vote record along with a human-readable image of the ballot that has been scanned. The image, called AuditMark provides the user with scanned results that is verifiable. However, media reports indicate that not only did the ImageCast fail to properly verify absentee ballots; it also failed to maintain records of the AutitMark that would be necessary to conduct an audit. The only way to alter this protocol is to alter the system configuration and prevent the ImageCast scanner from rejecting illegal ballots; and reprogram AuditMark to store ballot image that could be verified. This is evidence of fraud perpetrated to prevent investigators to discover the number of invalid votes that were cast.

f. The cryptographic key store on DVS thumb drive (reported stolen in Philadelphia) was used alter vote counts prior to up chain reporting. Since DVS uses the same cryptographic key for all its voting systems in all battleground states, the key allowed a remote operator to conduct massive attacks on all battleground state data set without being detected.

g. Beginning on approximately 4:30 AM EST on November 4, 2020, the vote counts favored Vice President Biden by nearly 80% in many jurisdictions. The data distribution is statistically congruent, even when considering a larger number of absentee ballots were collected for Vice President Biden.

h. The data variance favoring Vice President continues to accelerate after 4:30 AM EST on November 4, 2020 and continues until it momentum through November 9, 2020. This abnormality in variance is evident by the unusually steep slope for Vice President Biden in all battleground states on November 4, 2020. A sudden rise in slope is not normal and demonstrates data manipulation by artificial means. For example in PA, President Trump's lead of more than 700,000 count advantage was reduced to less than 300,000 in a few short hours, which does not occur in the real world without an external influence. I conclude that manually feeding more than 400,000 mostly absentee ballots cannot be accomplished in a short time frame (i.e., 2-3 hours) without illegal vote count alteration. In another case for Edison County, MI, Vice President Biden received more than 100% of the votes at 5:59 PM EST on November 4, 2020 and again he received 99.61% of the votes at 2:23 PM EST on November 5, 2020. These distributions are cause for concern and indicate fraud.

i. DVS has acknowledged that Chinese made parts are used in its voting machines. However, the company is unwilling to share details on its supply chains, foreign ownership, or its relationship with China, Venezuela and Cuba. In particular, I have seen USIC intelligence reports showing China's espionage activities in the United States and efforts to infiltrate elections. Since these countries are our enemies, I conclude that FIS and other operators were involved to influence the outcome of the 2020 election.

j. A Man-in-the-Middle (MITM) cyber attack was carried out by covert operators using sophisticated tools, such as Hammer and Scorecard. The MITM attack occurred in two ways. Initially, remote operatives used USB memory cards containing cryptographic keys and access system backdoors to alter votes in battleground states. Subsequently, the results were forwarded to Scytl/SOE Software servers located in Frankfurt, Germany (previously, Barcelona, Spain). The MITM attack was structured to ensure sufficient data alteration had occurred prior to forwarding the tallied results to the Scytl/eClarity Software Electronic Night Reporting (ENR) system. The reason election data are forwarded overseas is to avoid detection and monitoring by the USIC to obfuscate the MITM.

k. In my expert opinion, the DVS Democracy Suite, Scytl/SOE Software/eClarity and Smartmatic have not produced auditable results in the 2020 election. It is evident that ballots were not properly validated, system records were not kept, and the system experience considerable instability even several days prior to November 4, 2020 that require DVS to implement software changes at the last minute. In addition, the disparity in data distribution after 4:30 AM on November 4, 2020 indicates significant systemic anomalies that were widespread among all battleground states. The evidence is both extensive and persuasive and indicates large-scale fraud by remote operators.

16. I conclude that a combination of lost cryptographic key contained on stolen USB memory cards, serious exploitable system and software vulnerabilities and operating system backdoor in DVS, Scytl, SOE Software/eClarity and Smartmatic created the perfect environment to commit widespread fraud in all

states where these systems are installed. My analysis of the 2020 Election from NY Times data shows statistical anomalies across the battleground state votes. These failures are widespread and systemic - and sufficient to invalidate the vote counts.

17. I conclude with high confidence that the election 2020 data were altered in all battleground states resulting in a hundreds of thousands of votes that were cast for President Trump to be transferred to Vice President Biden. These alterations were the result of systemic and widespread exploitable vulnerabilities in DVS, Scytl/SOE Software and Smartmatic systems that enabled operators to achieve the desired results. In my view, the evidence is overwhelming and incontrovertible.

Pursuant to 28 U.S.S. 1746, I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct to the best of my knowledge.

EXECUTED ON: November 25, 2020

By: ______________________
Navid Keshavarz-Nia, Ph.D., Ed.D.