AFFIDAVIT

1. I, Clint Curtis, swear that the following is true and correct.

2. I was born in Illinois and I am 46 years old. I graduated from college at Illinois State University with a degree in political science history and later started my own company and learned to write computer software programs.

3. In the mid 1990s, I moved to Florida and later got a job with Yang Enterprises (YEI) in Oviedo, Florida in August 1998 as a computer programmer. I became the lead programmer for YEI and had daily meetings with YEI CEO Mrs. Li Woan Yang. At the time, I was a life long registered Republican.

4. In the early fall of 2000, a man came into YEI and was introduced to me as Tom Feeney, future Speaker of the House of Representatives in Florida as well as YEI's corporate counsel and lobbyist.

5. I sat in meetings with Mr. Feeney on at least a dozen occasions over the next several months and we discussed several potential projects to determine their viability. In short, I was the technology adviser to Mr. Feeney on these proposals. After these consultations, Mr. Feeney would advise YEI on how best to procure the contracts for these projects.

6. During a meeting in late September or October of 2000 at YEI, there were four people present including myself, Tom Feeney, Mike Cohen, Mrs. Yang, and to the best of my recollection, two other YEI employees came in and out of the room during the course of the meeting. Mr. Feeney said that he wanted to know if YEI could develop a prototype of a voting program that could alter the vote tabulation in an election and be undetectable. He was very specific in the design and specifications required for this program. He detailed, in his own words, that; (a) the program needed to be touch-screen capable, (b) the user should be able to trigger the program without any additional equipment, (c) the programming to accomplish this remain hidden even if the source code was inspected.

   I told him that it would be virtually impossible to hide such code written to change the voting results if anyone were able to review the uncompiled source code. However, if the code were compiled before anyone was allowed to review it then any vote fraud would remain invisible to detection. After further discussion, Mrs. Yang told Mr. Feeney that we would attempt to build a prototype for this program so he could see it, test it, and show it to others. It was my initial belief that Mr. Feeney was interested in such a program because of a concern that Democrats would try to use such a program to steal an election, and he wanted to be able to detect and prevent that if it occurred.

7. Shortly thereafter, as directed, I created the vote fraud software prototype by making a software program where each candidate is represented as an element of

an array of controls. Each candidate is listed in a database, and their number corresponds to where you want them to show up in that array. When the program starts, it reads the database, and takes the number assigned to the candidate and fills in the label with the index that matches that number. That allows the program to work dynamically. It doesn't matter who the candidate is as they have been equated to the index number assigned. From a normal perspective it allows the voter to select the candidate, click on the submit button and the candidate's selected previous vote total is then increased by one.

In the vote fraud prototype that I created things were not what they seemed. Hidden on the screen were invisible buttons. A person with knowledge of the locations of those invisible buttons could then use them to alter the votes of any candidate listed. By clicking the correct order of invisible buttons the candidate selected by the user is compared to other candidates within that same race. If the candidate they selected is leading the race, nothing happens. If the other candidate is leading the race, the vote totals are altered so that the selected candidate is now leading the race with 51% of the vote. The other candidates then share the remaining 49% in exact proportion to the totals they had previously. In the prototype supplied to Feeney, the vote totals showed on the screen. In an actual application, the user would receive no visible clues to the fraud that had just occurred. Since the vote is applied by race, any single race or multiple races can be altered. The supervisors or any other voter would never notice this fraud since no visible sign would appear. Additionally, the procedure could be repeated as many times as was necessary to achieve the desired results. No amount of testing or simulations would expose the fraud as its activation and process is completely invisible to everyone except the person programming the vote fraud routine.

The same procedure could be automated to activate without any user intervention whenever the machine detects a certain pattern of voting. The algorithm could also be altered from hidden keys or triggers that would allow the fraudulent user to manipulate both the margins and percentages of any particular race. In most national elections it is not necessary to win every area.

8. Once I had the software program done, I wrote a report on how a person could see voting manipulation simply by looking at the source code. Any manipulation of the vote and the procedures for flipping the vote would be obvious to a competent programmer. I provided the program to Mr. Hai Lin Nee, the Quality Control person at YEI, and discussed it with him. He approved its distribution.

9. I gave the software program, which was on a CD disc, and the report that was on disc and on paper, to Mrs. Yang. I stressed that she and Mr. Feeney could view the operation of the program and then see how to detect such fraudulent source code so it could be prevented. Conversely, if they allowed blind (already compiled) code to be used (no source code provided) and there were no paper receipts, the votes could be flipped from one candidate to the other without any possible way for the deception to be detected. I explained that this could be done with a touch

screen machine or automatically. She immediately stated, "**You don't understand, in order to get the contract we have to hide the manipulation in the source code. This program is needed to control the vote in South Florida.**" I was shocked that they were actually trying to steal the election and told her that neither I nor anyone else could produce any such program. She stated that she would hand in what I had produced to Feeney and left the room with the software.
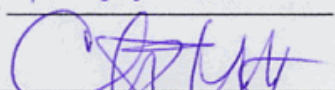
10. In my role as a technology advisor at YEI, I was present at subsequent meetings between Mr. Feeney and Mrs. Yang. In several of those meetings, prior to the 2000 election, it became clear to me that Mr. Feeney was well aware that by artificially reducing the margin of victory of the opposition party in areas where they were the strongest, the overall outcome would then favor his candidate. As well, he bragged that he had already implemented "exclusion lists" to reduce the "black vote". He further mentioned that the "proper placement of police patrols could further reduce the black vote by as much as 25%." I didn't know at the time, if Mr. Feeney had meant that as a racial joke or actually part of the plan.

