DEBUNKING RESPONDANT CLARK COUNTY REGISTRAR JOE GLORIA'S CLAIMS OF PERFECT SECURITY OF NEVADA ELECTION SYSTEM AS SUBMITTED IN RESPONDENTS' APPENDIX TO WRIT OF MANDAMUS DATED 27SEP2016

Prepared by Expert Witness, Colonel Robert E. Frank, USAF (Ret.)
October 9, 2016

Concerning NV Supreme Court Case 71204, Document No. ERA00001-00035, Appendix Vol. 1

Writ of Mandamus Rules apparently bar submission of new evidence, so it seems the Respondent's Appendix should be totally disallowed. But, if allowed in as new evidence, below are my selected responses. I have only responded briefly to the most egregious misstatements and/or seemingly willful false claims in Mr. Gloria's 2015 statements.

My comments are limited at this time to Mr. Gloria's unsubstantiated and unsworn claims on Appendix Vol. 1 pages ERA00025--ERA00029. Mr. Gloria's statement was not notarized and sworn when delivered to the Nevada Legislature Committee in March 2015. And, while he claimed his statements at that time were speaking for all Nevada Counties and the NV Secretary of State, nothing was submitted for the record to establish/confirm that claim.

Mr. Gloria also failed to submit a statement of computer systems security claims in a notarized affidavit under oath to the 8th District Court. He had admitted he has had no IT education, training or professional IT experiences. But, he has never allowed open cross examination of him or his staff concerning his highly questionable NV computer system security claims. He basically demands that citizens blindly accept his unqualified opinions. Finally, the NV Secretary of State organization has never published anything claiming its election system is secure, should be considered secure, or even complies with any basic IT security standards.

Also, contrary to the headline on this document claiming "*ELECTED RESPONDENTS' APPENDIX TO ANSWER TO EMERGENCY PETITION FOR WRIT OF MANDAMUS, VOL. 1*", the Clark County Registrar of Voters, Mr. Joe Gloria is not an "elected" official. Unlike the Clark County Clerk, Ms. Lynn Goya who is elected, Mr. Gloria is an appointed government employee and subject to employee ethical and statutory constraints.

1. Appendix Page ERA00025, Line 35, Mr. Gloria States: *"…we have had no documented incidents related to the tabulation of votes or the accuracy of our system in the state of*

Nevada since the implementation of direct record electronic machines."

- Q: Is it not true there are no precise ways to detect or openly document "all vote tabulation errors"—now or during the past decade? Nor can anyone obtain current facts about election system accuracy without opening up the sealed records?

- A: It is true that despite the statute provisions for election contests, the election system has never allowed unsuccessful candidates or concerned citizens to successfully petition a Nevada Judge to order sealed records of questioned precincts to be compared to the electronic reports. But, it is clear that is the only way the truth can be learned. The statement is deceptive because during every election cycle there are many reports of apparent voting machine malfunctioning and "calibration" errors. But, as stated by the White Pine District Attorney in April 2016 (attached), if criminal tampering might be involved, without a judge allowing the opening of the sealed records it is impossible to investigate and prosecute election system fraud.

2. Appendix Page ERA00026, Lines 6-15, Mr. Gloria States: *"The reason for our level of success is because we use the direct-recording electronic voting system, which is the most accurate form of recording votes available in the industry. We have utilized this technology since 1996, and it has proven itself to be 100 percent accurate in tabulating results. There is a system of oversight provided by federal and state law which ensures the accuracy of our system. The processes and procedures put in place by every county in the state of Nevada, with oversight from the Office of the Secretary of State, provides for a transparent and reliable election process with a high degree of integrity."*

- Q: Is it not true the Nevada DRE system components (manufactured by Diebold and now called Dominion) was acquired as insecure systems with federal funds, and such DRE systems were shown on national TV and the Internet as being easily corrupted or hacked by such credible organizations as the Princeton Department of Computer Science? (video link)

- Q: Is it not also true that computer professionals will agree that no computer system composed of hundreds of devices and managed with normal controls at hundreds of sites can deliver 100% accurate results for over a decade? Even simple machine usage failures, wear and tear, and mal-calibration from frequent transport from central storage to dozens of voting sites can create a minimum of 5% to 10% machine failure rates.

- Q: And, is it not also true it is impossible for the Nevada Secretary of State with its insufficient computer security expertise and inadequate resources to provide 100% oversight with a high degree of integrity for system security in all voting sites in the state?