11. Soon thereafter, I resigned from YEI and took another job at the Florida Department of Transportation (FDOT). While there, I discovered some other illegal activities of YEI, who had contracts with FDOT, involving over-billing and defrauding of the State of Florida regarding contracts that I had worked on at YEI. I reported this information to the FDOT Inspector General's office and they began harassing me and another employee, Mavis Georgalis, who had made similar reports and eventually we were both fired by FDOT on the same day. We later filed whistleblower complaints against FDOT. Mrs. Georgalis was successful but mine was filed after the deadline and was dismissed.

12. The IG at the FDOT, Raymond Lemme, pursued some of the allegations I made against YEI, as I had advised him of the information concerning Tom Feeney and the vote fraud issue, illegal aliens employed by YEI, fallacious over-billing, and a wiretapping module that was placed into a FDOT software program for the document management system. Mr. Lemme continued to meet and talk with me about matters relating to the case after I was fired from FDOT, and in June of 2003, he told me that he had tracked the corruption "all the way to the top," and that the story would break in the next few weeks and I would be satisfied with the results. A few weeks later, on July 1st, Mr. Lemme was found dead with his arm slashed in a hotel room in Valdosta, Georgia.

13. Hai Lin Nee, the Quality Control manager at YEI, also worked with a company called Azure Systems of Orlando. While at YEI, Mrs. Yang provided Mr. Nee with many gigabytes of downloaded information from NASA projects that YEI was working on, including the Maximo facilities repair maintenance database, which he then took from the premises of YEI. This happened on several occasions. Also, I saw Mrs. Yang send a great deal of internal information to her brother in China, who, she had informed me, had been deported for spying. Wayne Leaders, an investigator for NASA, later confirmed this deportation of Mrs. Yang's brother.

Mr. Leaders was responding to one of my multiple attempts to contact NASA on the YEI matter. I had also made a report to Mr. Leaders regarding a program that I had written for FDOT that allowed for outside contractors to submit documents to FDOT. Between the time I wrote the program and the phase of Mr. Nee's quality assurance, I discovered that Mr. Nee had inserted a wiretapping module into the software that copied all the information bound to FDOT and sent it via the Internet to YEI. I have reason to believe that he also did this with a similar program I had written for NASA.
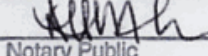
14. In late 2003 or early 2004, I provided information to Detective Rob Pace at the Leon County Terrorist Task Force concerning Hai Lin Nee who I had learned was an illegal Chinese alien. I informed Detective Pace that Mr. Nee was working at YEI on NASA programs. Hai Lin Nee was subsequently arrested by federal officials in Orlando, Florida on or about March 17, 2004 on charges that included sending radar guidance system chips for Hellfire Anti-Tank Missiles to a company in Communist China.

15. I reported much of this information to the FBI, CIA, Homeland Security and Florida Department of Law Enforcement through emails but the only one to respond was Tom Yowell, a Special Agent with the Florida Department of Law Enforcement assigned to the FBI Joint Terrorism Task Force. Mr. Yowell responded via email on November 22, 2004, that YEI was under investigation by another office of the FBI and that if I supplied him with my telephone number and name, he would pass that information to the other office so that they could contact me. I did, but I have not yet heard back from the FBI or Mr. Yowell as of today's date. I have filed a QUITAM, which is still pending, with the State of Florida concerning the over-billing by YEI.

I have never been charged or convicted of any crime although I have been involved with two civil matters. The first is a copyright infringement case dating from 1997. The case was ultimately settled out of court with no finding of wrongdoing by anyone, and with both parties agreeing to pay their own attorneys' fees. The second being a suit that YEI has brought against Mavis Georgalis and me in retaliation for reporting on its illegal activity. The YEI civil suit is still pending and the court eventually required that FDOT to be included as a co-defendant as well because it was the sole owner of the software that Ms. Georgalis and I were falsely accused of having appropriated. YEI employees have so far refused to subject themselves to depositions in that pending case.

I declare under penalty of perjury, pursuant to 28 USC § 1746, that the above is true and correct.

Executed on 12-06-04

Clinton
Clint Curtis

Subscribed and sworn to before me, in my presence, this 6th day of December, 2004 a Notary Public in and for the State of Maryland.

Notary Public

My commission expires February 12, 2007