- A: If any or all the above is true, such bald statements must be seen as outrageously indefensible and willfully false? And, if disputed, the Registrar and NV SoS must prove such unbelievable assertions. Blind acceptance of such claims is simply unacceptable. Meanwhile, the only way to audit suspected failures or corruption is by reviewing the sealed ballet records from suspected failing precincts with the reported summaries.

3. Appendix Page ERA00026, Lines 16-25, Mr. Gloria States: *"Starting at the federal and state level, there are standards for voting equipment. Before any system can be considered far purchase at the state level, it must pass the federal level of compliance. There are three certified laboratories that are authorized to provide this testing and scrutiny. There is a system of oversight in place also at the state level. Once they have a system certified at the federal level, the State of Nevada, in partnership with the State Gaming Control Board, puts the machine through its paces to ensure that it tabulates correctly and has redundancy. Also, each county is required to run its own certification with each machine. So there are three levels where we put these machines through their paces, starting with the federal level."*

   - Q: Is it not true that the claimed federal and state "standards" for a limited number of voting equipment types have nothing to do with end-to-end election system integrity and security of results?

   - Q: Is it not also true that federal testing laboratories are only responsible for machine reliability criteria to reduce the incidence of poorly constructed equipment—not to ensure hardware, firmware and software voting results integrity and security?

   - Q: Is it not also true that testing is only done on sample equipment, and that the hundreds of machines shipped to the states over the years are only tested in NV for basic functionality by the state's contractors and a few employees?

   - Q: And, is it not true that such voting machines, scanners, related PCMCIA memory cards, PC laptop consolidation systems and networking devices and all software used in the SoS election system can be easily damaged and/or software corrupted without being detected before, during and after elections?

   - Q: Finally, is it not true that, regardless of how effective all of the claimed testing might be, it is possible (as recently declared by the FBI and DHS) that local, national and international hackers could corrupt any election system if modern cyber defensive expertise was not available?

A: Of course, all of the above is true. If the White House, Democratic Party, FBI, dozens of military systems, etc. can be illegally penetrated and corrupted, how can the NV election system management claim to be smarter and more capable that everyone else?

4. Appendix Page ERA00027, Lines 4-11, Mr. Gloria States: *"There is a different set of testing before an election. There are three rounds of certification testing. It is performed prior to early voting, prior to Election Day, and after Election Day. There is a certification board made up of members of the community, and these citizens witness each round of testing, which involves the following areas, Hash code testing verifies we are using the certified version of software tested in federal laboratories as mandated by the State of Nevada. It also ensures the accuracy of the tabulation by our system, because we place a predetermined tally into it through our mail system, our early voting system, and through Election Day. This predetermined tally is run on all of the machines and tabulated to ensure that we can accurately predict the outcome. This proves that the system tabulates accurately and is the purpose of that round of testing. The testing is performed before every election, whether at the state, county, or city level."*

   - Q: Is it true the hash code testing process described could be vulnerable to a variety of well known cyber attacks? Has there been any professional risk assessment studies performed on the NV system by professionals in recent years?

   - Q: Is it true the local election system testing series including hash code testing described by the Registrar could be invisibly penetrated/defeated by criminal hackers? Or, does the Secretary of State and/or Clark County Election Department follow commercial practices by secretly employing or contracting with "ethical hackers" working independently to discover and repair security weaknesses in the election system prior to elections?

   - A: Since there is no public knowledge of any special cyber security and/or fraud examiner expertise available to the SoS or CC Election Department, we must conclude that allegations of high risks to corruption and tampering of votes through the NV Election System are valid.

5. Appendix Page ERA00027, Lines 13-25, Mr. Gloria States: *"I want to address the certified fraud examiner and its fiscal impact. In Clark County, the fiscal impact could reach over $400,000 annually. As written and as reported by our internal auditor director, it would be difficult for any accounting firm to bid on the work. Any auditor who can say there is no fraud, no errors, or that all policies and procedures were followed, is misleading the client.*

The best we can do is attest that we have reasonable reassurance there were no material errors or deviation from policy and procedures. The amount of work is monumental. One full-time employee plus the majority of my staff at election time could not meet the 30-day time frame. The audit contract would cost approximately $300,000 a year, which is 3,000 hours at $100 an hour. It would also put requirements on the staff to provide information during the busiest times. You would have as many hours gathering the information and answering questions."

- Q: Is it true there has been no attempt by the State of Nevada or Counties to design and implement an end-to-end, certifiably secure election system? And, is it true there has been no attempt to determine what it would cost to implement a truly secure election system or to establish independent fraud examiner services to certify operational security performances as expected?

- A: If true, then the stated cost claims are invalid as they are not based on facts. Such costs must be professionally developed based on the system characteristics and receipt of written, competitive bids from Certified Fraud Examiners. If not true, the SoS and CC Election Department must be required to openly demonstrate its end-to-end security capabilities and sincere interest in serving the public interest with an election system that is "trustworthy" and independently audited before, during and after every election (not on a 24/7, 365-day year basis).

6. Appendix Page ERA00027, Lines 34-39, Mr. Gloria States: *"…every voter is required to print from the voter-verifiable paper audit trail, known as the VVPAT, a printed record that identifies for them who they voted for in each and every contest. When their ballot is cast, a barcode is printed at the bottom of that printout that we can use to manually verify that the choices made are in fact what the voter intended."*

- Q: Is it true that VVPAT records are only visible at the time of voting to those who vote on DRE machines and copies of the voting record are not provided to the voters?

- Q: And, is it true there is no end-to-end audit trail and chain of custody processing procedures to enable voters to be sure their ballots were counted and certified as fully processed throughout the whole system—regardless of the various formats?

- Q: Is it also true there is no way for voters, election workers and managers to know if the votes cast at the source machine are 100% faithfully carried forward through all of the handling, election system machinery and software processing until the final summary records are reported to the public?

- A: All of the above is true, and that is why such vital features as end-to-end audit trails, chain of custody records, tamper-evident seals on all components, background checks on everyone who handles voting machines and ballots, etc. are required for the future to build a trustworthy system.

7. Appendix Page ERA00027, Lines 40-43 and ERA00028, Lines , Mr. Gloria States: *"It has been discussed that it is possible to hack into our system. Our network for tabulating votes is set up on a stand-alone secure network. It is a room that requires three levels of access: a key to enter the building, access to the alarm code, and biometric security for access to the system. Every employee assigned to work in the tabulation room cannot log into the tabulation system without verifying that the fingerprints match."*

   - Q: Is it not true that while multi-layered defenses to control physical access to election facilities is vital, the security system features must not stop there? Is it not true that the Argonne National Laboratory's Secure Computer Scientist Team (who manage security procedures for our military nuclear weapons stockpiles) showed in recent years via Internet Utube that anyone with access to common types of DRE voting machines can (within a minute or so) install a $26 electronic component purchased from a Radio Shack retail store that provides remote radio control of a voting machine? (see link) Have SoS and County election managers responded to that threat and taken action to prevent it from happening in NV?

   - Q: Is it false to claim that because the DRE/voting machines are not directly connected to the Internet they are invulnerable to hacking?

   - Q: Is it true that Voting Machines can be remotely accessed through corrupted or counterfeit PCMCIA Memory/data Transfer Cards, scanning machines using the same PCMCIA data Transfer cards, Personal Computer laptop using the same PCMCIA memory/data cards and modems being used on phone lines and/or the Internet? (Click link for video evidence.)

   A: If so, why have not the problems and vital corrective actions taken for the wide variety of known electronic election system vulnerabilities been reported to our citizens?

Appendix Page ERA00027, Lines 7-18 Mr. Gloria States: *"We have audits within each early voting site, and they are electronically tied to each machine. The software has a check sum value that is written to each one of the electronic cartridges within these machines. If anyone makes an attempt to hack into the system, there is a redundant data path that has three areas* *of storage: the results cartridge that we tally every night, the central processing unit (CPU), and the printed record. I have the highest degree of confidence in the processes we use to ensure the integrity of our elections in Clark County and the state of Nevada. Our state is highly regarded in the election community, as evidenced by being named in the top five as ranked by the Pew Elections Performance Index for two years in a row. If funds are allocated to promote election integrity, it should be spent in other areas."*

- Q: Since you have admitted to not having IT education, training or work experience, how can you have the "highest degree of confidence" in the ensuring the integrity of NV election systems? Have you contracted with national IT security experts to augment your lack of expertise?

- Q: Who on your staff do you delegate the system security responsibilities to, and where can we find documents detailing his professional duties and responsibilities?

- Q: What are the criteria for being selected into the top five Pew Elections Performance criteria? Is end-to-end election system security part of the criteria?

-A: Until independent audits by CFE's are accomplished, no one can consider the Nevada Election System trustworthy.

Robert E. Frank